REKONSTRUKCE A VÝSTAVBA SVĚTELNĚ SIGNALIZAČNÍCH ZAŘÍZENÍ

TECHNICKÁ SPECIFIKACE ZADAVATELE PRO TECHNOLOGII SSZ

Část určená pro zhotovitele díla

Platnost dokumentu od:	03. 02. 2023
Dokument nahrazuje verzi ze dne:	22. 02. 2022
Zpracovatel dokumentu:	Brněnské komunikace a.s.
Zadavatel:	Statutární město Brno

Únor 2023

Obsah

1. Seznam použitých zkratek

BKOM	Brněnské komunikace a.s.
BO	Back Office, centrální prvek systému
C-ITS	kooperativní inteligentní dopravní systémy
CTD	centrální technický dispečink
DHCP	dynamic host configuration protocol
DPMB	Dopravní podnik města Brna, a.s.
DŘ	dopravní řešení
DÚ	dopravní ústředna
EVA	Emergency Vehicle Approvaching
FNr	číslo připojeného zařízení
FW	programové prostředí výrobce pro řízení systému (firmware)
GIS	geografický informační systém
HLN	Hazardous Location Notification
HW	veškeré fyzicky existující technické vybavení (hardware)
IAD	individuální automobilová doprava
ISMS	systém řízení bezpečnosti informací (Information Security Management System)
ISV	Intersection Signal Violation
ITS	Inteligentní dopravní systémy (Intelligent Transport Systems)
ITS-G5	komunikační standard ve vyhrazeném pásmu 5,9 GHz pro ITS
IZS	integrovaný záchranný systém
IZS plán	signální plán pro vozidla IZS spouštěný na základě komunikace V2X
LED	elektroluminiscenční dioda (Light-Emitting Diode)
MAPEM	MAP (topologie komunikace) rozšířená zpráva
MHD	městská hromadná doprava
MMB	Magistrát města Brna
Mp-SÚ	metodický pokyn vydaný správním úsekem BKOM
OBU	palubní jednotka vozidla s V2X (On-board unit)
OCIT-O V2.0	komunikační protokol pro komunikaci DÚ s řadiči SSZ
OCIT-O profil 3	přenos dat prostřednictvím sítě Ethernet za použití DHCP
PC	počítač (personal computer)
PČR	Policie České republiky
PD	projektová dokumentace
PK	pozemní komunikace
PKI	Public Key Infrastructure
PTP	Public Transport Preference
PVD	Probe Vehicle Data
RIS II	řídící a informační systém DPMB
RSU	stacionární jednotka pro V2X komunikaci, umisťovaná na dopravní infrastrukturu (Road size unit)
RWW	Road Works Warning
SMB	Statutární město Brno
SmGŘ	směrnice vydaná generálním ředitelem BKOM
SP	signální plán
SPATEM	SPaT rozšířená zpráva o stavu signálů na návěstidlech

SRM	zpráva pro požadavek na preferenci z vozu (Signal Request Message)
SSM	zpráva pro odpověď z řadiče přes RSU (Signal Status Message)
SSZ	světelné signalizační zařízení
SÚ	Správní úsek
SW	data a programové vybavení (software)
TP	technické podmínky
TSZ	technická specifikace zadavatele
Tx	aktuální hodnota časové osy signálního plánu udávaná ve vteřinách
ÚDI	útvar dopravního inženýrství
V2X	komunikace vozidla s okolím (vozidlo, infrastruktura)
VIP plán	signální plán pro vozidla s právem přednosti jízdy spouštěný z DÚ
VO	veřejné osvětlení
WCW	Weather Condition Warning
ZNr	číslo serveru

2. Platnost dokumentu

2.1 Tento dokument ruší platnost předchozí verze.

2.2 Tento dokument je platný od data uvedeného v úvodu, do vydání aktualizované verze, ale nikdy ne déle než 3 roky.

2.3 Tento dokument řeší požadavky na technologie SSZ a proces předání technologické části díla zadavateli. Tento dokument neřeší stavební a elektromontážní práce, které jsou obsaženy v projektové dokumentaci.

3. Předmět dodávky technologie SSZ

3.1 Dodávka řadiče SSZ (viz Kapitola 5).

3.2 Programování řadiče dle DŘ dodaného zadavatelem ve formátu PDF, včetně případných následných doladění. Aktuální časová hodnota signálního plánu (Tx) a tomu odpovídající signální obrazy skupin zpracovávaných řadičem musí být shodné s časovou hodnotou SP a odpovídajícím stavem světelných skupin dodaného DŘ (viz příloha 14.10).

3.3 Dodávaný řadič bude odpovídat požadavkům zadavatele na kybernetickou bezpečnost (viz Kapitola 6)

3.4 Dodávka technologických periferií SSZ (viz Kapitola 7) a dodání aktuálního servisního SW k periferiím.

3.5 Dodávka hardwarového a softwarového vybavení pro preferenci vozidel MHD a IZS na SSZ (viz Kapitola 8).

3.6 Dodání servisního SW řadiče (viz. Kapitola 9).

3.7 Připojení řadiče k nadřazené dopravní ústředně (viz. Kapitola 10).

3.8 Poskytování úplného servisu nutného pro trvání záruky v délce minimálně 24 měsíců. Nejedná se však o úkony běžné údržby, které po převzetí díla bude zajišťovat provozní středisko servisu a údržby SSZ provozovatele, jako jsou nutné testy dopravního řadiče a revize zařízení SSZ.

3.9 Deset doladění signálních plánů a logiky řízení, které může být zadavatelem díla v průběhu jeho realizace, zkušebního provozu a záruční doby požadováno. Doladění bude realizováno dle změnového DŘ dodaného zadavatelem ve formátu PDF, na základě jeho výzvy.

3.10 Zaškolení obsluhy budoucího správce SSZ (BKOM) s dodanými SW prostředky (viz bod 13.19).

3.11 Předmětem zakázky není poskytování pozáručního servisu.

4. Soulad řešení s platnými předpisy a normami

4.1 Zadavatel požaduje dodržení následujících zákonů a technických norem v platném znění:

Zákon 110/2019 Sb.	–	Zákon o zpracování osobních údajů
Zákon 181/2014 Sb.	–	Zákon o kybernetické bezpečnosti
GDPR (General Data Protection Regulation)	–	Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
ČSN EN 12 368 ed.2	–	Řízení dopravy na PK – Návěstidla
ČSN EN 12 675	–	Řízení dopravy na PK – Řadiče světelných Signalizačních zařízení – Funkčně bezpečnostní požadavky
ČSN EN 50556 ed.2	–	Systémy silniční dopravní signalizace
ČSN EN 61508-6 ed.2	–	Funkční bezpečnost elektrických/elektronických/ programovatelných elektronických systémů související s bezpečností
ČSN 73 7042	–	Řízení dopravy na pozemních komunikacích – Národní požadavky
ČSN 36 5601 – 1	–	Světelná signalizační zařízení, Technické a funkční požadavky – část 1: Světelná signalizační zařízení pro řízení silničního provozu
ČSN 73 6101	–	Projektování silnic a dálnic
ČSN 73 6102 ed.2	–	Projektování křižovatek na silničních komunikacích
ČSN 73 6110	–	Projektování místních komunikací
ČSN 73 6021	–	Umístění a použití návěstidel

4.2 Zadavatel požaduje dodržení následujících TP Ministerstva dopravy ČR:

TP 65	–	Zásady pro dopravní značení na PK
TP 81	–	Navrhování SSZ pro řízení provozu na PK
TP 133	–	Zásady pro vodorovné dopravní značení na PK
TP 165	–	Proměnné svislé dopravní značky a zařízení pro provozní informace
TP 169	–	Zásady pro označování dopravních situací na pozemních komunikacích
TP 182	–	Dopravní telematika na PK
TP 188	–	Posouzení kapacity neřízených úrovňových křižovatek
TP 189	–	Stanovení intenzity na PK

4.3 Další standardy, jejichž dodržení, dle aktuálního znění, zadavatel požaduje:

OCIT®	–	Open Communication Interface for Road traffic control systems (http://ocit.org)
		Pro komunikaci DÚ s řadiči SSZ zadavatel v současnosti využívá otevřený komunikační protokol OCIT-O ve verzi V2.0. Ve všech podmínkách uvedených v této technické specifikaci zadavatel požaduje zajištění kompatibility s tímto protokolem a využití funkcionalit pro ovládání a nastavování řadiče z DÚ v plném rozsahu.
Preference MHD RIS II	–	Komunikační protokol pro komunikaci vozidel MHD s RSU jednotkami na SSZ, viz příloha.
C-ROADS CZ	–	C-ROADS CZ Use Case katalog https://c-roads.cz/systemy-c-its/technicke-normy-a-standardy/
C-ROADS CZ	–	C-ROADS CZ Seznam C-ITS standardů https://c-roads.cz/systemy-c-its/technicke-normy-a-standardy/
C2C Consortium	–	C2C Communication consortium Automotive Requirements for SPaT and MAP https://bit.ly/2XICTlv
SmGŘ – 039	–	Bezpečnostní politika informací
SmGŘ – 042	–	Bezpečné chování uživatele
SmGŘ – 044	–	Směrnice pro správu a uživatele CTD
SmGŘ – 046	–	Organizace kybernetické bezpečnosti
SmGŘ – 061	–	Řízení dodavatelů

5. Požadavky zadavatele na řadič SSZ

5.1 Dodaný řadič musí být certifikován na úroveň integrity bezpečnosti SIL 3 ve smyslu ČSN EN 61508 a musí splňovat kromě platných ČSN a EN i požadavek dle ČSN EN 50556 ed.2 čl. 5.2.3.3 pro třídu AG3 s maximální dobou přechodu do bezpečného stavu 200ms od zjištění poruchy.

5.2 Skříň řadiče musí být plastová z materiálu odolného proti teplotám a vlivu slunečního záření.

5.3 Svorkovnice v řadiči musí být bez šroubové s možností rozpojení proudového okruhu bez vytažení vodiče ze svorky.

5.4 Řadič musí umožňovat rozdělení křižovatky na minimálně 4 dílčí uzly ovladatelné samostatně.

5.5 Řadič musí být vybaven snímačem otevření dveří řadiče.

5.6 Řadič musí být schopen detekovat a správně rozlišit všechny běžné poruchové stavy minimálně v rozsahu:

- Stavy vedoucí k vypnutí SSZ:
  - výpadek napájení
  - primární poruchy s rozlišením signální skupiny, návěstidla a komory návěstidla
  - chyby dohlídání s nutnou deaktivací SSZ
- Poruchy s částečnou deaktivací:
  - vypnutí dílčích uzlů křižovatky
- Poruchy bez deaktivace:
  - sekundární porucha s rozlišením skupiny, návěstidla a komory návěstidla
  - další chyby dohlídání bez nutné deaktivace SSZ
- Vnitřní poruchy bez deaktivace:
  - chyby komunikace
  - chyba komunikace s RSU
  - poruchy detektorů
  - chyby zdroje času

Detekce a odstranění nebezpečného stavu musí být nejméně ve třídě AG3 (do 200ms), dle normy ČSN EN 50556.

5.7 Řadič bude vybaven spolehlivým zařízením pro příjem signálu pro synchronizaci reálného času řadiče, například GPS.

5.8 Řadič musí umožňovat nastavení stmívání návěstidel pomocí:

- bezpotenciálového vstupu řadiče z důvodu aktivace ztlumeného stavu soumračným spínačem (světelné podmínky dané lokality nebo stavu VO)
- časového rozvrhu zadaným v SW řadiče

Na připojeném servisním PC a dopravní ústředně (lokálně i dálkově) musí být jasná a zřetelná textová informace o tom, že SSZ je ve ztlumeném stavu; v provozním deníku musí být uvedeny časové údaje o okamžiku ztlumení návěstidel a přepnutí do plného svitu.

5.9 Řadič musí umožňovat úpravu následujících parametrů komunikace:
- FNr
- jméno řadiče
- název domény
- adresa nebo doménové jméno serveru (ZNr)
- IP adresy zařízení nebo zapnutí přidělování adresy pomocí DHCP
- editace routovací tabulky
- „OCIT password“

5.10 Řadič musí umožňovat definici následujících parametrů signálních skupin:
- číslo signální skupiny
- jméno signální skupiny
- typ signální skupiny (například vozidlová, chodecká)
- stanovení délky přechodových stavů signálních skupin (například žlutá u vozidlových skupin)
- přiřazení k dílčímu uzlu křižovatky

5.11 Řadič musí umožňovat definici následujících parametrů detektorů:
- číslo detektoru
- jméno detektoru
- typ detektoru (například smyčka nebo video-detektor)

5.12 Řadič musí umožňovat vytvoření a editaci tabulek mezičasů, minimálních zelených a minimálních červených.

5.13 Pro realizaci konkrétního dopravního řešení i případné pozdější změny se požaduje, aby řadič umožňoval realizaci způsobů řízení minimálně v rozsahu TP 81 a umožňoval volné programování.

5.14 Řadič musí umožňovat dosažení požadovaného řízení místně bez nutnosti komunikace s nadřízeným systémem.

5.15 Řadič musí umožňovat řízení provozu v dynamickém režimu bez pevně stanovené délky cyklu signálního plánu.

5.16 Řadič musí umožňovat vytvoření minimálně:
- 30 signálních plánů
- 8 zapínacích plánů
- 8 vypínacích plánů
- 5 VIP plánů
- 8 taktů ručního řízení
- 6 tras pro průjezd vozidel IZS

5.17 Řadič musí umožňovat vytvoření a editaci zapínacích a vypínacích plánů obsahujícího následující:
- jméno signálního plánu
- délku signálního plánu
- podobu signálního plánu (časy změn signálů jednotlivých skupin)

5.18 Řadič musí umožňovat vytvoření a editaci pevných signálních plánů obsahujících následující:
- číslo signálního plánu
- jméno signálního plánu
- přiřazení tabulky mezičasů
- přiřazení tabulky minimálních zelených
- přiřazení tabulky minimálních červených
- délku signálního plánu
- přiřazení zapínacího plánu
- přiřazení vypínacího plánu
- časy změn signálů jednotlivých signálních skupin umožňujících i využití „opakované zelené“ v jednom cyklu
- zadání zapínacího, přepínacího a vypínacího bodu

5.19 Řadič musí umožňovat vytvoření a editaci dynamických signálních plánů obsahujících minimálně následující:
- číslo signálního plánu
- jméno signálního plánu
- definice jednotlivých fází
- přiřazení jednotlivých nekolizních signálů do fází
- definice jednotlivých fázových přechodů
- definice jednotlivých oblastí výzev fází
- definice jednotlivých oblastí prodlužování fází
- definice jednotlivých délek fází
- přiřazení tabulky mezičasů
- přiřazení tabulky minimálních zelených
- přiřazení tabulky minimálních červených
- délku signálního plánu
- definice zapínacího bodu
- definice vypínacího bodu
- definice přepínacího bodu
- definice synchronizačního bodu a maximální délky čekání v tomto bodě
- přiřazení zapínacího signálního plánu
- přiřazení vypínacího signálního plánu
- přiřazení sady parametrů dle logiky řízení DŘ (každý dynamický sign. plán může mít přiřazenu vlastní sadu parametrů), tento bod musí být splněn i pro dynamické plány s proměnnou délkou cyklu

5.20 Řadič musí umožňovat vytvoření a editaci VIP a IZS plánů obsahujících následující:
- číslo plánu
- jméno signálního plánu
- přiřazení tabulky mezičasů
- bod zastavení VIP plánu
- délku signálního plánu
- časy změn signálů jednotlivých signálních skupin

5.21 Řadič umožní vytvoření a editaci lokálních denních plánů (rozvrhů) v následujícím rozsahu:
- číslo denního plánu
- jméno denního plánu
- příkaz k provedení obsahující:
  - čas změny přepnutí s rozlišením na minuty
  - požadovaný stav SSZ (zapnuto/vypnuto)
  - číslo požadovaného signálního plánu
  - požadovaný stav dopravně závislého řízení s rozlišením na IAD a MHD
  - požadovaný režim stmívání návěstidel
  - požadovaný stav jednotlivých dílčích uzlů křižovatky

5.22 Řadič umožní vytvoření a editaci lokálního týdenního plánu rozlišujícího jednotlivé dny v týdnu.

5.23 Řadič musí umožňovat zadání a editaci státních svátků včetně automatického výpočtu plovoucích svátku.

5.24 Řadič umožní vytvoření a editaci lokálních zvláštních denních plánů obsahujících:
- jméno zvláštního intervalu
- přiřazený denní plán
- prioritu
- datum nebo interval

5.25 Řadič bude ukládat do své vnitřní paměti následující archivy ve smyslu uvedených požadavků po dobu minimálně 72 hodin:

- Operační archiv obsahující:
  - časovou značku záznamu
  - chybové stavy (viz bod 5.6)
  - stav SSZ
  - číslo aktivního signálního plánu
  - stav dílčích uzlů křižovatky
  - požadovaný stav dopravně závislého řízení s rozlišením na IAD a MHD
  - režim stmívání návěstidel
- Archiv zpráv obsahující:
  - všechny vytvořené zprávy včetně těch, u kterých nedošlo k odeslání vlivem výpadku komunikace
- Systémové logy
- Archiv servisních zásahů do systému
- Signalizační archiv obsahující:
  - číslo aktivního signálního plánu
  - Tx
  - stav všech signálních skupin
  - stav všech připojených detektorů
- Archiv dopravních zátěží obsahující:
  - agregované měření dopravních zátěží z dopravních detektorů
- Archiv dat detektorů obsahující:
  - nezpracovaná data detektorů

5.26 Řadič bude vybaven detektory dle stavební části PD. Všechny detektory, včetně chodeckých tlačítek a virtuální detekce (DPMB, IZS), budou zobrazeny ve vizualizaci signálních plánů (lokálně v PC i dálkově na DÚ).

5.27 Kapitola č. 5 uvádí minimální požadavky na dodávaný řadič. V případě vyšších požadavků PD na dodávaný řadič musí být tyto požadavky zhotovitelem splněny, dále časy změn dle bodů 5.18 a 5.19 musí odpovídat Tx dle DŘ.

6. Požadavky zadavatele na kybernetickou bezpečnost řadiče SSZ

6.1 Dodavatel dodá kompletní DSPS včetně popisu všech spuštěných služeb v řadiči, které se dotýkají síťového rozhraní.

6.2 Zadavatel si vyhrazuje právo provádět bezpečnostní testy za účelem zjištění kybernetických bezpečnostních zranitelností.

6.3 Zjištěná kybernetická bezpečnostní zranitelnost popsaná pomocí údajů z databáze CVE (Common Vulnerabilities and Exposures; dostupná z https://cve.mitre.org/) se považuje za vadu Zboží, kterou je Prodávající povinen odstranit, jestliže byla Prodávajícímu oznámena během Záruční doby.

6.4 Závažnost takové vady Zboží (dále jen „severita“) bude ohodnocena dle standardu CVSS (Common Vulnerability Scoring System; dostupný z https://www.first.org/cvss/). Odstraněním vady Zboží dle tohoto odstavce se rozumí zejména provedení aktualizace programového vybavení nebo implementace bezpečnostního opatření, které zamezí možnosti využití zjištěné zranitelnosti. Nedohodnou-li se smluvní strany jinak, je Prodávající povinen tyto vady odstraňovat za následujících podmínek:

a) pokud je severita vady větší než 8,9, je Prodávající povinen vadu odstranit do 2 pracovních dnů od jejího oznámení;
b) pokud je severita vady od 8,0 do 8,9, je Prodávající povinen vadu odstranit do 5 pracovních dnů od jejího oznámení;
c) pokud je severita vady od 6,0 do 7,9, je Prodávající povinen vadu odstranit do 10 pracovních dnů od jejího oznámení.
d) pokud je severita vady od 4,0 do 5,9, je Prodávající povinen vadu odstranit do 30 kalendářních dnů od jejího oznámení;
e) pokud je severita vady menší než 4,0, je Prodávající povinen vadu odstranit do 2 měsíců od jejího oznámení.

6.5 Dodavatel dodá v rámci DSPS i protokol z testování zranitelnosti dodávaného řadiče.

6.6 Zadavatel nepřipouští dodávku s vyšším skóre než středním.

6.7 Dodávaný řadič bude vybaven mechanickým dveřním kontaktem pro kontrolu otevření/zavření dveří. Zadavatel nepřipouští použití magnetického snímače potvrzujícího stav otevření/zavření dveří.

6.8 Zadavatel požaduje přístup/připojení k řadiči na místě i dálkově ze sítě logovat a vyhodnocovat počty úspěšných a neúspěšných přihlášení, po třech pokusech musí být vysláno upozornění do DÚ.

6.9 Dodavatel je povinen, jakékoliv změny FW nebo SW řadiče zdokumentovat v helpdesku správce SSZ a přiložit kopii SW do tohoto systému.

6.10 Dodavatel provede aktualizace FW 2x/rok dle kompetenčního modelu. V době záruky na náklady zakázky (zohledněno v cenách výrobků uvedených v zakázce nebo samostatná položka Rozpočtu dodávky „Kybernetická bezpečnost řadiče a RSU“).

7. Požadavky zadavatele na periferie řadiče

7.1 Umístění, funkce i velikost návěstidel a všech periferních zařízení musí splňovat požadavky projektu.

7.2 Každé návěstidlo, detektor nebo zařízení akustické signalizace nevidomých bude připojeno na samostatné vstupy/výstupy z řadiče.

7.3 Uchycení návěstidla na výložník musí být stavitelné ve vodorovné i svislé poloze. Požadujeme použití kovových držáků výložníkových návěstidel. Všechny prvky návěstidel musí být z materiálu odolného proti teplotám a vlivu slunečního záření.

7.4 Všechny komory návěstidel budou vybaveny stínítkem proti přímému osvětlení slunečním svitem.

7.5 Zadavatel požaduje využití LED návěstidel, splňujících normu ČSN EN 12368 ed.2., umožňujících snížení svítivosti alespoň o 30%, s provozním napětím do 50V o příkonu do 20W,

7.6 nebo návěstidel třídy D0, která musí splňovat následující požadavky:

- návěstidla s průměrem světelného pole 200 mm budou odpovídat třídě svítivosti B2/1 typu E nebo W, provozní napětí do 30V s odběrem do 2W a plnit třídu bezpečnosti SIL3,
- návěstidla s průměrem světelného pole 300 mm budou odpovídat třídě svítivosti B3/1, rozložení svítivosti typu N, provozní napětí do 30V s odběrem do 2W a plnit třídu bezpečnosti SIL3.

7.7 Zařízení akustické signalizace bude vybaveno přijímačem radiového signálu umožňujícím aktivaci signalizace pouze na poptávku zrakově postiženého chodce. Zároveň, při použití výzvy chodeckými tlačítky, bude signál pro aktivaci akustické signalizace spouštět chodecké výzvy na daném SSZ po dobu 2 až 5 min.

7.8 Použité detektory musí být schopny z důvodu zjišťování dopravních intenzit spolehlivě rozpoznat jednotlivá vozidla i v koloně a spolehlivě detekovat přítomnost i jednostopých motorových vozidel a cyklistů, a to i v nočních hodinách.

7.9 Zadavatel požaduje použití bez šroubových svorkovnic ve stožárech SSZ.

8. Požadavky zadavatele na technologii V2X

8.1 V současné době probíhá komunikace nad preferencí vozidel MHD na SSZ za použití technologie V2X pomocí jednotek OBU (ve vozidlech DPMB) a RSU (na SSZ).

8.2 V současné době probíhá komunikace nad přednostní preferencí vozidel IZS na SSZ za použití technologie V2X pomocí jednotek OBU (ve vozidlech HZS) a RSU (na SSZ).

8.3 Přesně určené údaje jsou do řadičů vysílány z preferovaných vozidel (MHD nebo IZS) na základě požadavků dopravního řešení a možností komunikačního protokolu.

8.4 Z poskytnutých údajů musí být řadič schopen určit míru preference vozidla v souladu s požadavky dopravního řešení.

8.5 Informace z RSU jednotky musí být do řadiče SSZ předávány prostřednictvím datové linky.

8.6 Dodané zařízení musí zajistit komunikaci se všemi vozidly MHD blížícími se k SSZ současně tak, aby nedošlo ke ztrátě jediné informace, která vede k preferenci MHD.

8.7 RSU jednotka na SSZ musí být schopna obousměrné komunikace s vozidly MHD prostřednictvím zpráv SRM a SSM, dle standardu ITS-G5.

8.8 Řadič bude ukládat do paměti všechny přijaté informace systému RIS II DPMB vysílané do řadičů SSZ z vozidel MHD. Tyto informace musí být možné zpětně načíst, aby správce SSZ (BKOM) měl možnost tato data na vyžádání poskytnout DPMB nebo vlastníkovi SSZ. Na lokálně připojeném servisním PC musí být v reálném čase zobrazeny všechny řadičem SSZ přijaté pakety z vozů MHD.

8.9 Řadič musí umožňovat zobrazení informací o průjezdu preferovaných vozidel (MHD nebo IZS) na pracovišti CTD prostřednictvím pásového diagramu (stavy detektorů).

8.10 RSU jednotka na SSZ musí být vybavena SW a HW prostředky minimálně v rozsahu nejnovějších požadavků pro C-ITS systémy (C-ROADS CZ viz bod 4.3) následujícími Use Case: EVA, ISV, PTP, PVD, WCW, HLN, RWW včetně Security PKI.

8.11 Zhotovitel musí dodat servisní SW prostředky pro dodanou RSU jednotku umožňující diagnostiku nastavení a funkcionality zařízení.

8.12 RSU jednotka na SSZ musí být připravena pro připojení k BO C-ITS.

9. Požadavky zadavatele na servisní aplikace řadiče

9.1 Ke každému typu řadiče bude dodána aktuální servisní aplikace v počtu 3 přístupů (licencí) umožňující provádění všech potřebných pravidelných testů řadiče.

9.2 Servisní aplikace bude po připojení k řadiči ukazovat všechny potřebné informace. Jedná se zejména o podrobné informace o aktuálních poruchách k přesnému určení závady.

9.3 Veškeré informace poskytované servisní aplikací řadiče SSZ pracovníkům servisu musí být v českém nebo anglickém jazyce.

9.4 Význam hlášení má vycházet z běžně zaužívaných pojmů a zkratek. Ke stanovení významu hlášení nesmí být potřeba manuálu s převodem kódových (číselných) zpráv, zadavatel souhlasí s použitím textu bez diakritiky.

9.5 Tento SW dále umožní online vizualizaci signálního plánu obsahujícího:

- časovou osu
- číslo aktivního signálního plánu
- Tx
- číslo probíhající fáze, pokud je aktivní fázový signální plán
- číslo probíhajícího fázového přechodu, pokud je aktivní fázový signální plán
- stav všech signálních skupin
- jednoznačně graficky odlišenou oblast prodlužování u signálních skupin majících prodlužovací detektor (např. odlišným označením v pásu signální skupiny ve vazbě na číslo prodlužovacího kroku)
- stav všech připojených detektorů
- stav všech binárních vstupů
- přítomnost výzev preference RIS II

Okno pásového diagramu bude vybaveno posuvníkem pro snadné prohlížení průběhu signálního plánu a porovnávání změn v jednotlivých cyklech u dynamického řízení.

Online vizualizace pásového diagramu nesmí mít proti reálnému stavu křižovatky zpoždění větší než 2 vteřiny.

9.6 Servisní aplikace umožní základní ovládání řadiče v rozsahu:
- zapnutí dopravního řadiče
- vypnutí dopravního řadiče
- zapnutí dílčího uzlu dopravního řadiče
- vypnutí dílčího uzlu dopravního řadiče
- přepnutí signálního plánu v dopravním řadiči
- přepnutí řadiče do místního řízení
- simulaci všech připojených detektorů (včetně všech virtuálních detektorů např. MHD, IZS), formou cyklického obsazení, jednorázového a trvalého obsazení nebo neobsazeného stavu - současně musí být umožněna simulace libovolného počtu detektorů s různým nastavením simulace, a to i všech zároveň
- zapnutí dopravně závislého řízení
  - zapnutí dopravně závislého řízení IAD
  - zapnutí preference MHD
- vypnutí dopravně závislého řízení
  - vypnutí dopravně závislého řízení IAD
  - vypnutí preference MHD

9.7 Dodané SW vybavení musí umožňovat stažení, úpravu a nahrání konfigurace popsané v bodech 5.4 – 5.26.

9.8 Zavedení nových, tedy i dopravně závislých signálních plánů nebo úpravy dopravního řešení (dopravně závislého řízení), musí proběhnout za provozu, bez nutnosti vypnutí SSZ tedy i přímo z hlavní dopravní ústředny.

9.9 Servisní aplikace musí umožňovat stažení archívů popsaných v bodě 5.25 a jejich zobrazení v uživatelsky přívětivé podobě (informace nesmí být formou číselných kódů, ale musí být srozumitelná s jednoznačnými zaužívanými texty, obsahujícími příslušné údaje).

9.10 Export archivů ve srozumitelné podobě do některého z běžně využívaných formátů (například PDF, XLSX nebo CSV)

9.11 Dodané SW vybavení umožní export dopravních intenzit ze všech do řadiče připojených detektorů. Načtené dopravní intenzity ze všech do řadiče připojených detektorů (výstup ve formátu zpracovatelném programem Excel) musí být v jednotlivých časových úsecích (minimálně v 5, 15 a 60 minutových intervalech) musí být stále stejné, jejich součet vytvoří celou hodinu a musí začínat vždy v celou hodinu.

9.12 Dodané SW vybavení umožní export konfiguračního souboru .xml definovaného protokolem OCIT® (zadavatel preferuje nejnovější verzi OCIT-O, momentálně disponuje verzi V2.0 tohoto otevřeného protokolu), obsahujícího údaje potřebné pro připojení křižovatky k ústředně kompatibilní s tímto protokolem, včetně následného ovládání a provádění změn (viz bod 10.13).

10. Požadavky zadavatele na připojení řadiče k nadřazené DÚ SSZ

10.1 Zadavatel požaduje využití přenosových cest pro připojení řadiče SSZ k pracovišti CTD na adrese Renneská tř. 1a, 639 00 Brno - Štýřice dle projektové dokumentace (optický kabel, metalický kabel nebo LTE). Dle vyprojektované varianty dále zadavatel požaduje pro:

1. Optický kabel OD MMB
   - použití datového switche v průmyslovém provedení s osmi metalickými a dvěma optickými porty pro případné připojení dohledových kamer
   - zařízení musí umožňovat splnění všech zákonných požadavků a vnitřních směrnic zadavatele na IT systémy (viz. Přílohy)
2. Metalický kabel OD MMB
   - připojení řadiče napřímo k dopravní ústředně jedním komunikačním párem
   - další pár může být použit pouze pro potřeby určené zadavatelem např. telefon
3. Mobilní sítě
   - SIM kartu pro připojení křižovatky dodá zadavatel
   - SIM karta bude využívat datových služeb mobilních sítí třetí nebo vyšší generace

10.2 Zadavatel požaduje, aby u běžných operátorských zásahů, jako je zapnutí a vypnutí křižovatky nebo jejího uzlu, přepnutí signálního plánu, spuštění vizualizace signálního plánu atd., z dopravní ústředny nebyl mezi těmito technologiemi rozdíl.

10.3 Všechny nově budované/rekonstruované SSZ musí být přímo připojeny k dopravní ústředně zadavatele otevřeným komunikačním protokolem určeným pro systémy centrálního řízení dopravy na pozemních komunikacích pomocí SSZ schváleného k nasazení v zemích evropské unie. Zadavatel požaduje použití nejnovější verze otevřeného komunikačního protokolu.

10.4 Zadavatel požaduje, aby řadič komunikoval s DÚ pomocí sítě Ethernet (např. využitím profilu 3 protokolu OCIT-O) a to v plném rozsahu funkcionalit pro protokol OCIT-O V2.0.

10.5 Řadič bude vybaven standardním konektorem RJ45 pro připojení k DÚ a pro připojení k RSU.

10.6 Řadiče musí být trvale spojeny s dopravní ústřednou SSZ (Scala) a umožňovat průběžnou kontrolu komunikace ze strany ústředny.

10.7 Všechny řadičem detekované poruchy budou odesílány na ústřednu.

10.8 Otevření i zavření dveří bude odesíláno na ústřednu SSZ.

10.9 Změna režimu stmívání návěstidel bude odesílána na ústřednu SSZ.

10.10 Řadič musí umožňovat automatickou synchronizaci času s NTP serverem ústředny, tento čas bude mít v systému vyšší prioritu než přijímač času v řadiči.

10.11 Řadič musí reagovat na požadavky ústředny v rámci 1 sec od obdržení požadavku. Okamžité změně režimu řízení brání bezpečností požadavky a prioritní zásah do řízení.

10.12 Řadič musí komunikovat s DÚ zadavatele otevřeným protokolem nejnovější dostupné verze (DÚ zadavatele disponuje protokolem OCIT-O V2.0) ve smyslu následujících požadavků DÚ:

- Požadavek ústředny na zjištění stavu řadiče obsahující:
  - časovou značku poslední změny
  - chybové stavy (viz bod 5.6)
  - stav SSZ
  - řídící úroveň (např. místní rozvrh, ruční řízení, centrální řízení nebo trasa IZS)
  - číslo aktivního signálního plánu
  - stav dílčích uzlů křižovatky
- zapnutí dopravního řadiče
- vypnutí dopravního řadiče
- zapnutí dílčího uzlu dopravního řadiče
- vypnutí dílčího uzlu dopravního řadiče
- přepnutí signálního plánu v dopravním řadiči
- přepnutí řadiče do místního řízení
- zapnutí dopravně závislého řízení
  - zapnutí dopravně závislého řízení IAD
  - zapnutí preference MHD
- vypnutí dopravně závislého řízení
  - vypnutí dopravně závislého řízení IAD
  - vypnutí preference MHD
- stav režimu stmívání
- požadavek na přenos dat potřebných pro vytvoření pásového diagramu
  - číslo aktivního signálního plánu
  - Tx
  - číslo probíhající fáze, pokud je spuštěn fázový signální plán
  - číslo probíhajícího fázového přechodu, pokud je spuštěn fázový signální plán
  - stav všech signálních skupin včetně informací o prodlužování
  - stav všech připojených detektorů
  - stav všech binárních vstupů
  - přítomnost výzev preference RIS II
- stažení dat ze všech dostupných archivů řadiče
- spuštění VIP trasy na uživatelsky zadanou dobu

Tyto požadavky bude možno zadat s časem začátku a ukončení příkazu nebo okamžitě „do uvolnění“.

10.13 Řadič musí umožňovat stažení, úpravu a nahrání konfigurace popsané v bodech 5.12, 5.17 až 5.24 z dopravní ústředny.

11. Kontrola SSZ, technická přejímka, zkušební provoz a předání díla zadavateli

11.1 Technickou přejímku provádí zadavatel a slouží ke kontrole kompletnosti a kvality technických částí díla a jeho základních funkcí. Úspěšný průběh technické přejímky je podmínkou pro uvedení díla do zkušebního provozu.

11.2 Zhotovitel požádá provozního dopravního inženýra CTD BKOM o kontrolu SSZ a vyhotovení protokolu pro připojení řadiče k DÚ dle přílohy 14.8. Protokol o připojení dopravního řadiče k dopravní ústředně SSZ bude vyhotoven provozním dopravním inženýrem do 10 pracovních dní. Pokud zhotovitel požádá o kontrolu více SSZ současně, lhůta pro kontrolu se prodlužuje na násobek odpovídající počtu kontrolovaných SSZ. Po ukončení kontroly SSZ bude zhotovitel prostřednictvím elektronické komunikace informován o jejím výsledku a případných nalezených nedostatcích. Dle závažnosti nalezených nedostatků, může být vyhotoven vyhovující protokol o připojení dopravního řadiče k dopravní ústředně SSZ s poznámkami o nedostatcích. V tomto případě musí být zjištěné nedostatky odstraněny do 10 pracovních dní od vytvoření protokolu, v odůvodněných případech v jiném domluveném termínu. V případě závažných nedostatků bude vyhotoven nevyhovující protokol, po odstranění závad musí zhotovitel požádat o novou technickou přejímku. O závažnosti nedostatků rozhodují odpovědní zástupci CTD, provozního úseku a ÚDI BKOM.

11.3 Zhotovitel musí pro kontrolu SSZ na výzvu dopravního inženýra CTD poskytnout součinnost specialisty dodávané technologie při místním šetření. Tato součinnost musí proběhnout nejpozději do tří pracovních dnů v čase od 8:00 do 14:00. Při místním šetření musí být možné spustit vizualizaci signálního plánu včetně detektorů, přepínat jednotlivé signální plány a simulovat libovolnou kombinaci obsazenosti či neobsazenosti detektorů včetně preference MHD a IZS za účelem vyzkoušení plného rozsahu logiky dynamického řízení.

11.4 K provedení přejímky díla vyzve zhotovitel investora min. 3 pracovní dny předem.

11.5 Základními částmi technické přejímky jsou:

- předložení vyhovujícího protokolu o připojení dopravního řadiče k dopravní ústředně SSZ (Scala) dle přílohy 14.8, potvrzený odpovědným zástupcem CTD, provozního úseku a ÚDI BKOM
- kontrola kompletnosti díla
- předání a převzetí kompletního stanoveného trvalého DZ
- kontrola splnění technické specifikace zadavatele
- předání dokladů o provedení bezpečnostních testů dopravního řadiče
- předání potvrzené dokumentace dopravního řešení nahraného v dopravním řadiči ve 3 vyhotoveních a elektronicky ve formátu neumožňujícím změny (například .pdf)
- zapnutí dopravního řadiče a provedení vizuální a protokolární kontroly jeho hlavních funkcí, správného zapojení a funkce připojených zařízení (detektorů, návěstidel apod.) dopravním inženýrem zadavatele

11.6 Po dobu zkušebního provozu zůstává dílo v majetku zhotovitele.

11.7 Po dobu zkušebního provozu bude dílo plně využíváno budoucím správcem (BKOM), přičemž tento nesmí žádným způsobem zasahovat do HW a SW řadiče bez vědomí zhotovitele.

11.8 Po dobu zkušebního provozu musí zhotovitel veškeré zásahy do předmětného zařízení dohodnout s budoucím správcem (BKOM).

11.9 Během realizace, zkušebního provozu a záruční doby má zadavatel právo požadovat doladění dle předlohy změnového DŘ (viz kapitola 12).

11.10 Po splnění výše uvedených podmínek lze zahájit protokolární převzetí díla do majetku zadavatele které se skládá z:

- předání dokumentace skutečného provedení stavby ve 3 vyhotoveních a elektronicky ve formátu neumožňujícím změny (například .pdf).
- předání dokladů platné revize elektrického zařízení
- předání potvrzení o shodě el. zařízení
- předání dokladů o ekologické likvidaci vytěženého materiálu a zařízení
- předání protokolu o předání stavbou dotčených povrchů do správy správního úseku BKOM
- podpisu protokolu o předání a převzetí díla

11.11 Protokol o předání a převzetí díla podepsaný zadavatelem opravňuje zhotovitele k provedení fakturace. Od této chvíle nesmí zhotovitel zasahovat do HW a SW řadiče, ani stahovat data bez souhlasu zadavatele nebo správce SSZ (BKOM).

12. Doladění

12.1 Doladění je úprava SW části řadiče pro řízení provozu, vyžádána zadavatelem. Tyto úpravy zahrnují např.: změny signálních plánů, schématu fází, fázových přechodů, mezičasů, logiky řízení, nastavení veškerých parametrů atp., obsažených v DŘ sestaveného v souladu s přílohou 14.9. Nejedná se tedy o změny v HW části díla.

12.2 Jedno doladění může obsahovat libovolnou kombinaci a počet změn obsažených v předaném změnovém DŘ.

12.3 Může být požadováno celkem až 10 doladění DŘ v průběhu realizace, zkušebního provozu a záruční doby díla.

12.4 Na realizaci doladění má zhotovitel max. 10 pracovních dnů od dodání změnového DŘ zadavatelem, nebude-li se zadavatelem dohodnuto jinak (pro každé změnové DŘ).

12.5 Pro každé doladění bude zažádáno o novou kontrolu SSZ a technickou přejímku dle kapitoly 10.

12.6 Zhotovitel je povinen zajistit spolupráci specialisty provádějícího doladění s dopravním inženýrem zadavatele.

13. Další požadavky zadavatele pro realizaci a předání díla

13.1 Zhotovitel dodá zadavateli výsledný podklad pro MAPEM a SPATEM zprávy, které budou vycházet z topologického podkladu křižovatky vč. VDZ, SDZ a SSZ. Podklad bude zpracovaný dle nejaktuálnější verze dokumentu „Požadavky na automobilový průmysl pro SPaT a MAP“ viz https://bit.ly/2XICTlv .

13.2 Sloupy SSZ musí být oboustranně pozinkované.

13.3 Sloupy SSZ budou opatřeny ochranným nátěrem do výšky 60 cm nad okolní terén.

13.4 Všechny použité stávající kabelové prostupy pod vozovkou musí být v souladu s projektem před položením kabeláže SSZ vyčištěny tlakovou vodou a následně zakonzervovány.

13.5 Přesný termín vypnutí opravovaného SSZ musí být dohodnut mezi zhotovitelem, zadavatelem, servisem SSZ a PČR z důvodu zabránění vzniku časové kolize s jinou akcí SMB.

13.6 Regulační a aktivační práce na řadiči SSZ mohou být prováděny pouze firmami autorizovanými výrobcem řadiče k provádění těchto prací. Uchazeč na realizaci veřejné zakázky musí prostřednictvím své nabídky písemně doložit, že má tuto součinnost autorizované firmy zajištěnu.

13.7 Veškeré výrobky obsažené v dodávce musí odpovídat platné legislativě.

13.8 Dotčená zeleň musí být obnovena náhradní výsadbou.

13.9 Veškeré náklady na přechodné dopravní značení vyvolané stavbou budou zajišťovány zhotovitelem (viz soupis prací -> oddíl VRN -> položka „Dopravní značení na staveništi“).

13.10 Realizace díla musí obsahovat realizaci trvalého dopravního značení, které odpovídá projektové dokumentaci a platnému stanovení užití.

13.11 Vodorovné dopravní značení, dotčené výstavbou SSZ, bude provedeno strukturálním plastem v souladu s TP 133 – Zásady pro vodorovné dopravní značení na pozemních komunikacích. Pokud nové povrchy v době realizace stavby neumožňují okamžitou pokládku vodorovného dopravního značení strukturálním plastem, bude zhotoveno dočasné vodorovné dopravní značení barvou, které bude po vyzrání povrchu nahrazeno vodorovným dopravním značením strukturálním plastem.

13.12 Svislé dopravní značení musí odpovídat PD, sloupky dopravního značení musí být v pozinkované úpravě, přičemž třída použité reflexní fólie pro svislé dopravní značení bude vycházet z platné legislativy.

13.13 V případě že zemní práce budou prováděny v chodnících a vozovkách, na které se vztahuje záruční lhůta jiného zhotovitele, musí být zpětná úprava tohoto povrchu ze záručních důvodů objednána jako subdodávka u tohoto zhotovitele.

13.14 Geodetická dokumentace skutečného provedení stavby bude zhotovitelem předána v souladu s předpisem pro vyhotovení geodetické dokumentace skutečného provedení staveb (Mp-SÚ3200-01 viz Příloha 14.7) ve dvou vyhotoveních investičnímu odboru MMB a v jednom vyhotovení geodetické skupině BKOM pro potřeby GIS (viz soupis prací -> oddíl VRN -> položka „Geodetické práce po výstavbě“).

13.15 Na základě geodetického zaměření stavby zhotovitel vyhotoví geometrický plán pro vyznačení věcného břemene v 6 vyhotoveních ke všem dotčeným pozemkům, které nejsou ve vlastnictví SMB. Rozsah věcného břemene musí být předem konzultován se zadavatelem (viz soupis prací -> oddíl VRN -> položka „Geodetické práce po výstavbě“).

13.16 Všechny dotčené povrchy budou po dokončení díla předány zpět do správy sektoráři BKOM.

13.17 Veškerý vytěžený materiál ze SSZ bude odvezen a protokolárně předán zhotovitelem na adrese Brněnské komunikace a.s., Masná 7, Brno. V případě, že tento vytěžený materiál bude Brněnskými komunikacemi a.s. odmítnut, musí zhotovitel zajistit jeho ekologickou likvidaci zákonným způsobem a o jejím provedení předat zadavateli při předání a převzetí díla prokazující doklad.

13.18 Při pracích v blízkosti kolejí MHD (blíže než 1m a při budování kabelových prostupů pomocí protlaků) musí být před a po provedení prací provedeno geodetické zaměření kolejí. Při provádění prací nesmí dojít ke změně nivelety kolejí.

13.19 Nabídková cena musí obsahovat nutné zaškolení obsluhy budoucího správce SSZ (BKOM) v plném rozsahu pro práci s dodanými HW a SW prostředky minimálně v následujícím rozsahu:

- 10 pracovníků na uživatelské úrovni servisní technik, včetně zaškolení pro profylaktické prohlídky,
- 4 pracovníci na uživatelské úrovni dopravní inženýr, která umožní provádění změny v nastavení SSZ (např. automatika pro přepínání SP-ů, vytváření a úpravy pevných a dynamických SP-ů atp.).

14.Přílohy

14.1 Komunikační protokol pro komunikaci vozidel MHD s RSU jednotkami na SSZ
14.2 SmGŘ – 039 – Bezpečnostní politika informací
14.3 SmGŘ – 042 – Bezpečné chování uživatele
14.4 SmGŘ – 044 – Směrnice pro správu a uživatele CTD
14.5 SmGŘ – 046 – Organizace kybernetické bezpečnosti
14.6 SmGŘ – 061 – Řízení dodavatelů
14.7 Mp-SÚ3200-01 - Předpis pro vyhotovení geodetické dokumentace skutečného provedení staveb
14.8 Vzor protokolu o připojení dopravního řadiče k dopravní ústředně SSZ
14.9 Obsah DŘ
14.10 Vzor pásového diagramu pro on-line vizualizaci

Preference vozidel MHD přes V2X protokol

(návrh standardu protokolu)

„Technický popis – V1.03“

Dodavatel/výrobce	**Ing. Ivo Herman, CSc., Na Vyhlídce 559/8, 66448 Moravany**			Verze: V2X101_190731
Založení dokumentu	Ing. Ivo Herman, PhD.	Datum	28. 05. 2019	
Opravil	Ing. Ivo Herman, PhD.	Datum	31. 07. 2019	
Dokument: Preference vozidel MHD přes V2X protokol				
Část: Technický popis V_1.03				

OBSAH

Revize dokumentu:

1.01 – 30.5.2019 – výchozí verze dokumentu
1.02 - 24.6.2019 – formální úpravy dokumentu

1.03 – 31. 7. 2019 – přesunuta sekce CAM zpráv, přidány odkazy na normy, upravena struktura PTActivation v CAM

1. ÚVOD

1.1. ÚČEL DOKUMENTU

Tento dokument představuje návrh způsobu realizace obecné preference vozidel MHD v situaci, kdy komunikace bude probíhat přes protokoly V2X systému (neboli přes C-ITS systémy).

Dokument má za cíl obecně definovat způsob komunikace mezi vozidly vybavených jednotkami OBU (On Board Unit) a jednotkami u řadičů křižovatek RSU (Road-Size Unit). Cílem je zejména definovat komunikační diagram pro přidělení preference, tj. kdy vozidlové stanice blížící se a projíždějící křižovatkou pošlou požadavek a přijmou odpověď o možnosti přidělení preference.

Dokument vychází z dokumentu: **C-ROADS CZ PTP 1.52** (dále jen „Dokument C-ROADS“) tak, jak byl schálen na Řídicím výboru konsorcia C-ROADS CZ.

Nově definovaný systém preferencí má takové vlastnosti, aby umožnil hladké nasazení do provozu a současně zahrnoval všechny dosavadní zkušenosti s komunikací vozidlo – řadič křižovatky:

1) Pro jednodušší aplikace zajišťuje nahrazení stávající radiové cesty vozidlo-řadič řešením pomocí V2X protokolu. Např. pro DPMB a.s. umožnit nahrazení stávající technologie v pásmu 960 MHz (radiové modemy Racom MR900) technologií V2X. Při této výměně je třeba vzít v potaz fakt, že nový systém V2X musí po určitou dobu fungovat i se starými řadiči, v nichž již není možné upravit software (řadiče křižovatek jsou zastaralého typu). Proto u starých řadičů zůstává stejný způsob komunikace mezi **řadičem a RSU jednotkou** (dříve radiovým modemem).
2) Současně návrh umožňuje využít potenciálu moderních komunikací, který V2X nabízí, a to buď ihned, nebo v budoucnu, aniž by bylo třeba zasahovat do způsobu komunikace, tj. měnit a upravovat tento návrh standardu (přenosového protokolu). Jinými slovy, níže uvedený návrh standardu je vytvořen tak, aby respektovat doposud nám známé situace pro řízení preferencí s tím, že například nové řadiče mohou využít výrazně častější informace o poloze vozu z V2X k přesnějšímu rozhodnutí o přidělení preference, možnosti zpracování velikosti vozidla a dalších informací.

Dokument je psán tak, aby se mohl stát standardem v rámci ČR a byl v souladu z dokumenty C-ROADS a tím, by se dal použít i v dalších městech či krajích, která také uvažují o přechodu na technologii V2X.

1.2. TERMINOLOGIE

Pro účely zpracování servisního návodu a významu jednotlivých pojmů jsou následně uvedeny popisy jednotlivých pojmů.

Termín	Význam
C-ROADS	Projekt o zavádění V2X technologie v ČR
CAM	(Cooperative Avareness Message) – základní zpráva o stavu vozu
EPIS 4.0C3	Palubního počítače EPIS použitý v DPMB a.s.
EPCOMP	Software pro přípravu dat pro palubní počítače (provozní i konfigurační)
GLONASS	Globální navigační systém Ruska
GNSS	Globální navigační satelitní systém pro určení polohy. Obecný název navigačního systému, který může být realizován pomocí GPS, Galileo či systému Glonass
GPS	Global position system – systém pro určení polohy vozidla dle amerického standardu
ID	Identifikátor prvku (obvykle číselný znak)
ITS	Inteligentní dopravní systémy
OBU	On-board unit – palubní jednotka s V2X
PP	Palubní počítač – v tomto případě sestava EPIS 4.0C3
palubní systém	Palubní počítač s terminálem a periferie nutné pro komunikaci s dispečerským systémem a okolím vozidla vč. napájecí jednotky a hlásiče
RS 485	Komunikační standard sběrnice založené na symetrickém vedení
RSU	Road size unit – stacionární jednotka s V2X pro dopravní infrastrukturu
SRM	Signal Request Message – zpráva pro požadavek na preferenci z vozu,
SSM	Signal Status Message - zpráva pro odpověď od řadiče/RSU
V2X	Vehicle-to-evertyhing communication

2. ZPŮSOB DNEŠNÍ PREFERENCE MHD

2.1. POSLOUPNOST STAVŮ DNEŠNÍHO ŘÍZENÍ PREFERENCÍ

Dnešní stavu používání preference vozidel MHD má následující klíčové vlastnosti:

1) Vozidlo MHD samo aktivně vysílá požadavek na přidělení preference.
2) Tento požadavek na preferenci vysílá vozidlo MHD v předem definovaných geografických bodech (tzv. přihlašovacích či odhlašovacích oblastech), nebo při definované změně stavu vozidla (vůz zastavil v zastávce, odjel ze zastávky, zavřel dveře, apod…).
3) Vozidlo MHD se může postupně hlásit z více geografických bodů (zpřesňovat polohu), případně i jinak aktualizovat svůj stav.
4) Požadavek na preferenci vzniká ve vozidle MHD nejčastěji v palubním počítači a radiový modem na vozidle jej jen přenáší radiovou cestou k řadiči.
5) Požadavek ve vozidle (palubním počítači) vzniká na základě uložených dat a to ve vztahu k „jízdě“ vozidla (pokyny k chování).
6) Řidič vozidla může manuálně žádat o přidělení preference na křižovatce či při výjezdu z „bočního“ směru (volba např. přes palubní počítač).
7) Každý požadavek vyslaný z vozidla MHD je minimálně potvrzen radiovým modemem řadiče (v ČR neplatí u všech preferencí v rámci DP) a tato odpověď je zobrazena řidiči na displeji. Zobrazení je nutné zejména tam, kde systém preference ovlivňuje řadič tak, že tento musí zařadit individuální větev řízení.
8) Vozidlo může žádat o preferenci MHD současně na více křižovatkách.
9) Rozhodnutí, jestli a jak bude udělena preference, je plně v kompetenci řadiče a řidič se o stavu zpracování nedozví.
10) K ukončení žádosti o preferenci slouží odhlašovací zpráva, která je vysílána buď v dané geografické oblasti, nebo při určité změně stavu vozu (odjezd ze zastávky za křižovatkou).

Konfigurace chování vozu se děje na straně provozovatele vozů, tedy dopravních podniků a to v tomuto účelu vytvořeném programu. Konfigurují se zejména:

A) Geografické oblasti pro přihlášení/odhlášení.
B) Vjezdové a výjezdové rameno křižovatky.
C) Sekvence přihlašovacích a odhlašovacích požadavků (více přihlašovacích oblastí, reakce na zastavení v zastávce, opuštění křižovatky).

2.2. PŘENÁŠENÉ INFORMACE Z VOZIDLA

Vozidlo MHD o sobě v datovém paketu, který se přenáší na křižovatku, sděluje informace uvedené v následující **Tabulka 1**.

Tabulka 1 - Přenášené informace v požadavku na preferenci

Položka	Akce
Typ telegramu (typ paketu)	Paket sděluje typ požadavku a svůj stav – podrobnosti viz Tabulka 2.
Číslo křižovatky *)	Číslo křižovatky, na níž je požadována preference.
Číslo příjezdové větve	Číslo větve křižovatky, jíž vůz do křižovatky vjede.
Číslo odjezdové větve	Číslo větve křižovatky, jíž vůz z křižovatky vyjede.
Číslo linky	Číslo linky, na které vůz, jenž žádá o preferenci, aktuálně jede.
Číslo cíle	Číslo cíle, na který vůz, jenž žádá o preferenci, aktuálně jede.
Číslo vozu	Číslo vozu, který žádá o preferenci
Typ vozu	Typ vozu. Na výběr z: tramvaj, trolejbus, autobus
Odchylka od jízdního řádu	Aktuální zpoždění/předjetí vozu.

**) např. číslování je dle Brněnských komunikací (pro 2.06 se odešle 206)*

Typ telegramu do řadiče dává přesnější informace o konkrétní události v oblasti křižovatky, tedy o pohybu či stavu vozidla MHD. Specifikované typy telegramu jsou v **Tabulka 2** (převzata z popisu chování preferenci v městě Brně).

Tabulka 2 - Typy zpráv ve stávajícím systému

Událost	Kód typu paketu (hexadecimálně)
1=průjezd přihlašovacím místem	0H, 10H, 20H, 30H
2=odjezd ze zastávky před křižovatkou	1H
3=první zavření dveří v zastávce před křižovatkou	2H
4=neprvní zavření dveří v zastávce před křižovatkou	3H
5=příjezd do zastávky (za ní následuje křižovatka)	4H
6=průjezd odhlašovacím místem	80H
7=příjezd do zastávky těsně za křižovatkou (pokud nebyl rozeznán průjezd odhlašovacím místem)	84H
8=odjezd ze zastávky za křižovatkou	89H
9=stisk tlačítka šipek na PP v režimu linka/cíl v tramvaji (nouzový paket)	40H
10=testovací paket, neovlivňuje řadič (ten ale posílá odpověď)	C0H

2.3. PŘECHODOVÝ STAV MEZI SYSTÉMY

Vozidlo MHD v rámci přechodného stavu mezi systémy vysílá požadavek na preferenci následujícími způsoby:

- Přes V2X formou zpráv CAM.
- Přes původní radiový modem pro zpětnou kompatibilitu.

Tento dokument se zabývá pouze použitím V2X, ostatní způsoby neřeší. Přepnutí mezi systémy je možné až tehdy, pokud bude možno zajistit preferenci v provozu.

3. SYSTÉM ZALOŽENÝ NA V2X

3.1. POŽADAVKY NA NOVÝ SYSTÉM

Navrhovaný standard musí být schopen vykonávat všechny dnes známé případy preferencí a musí umožnit jejich rozšíření. Další jeho vlastností je, že musí být schopen transformovat nové požadavky do původního řešení v případech, kdy na křižovatce je použit řadič, který není schopen níže popsaného řízení (tento starší řadič, v němž již není možné změnit software a zajistit tak podporu V2X).

Pro minimalizaci změn v systému nový standard zachovat i to, že veškerá konfigurace probíhá na **straně provozovatele vozů s tím,** že je to vůz, kdo aktivně informuje řadič o svém stavu. Zároveň ale rozhodnutí o preferenci musí zůstat na řadiči křižovatky, případně mezi řadičem a RSU. Tím se minimalizují náklady na straně provozovatele jak vozů, tak SSZ. Systém tedy bude fungovat podobně, jako nyní, jen se změní „radiová cesta“ informace mezi vozem a řadičem SSZ

3.2. NAVRHOVANÝ STANDARD SE SYSTÉMEM V2X

Podmínkou použití nového standardu je, že všechny vozidla MHD jsou již vybaveny komunikační jednotkou, která podporuje V2X a používá evropské standardy (platí např. pro DPMB, a.s.). Jak bylo uvedeno výše, komunikační jednotka na vozidle MHD, která podporuje V2X, se označuje jako OBU (v DPMB a.s. jsou použity typy UCU 5.0V-2L2WVG a UCU 5.0V-VG).

Stejně tak řízení křižovatek musí být doplněno jednotkami **RSU** (Road-Side Unit) (v DPMB/B-KOM jsou použity typy s názvem UCU 5.0I-LVG). Tato jednotka RSU pak komunikuje s řadičem SSZ **(interně definovaným protokolem RSU – řadič, který není součástí návrhu tohoto standardu)** a přes protokol V2X s vozidly MHD (**je popsána v tomto standardu**).

3.2.1. POUŽITÉ ZPRÁVY V2X

Pro návrh standardu preferencí vozidel MHD jsou využity jen standardizované zprávy pro protokolu V2X. V souladu s Dokumentem C-ROADS jsou navrženy pro použití následující zprávy:

- **SRM** (Signal Request Message) pro požadavek na preferenci z vozu,
- **SSM** (Signal Status Message) pro odpověď od řadiče/RSU.

SRM tedy slouží pro odeslání požadavku na preferenci (případně aktualizaci požadavku), zatímco SSM slouží pro odpověď z řadiče na tento požadavek. Obě zprávy jsou adresné – je v nich uvedeno, pro jakou stanici jsou uvedeny. SRM má tedy v sobě **číslo křižovatky**, na niž směřuje požadavek na preferenci. Naproti tomu **SSM má v sobě číslo vozu**, kterému je odpověď určena.

SRM a SSM zprávy jsou definovány ve standardu ETSI TS 103 301, který se odkazuje na standard ISO TS 19091, který pak využívá datových struktur z normy SAE J2735 (profil C). Použití jednotlivých kontejnerů ve zprávě je blíže upraveno v normě C-Roads „C-ITS Infrastructure Functions and Specifications“ a dále v českém profilu C-ROADS CZ PTP 1.52.

Na každý požadavek či aktualizaci požadavku z vozidla MHD přes zprávu SRM musí RSU odpovědět zprávou či aktualizací zprávy SSM. Zpráva SSM se může průběžně aktualizovat i bez aktualizace požadavku, například na základě dat z řadiče (požadavek přijat, případně preference udělena).

V Dokumentu C-Roads je ještě zmíněna realizace preference přes zprávy typu CAM. Ačkoliv se preference přes CAM zprávy již v DPMB používá (v souladu s předchozí verzí Dokumentu C-ROADS), ukázala se jako nepříliš vhodná, protože vozidlo MHD může nyní vysílat požadavek na více křižovatek současně, ale zpráva typu CAM nemá konkrétního adresáta (neumožňuje zadat komunikaci s příslušným řadičem). Navíc chybí zpětný kanál pro doručení potvrzení o přijetí požadavku řadičem SSZ. Proto návrh standardu preference vozidel MHD využívající kombinaci zpráv typu SRM a SSM se tak jeví mnohem

vhodnější.

Struktura zpráv typu SRM a SSM je volena tak, aby umožnila přenést veškerá data, která se dnes přenáší do řadiče (respektuje např. i tzv. „staničení“. Pro starší řadiče pak provede RSU „rekonstrukci“ a sestaví paket, který se dnes přenáší do řadiče po sběrnici RS-232 nebo RS 485.

Jak bylo uvedeno výše, v řadičích křižovatek může být protokol mezi RSU a řadičem jiný a závislý na možnostech a schopnostech řadiče – není součástí tohoto dokumentu, protože není možno předjímat zvyklosti protokolů a vlastní požadavky výrobců řadičů.

3.2.2. ZPŮSOB KOMUNIKACE PRO PREFERENCI MHD

Požadavky na preference vozidel MHD bude jednotka OBU (=V2X jednotka na vozidle) vysílat na základě pokynu z palubního počítače. Palubní počítač bude generovat tyto pokyny na základě **stejné** logiky a **stejných konfiguračních dat**, jako je dělá dnes. Na základě pokynu z palubního počítače OBU (=V2X jednotka na vozidle) sestaví zprávu SRM a tuto zprávu odvysílá přes jednotku V2X. RSU jednotka zprávu přijme a sestaví paket pro řadič a odešle jej dle protokolu, kterým komunikuje s řadičem. Řadič potvrdí přijetí a jednotka RSU odvysílá přes V2X odpověď zprávou SSM.

Přesný popis je uveden v kapitole 3.2.3.

3.2.3. JEDNOTLIVÉ KROKY PŘI PREFERENCI SYSTÉMEM V2X

Celá komunikace pro řízení preferencí vozidel MHD bude probíhat následovně:

1) Palubní počítač ve vozidle MHD vyhodnotí dle polohy GNSS (v DPMB GPS + GLONASS) nutnost vytvořit požadavek na preferenci. K tomu využije svá konfigurační data zadávané v příslušném programu (např. v DPMB je to EPCOMP). Požadavek může vzniknout například na základě pozice vozu v některé přihlašovací oblasti nebo na základě přítomnosti v zastávce, případně i na základě manuální aktivace řidičem vozu.
2) Palubní počítač předá veškerá data nutná pro preferenci vozidla do jednotky OBU. Data jsou alespoň ta, která jsou uvedená v **Tabulka 1**. Nezbytnými informacemi pro preferenci jsou i čísla vjezdové a výjezdové větve, číslo křižovatky a typ telegramu.
3) Jednotka OBU na základě dodaných dat sestaví zprávu SRM dle evropských standardů a standardů C-ROADS EU a CZ. V nich je uvedena zejména cílová křižovatka a vjezdová a výjezdová větev.
4) OBU zahájí vysílání preferenční zprávy SRM. Jednotka OBU pak vysílá zprávu SRM přes protokol V2X a periodicky ji opakuje, dokud nedostane odpověď od jednotky RSU z řadiče křižovatky.
5) Jednotka RSU přijme zprávu SRM od vozidla MHD. Vyhodnotí, jestli patří pro danou křižovatku dle adresních bitů a jestli se jedná o dosud nepřijatou zprávu (zpráva SRM je totiž vysílána periodicky).
6) Pokud zpráva je určena pro danou křižovatku a jedná se o novou zprávu, RSU sestaví data pro řadič SSZ. Zprávu pro řadič sestaví na základě určeného protokolu s řadičem křižovatky (specifikace není součástí této dokumentace). Určený protokol tak závisí na typu řadiče a může/je proprietární mezi řadičem a RSU.
7) Řadič potvrdí přijetí požadavku odesláním odpovědi do RSU, příp. může sdělit i stav zpracování žádosti o preferenci, je-li znám a pokud jej protokol podporuje.
8) Jednotka RSU na základě paketu z řadiče sestaví zprávy SSM dle evropských standardů a standardů C-ROADS EU a CZ. Jako příjemce uvede vůz, který o preferenci žádal.
9) Jednotka RSU odvysílá zprávu SSM a bude ji opakovat po určitou dobu.
10) OBU jednotka ve vozidle MHD přijme zprávu SSM a vyhodnotí, jestli je určena pro dané vozidlo a jestli se nejedná o opakování již přijaté zprávy (zpráva SSM se totiž vysílá periodicky).
11) Pokud je zpráva určena pro dané vozidlo a jedná se o nově přijatou zprávu, jednotka OBU ukončí vysílání zprávy SRM.
12) Následně jednotka OBU vytvoří zprávu pro palubní počítač (např. v DPMB EPIS 4.0C3), v níž bude odpověď od řadiče SSZ a případně i stav zpracování požadavku na preferenci.
13) Palubní počítač stejně jako nyní zobrazí výsledek požadavku na preferenci na LCD terminálu řidiče.

Uvedený popis se týká zatím jednoho požadavku a jedné odpovědi od řadiče SSZ. Pro správně fungující preferenci je navíc třeba provést či umožnit provést:

- Aktualizaci požadavku SRM při změně pozice nebo stavu vozidla. Celý postup uvedený výše se zopakuje, když palubní počítač vyhodnotí nutnost informovat řadič o změně svého stavu (pozice, přítomnost v zastávce, manuální aktivace). Jen místo nové SRM zprávy se bude vysílat aktualizovaná SMR zpráva a místo nové SSM zpráva se bude vysílat aktualizovaná SSM zpráva. Aktualizace stavu vozidla se přenese na základě změny typu telegramu. Ten musí být jiný než v předchozím požadavku na stejnou křižovatku.
- Pokud by změna stavu požadavku byla na „odhlášení“, kromě typu telegramu je třeba specifikovat, že zpráva SRM je zprávou ukončovací. Při přijetí ukončovací zprávy SRM jednotka RSU přestane vysílat zprávu SSM pro daný vůz.
- Řadič SSZ může měnit stav zpracování požadavku (například rozhodnout o přidělení preference).

Pak aktualizuje zprávu SSM i bez nového požadavku z vozu. Aktualizace se v DPMB zatím nepoužívá, vozidlo je informováno pouze o přijetí požadavku, ne o stavu jeho zpracování. Pokud by se použila, je možné informovat vozidlo i o jistotě udělení preference a vyzvat jej tak například k odjezdu ze zastávky s garantovanou zelenou („staničení“, používané například v DPO – v DPMB se nepoužívá).

3.3. MOŽNÁ ROZŠÍŘENÍ

Pro využití potenciálu V2X je možné rozšířit v budoucnu systém o:

1) Monitorování pozice vozu z CAM zpráv. Řadič SSZ tak bude mít dobré informace o poloze vozu a může ve správný moment přidělit preferenci.
2) Sdělení na vůz, že má garantovánu preferenci. Takto se řidič dozví, že bude mít v době průjezdu zelenou a například může ve správný moment vyjet ze zastávky.
3) Sdělení na vůz, že preference byla odmítnuta. Například kvůli průjezdu IZS.

Tato rozšíření nebudou vyžadovat zásadní úpravy v přenášených zprávách, pouze by mohly zajistit lepší fungování preference.

4. OBSAH JEDNOTLIVÝCH ZPRÁV

Jak bylo uvedeno, preference vozidel MHD je založena na vysílání dvou základních zpráv v rámci protokolů V2X a to zpráv:

a. SRM
b. SSM

Obsah jednotlivých zpráv je uveden níže.

Tato kapitola popisuje návrh obsahu zpráv SRM a SSM tak, aby tato zpráva umožnila realizaci preference vozidla MHD v plném rozsahu dle dnešních zkušeností. Nebudou zde popsány všechny položky ve zprávě, ale jen ty, u nichž je třeba přesněji určit, jak je použít. Seznam jednotlivých prvků a jejich částečné použití je v Dokumentu C-Roads

4.1. OBSAH ZPRÁVY SRM

Pokud potřebuje vozidlo vysílat více požadavků na různé křižovatky, použije v jedné SRM zprávě více prvků SignalRequestPackage (tedy SRM/requests/request), jeden pro každou z křižovatek.

Tabulka 3: Obsah zprávy SRM

Atribut	Použití
SRM/sequenceNumber	Konkrétní verze zprávy. Musí se zvýšit, pokud dojde ke změně dat ve zprávě.
SRM/requests/request/signalRequest/id	ID křižovatky, které je požadavek určen.
SRM/requests/request/ signalRequest/id/region	Nepoužívat, případně použít identifikátor
SRM/requests/request/ signalRequest/id/id	Vyplnit číslo křižovatky dle číslování provozovatele (např. v Brněnských komunikacích „206“ pro křižovatku „2.06“).
SRM/requests/request/ signalRequest/requestID	Typ telegramu dle tabulky Tabulka 2. Tímto způsobem je možné do řadiče doručit stav vozu, případně typ oblasti. Tuto informaci dostane OBU od palubního počítače. Ve shodě se standardem bude pro změnu požadavku vždy jiné RequestID, jen nebude číslováno sekvenčně.
SRM/requests/request/ signalRequest/requestType	priorityRequest pro první žádost na křižovatku, priorityRequestUpdate pro každou další žádost, priorityCancellation pro ukončení požadavku na preferenci (například při vjezdu do odhlašovací oblasti)
SRM/requests/request/ signalRequest/inboundLane/lane	Nepoužije se, použije se číslo větve (approachID)
SRM/requests/request/ signalRequest/inboundLane/approach	Číslo větve křižovatky, kterou vozidlo do křižovatky vjede. Tuto informaci dostane OBU od palubního počítače.
SRM/requests/request/ signalRequest/inboundLane/connection	Nepoužije se, použije se číslo větve (approachID)
SRM/requests/request/ signalRequest/outboundLane/lane	Nepoužije se, použije se číslo větve (approachID)
SRM/requests/request/ signalRequest/outboundLane/approach	Číslo větve křižovatky, kterou vozidlo z křižovatky vyjede. Tuto informaci dostane OBU od palubního počítače.
SRM/requests/request/ signalRequest/outboundLane/connection	Nepoužije se, použije se číslo větve (approachID)
SRM/requestor/id/stationID	StationID, které vozidlo aktuálně má. Nesmí se měnit během interakce s křižovatkou
SRM/requestor/id/type/role	Role vozidla, typicky bude publicTransport
SRM/requestor/id/type/subrole	Zde není uvedeno v normě žádná konkrétní implementace. V souladu s nizozemským profilem navrhujeme použití následovně: 0 = neznámá 1 = autobus 2 = tramvaj 3 = metro 4 = vlak 5 = modrý maják 11 = trolejbus
SRM/requestor/name	Textový řetězec čísla vozu
SRM/requestor/routeName	Textový řetězec, oddělený středníkem, který tvoří tyto údaje: Linka;cíl;kurz
SRM/requestor/transitSchedule	Odchylka od jízdního řádu.

4.2. OBSAH ZPRÁVY SSM

Pokud potřebuje RSU vysílat více odpovědí různým vozidlům, použije v jedné SSM zprávě více prvků sigStatus (tedy SSM/status/SignalStatus/sigStatus), jeden pro každé z vozidel s požadavkem na preferenci.

Tabulka 4: Obsah zprávy SSM

SSM/sequenceNumber	Konkrétní verze dat ve zprávě. Musí se zvýšit, pokud dojde ke změně dat.
SSM/status/SignalStatus/id	ID křižovatky, které je požadavek určen.
SSM/status/SignalStatus/id /region	Nepoužívat, případně použít identifikátor
SSM/status/SignalStatus/id/id	Vyplnit číslo křižovatky dle číslování provozovatele (např. u Brněnských komunikací „206“ pro křižovatku „2.06“).
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/	V tomto kontejneru budou odpovědi pro jednotlivá vozidla
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/requester	Informace o odesílateli a jeho požadavku. Slouží pro spárování požadavku a odpovědi na straně vozidla.
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/requester/id/stationId	StationID odesilatele požadavku (SRM/requestor/id/stationId)
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/requester/request	**requestID=typ telegramu odesilatele požadavku (SRM/requestor/requestID)**
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/requester/sequenceNumber	sequenceNumber z požadavku, na který se odpovídá (SRM/sequenceNumber)
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/requester/typeData/role	Role odesilatele požadavku (SRM/requestor/id/type/role)
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/requester/typeData/subrole	Typ odesilatele požadavku (SRM/requestor/id/type/subrole)
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/inboundOn/lane	Použije se číslo větve (approachID)
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/inboundOn/approach	**Číslo větve křižovatky, kterou vozidlo do křižovatky vjede. Tuto informaci převezme RSU z požadavku od vozu.**
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/inboundOn/connection	Použije se číslo větve (approachID)
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/outboundOn/lane	Použije se číslo větve (approachID)
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/outboundOn/approach	**Číslo větve křižovatky, kterou vozidlo do křižovatky vjede. Tuto informaci převezme RSU z požadavku od vozu.**
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/outboundOn/connection	Použije se číslo větve (approachID)
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/minute	Tento prvek je dle SAE volitelný, ale profil C-ROADS EU z něj dělá povinný. Dle SAE se sem má zopakovat údaj z požadavku, který je ale volitelný. Nastavit na invalid (527040)
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/minute	Tento prvek je dle SAE volitelný, ale profil C-ROADS EU z něj dělá povinný. Dle SAE se sem má zopakovat údaj z požadavku, který je ale volitelný. Nastavit na unavailable (65535)

SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/duration	Tento prvek je dle SAE volitelný, ale profil C-ROADS EU z něj dělá povinný. Dle SAE se sem má zopakovat údaj z požadavku, který je ale volitelný. Nastavit na unavailable (65535)
SSM/status/SignalStatus/sigStatus/ SignalStatusPackage/status	Stav zpracování požadavku z vozidla v řadiči SSZ/RSU. Může se v čase měnit nezávisle na změně požadavku z vozu. Použitelné hodnoty pro Brno jsou: **unknown** – lze použít situaci, pokud je potřeba informovat, že zprávu SRM přijalo RSU, ale požadavek ještě nebyl předán do řadiče SSZ. **requested** – použije se v situaci, kdy požadavek z vozu byl přijat řadičem SSZ, ale není známo, jak s požadavkem řadič naloží. **granted** – požadavek byl přijat a preference je právě aktivní. Může sloužit pro indikaci, že vůz má vyjet ze zastávky, protože projede na zelenou. **rejected** – odmítnutí, například z důvodu preference IZS Typický cyklus tedy může být: unknown (není třeba vysílat, pokud požadavek do řadiče dojde rychle), requested a následně případně granted. U starších řadičů budou z uvedených použity jen stavy unknown a requested, protože ostatní stavy řadič nesděluje. Další stavy, které povoluje norma, nebudou zatím v Brně použity (palubní počítač je nepodporuje). Pokud je ale budou podporovat řadiče, je možné je začít používat.

5. INFORMACE O STAVU VOZIDLA – OBSAH CAM

Použitím zpráv SRM a SSM pro preferenci se uvolnilo až 20 bajtů v CAM zprávě (PublicTransportActivation container), které navrhujeme použít pro informace o stavu vozidla pro interní potřeby dopravního podniku. **Tyto bajty tedy nebudou použity pro preferenci a RSU u řadiče křižovatky s nimi nemusí nijak pracovat.**

Takto definovaná zpráva se odesílá 1x za sekundu do okolí vozidla a může nést informaci o stavu vozidla – je uživatelsky definovaná (v tomto případě pro DP).

Návrh využití volných 20 bajtů pro vozidla MHD:

1. Typ zprávy - 1 bajt - hodnota 0 – neurčeno, 1 pro MHD, ostatní pro budoucí použití
   - typ trakce - ED, AD, TB, - 4 bity
2. Číslo vozu - 2 bajty - rozsah 0 - 65536 (příp. 2 bity rezerva – např. zácvik)
3. Číslo linky - 3 bajty - rozsah 0 – 16384 tis. (rozsah 6 čísel – možno linka/kurz)
4. Číslo spoje - 2 bajty - rozsah 0 – 65536
5. Zpoždění - 2 bajty - zpoždění v sekundách (+/- 32 tis. sekund)
6. Provozovatel - 2 bajty - DPMB, Kordis, Arriva,……. Dle označení platného v ČR
7. Stav vozidla - 1 bajt - **v návrhu**

8. Pokyny na trasu – 8 bajtů**?** - **v návrhu -** jednokolejka, výhybka,
   - označník, vozidlo, vozovna, testovací systém vozovny ……

Preference vozidel MHD se vysílá samostatně, a proto zde není uvedena – viz sekce 3 .

Ostatní stavy – jako např. rozměry vozidla, zrychlení, apod. jsou vysílány častěji a lze je použít k detekci možných kolizí vozidel, zejména tramvají.

Bezpečnostní politika informací

(SmGŘ-039)

4. vydání ze dne 26.01.2023 Účinnost ode dne 01.02.2023

Číslo revize	Čísla revidovaných stránek	Zaznamenal a zařadil Jméno	Datum	Podpis
1				
2				
3				
4				
5				

	Odborný garant	Formálně ověřil	Vydavatel	Schválil
Úsek	SŘ	GŘ	SŘ	GŘ
Funkce	Manažer kybernetické bezpečnosti	Správce řízené dokumentace	Předseda výboru pro řízení kybernetické bezpečnosti	Generální ředitel
Jméno	Ing. Igor Prosecký (I3 Consultants s.r.o.)	Ing. Pavel Burian	Ing. Roman Nekula, MBA	Ing. Luděk Borový
Datum	26.01.2023	26.01.2023	26.01.2023	26.01.2023
Podpis				

Obsah směrnice
(SmGŘ-039)

1. ÚVODNÍ USTANOVENÍ

1.1. Účel

Účelem dokumentu Bezpečnostní politika informací je stanovit cíle, princip, potřeby, rozsah a hranice Systému řízení bezpečnosti informací (dále také „SŘBI“) ve společnosti Brněnské komunikace a.s. a současně stanovit pravidla pro bezpečný provoz a správu informačních systémů provozovaných v SŘBI.
Pravidla stanovená tímto dokumentem obsahují postupy, které vycházejí z požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), navazující vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) a bezpečnosti informací, zejména dle ČSN EN ISO/IEC 27001.

1.2. Závaznost

Bezpečnostní politika informací je závazná pro všechny zaměstnance BKOM dnem jejího vydání. Zásady stanovené v této politice musí být prosazovány do realizace všech procesů, vykonávaných v BKOM. V případě přístupu extérních subjektů k aktivům BKOM, je extérní subjekt seznámen s relevantními pravidly této politiky, k jejíchž dodržování je zavázán zapracováním vybraných pravidel do smlouvy.

1.3. Správa normy

1.3.1. Sběr připomínek a případné změnové řízení zajišťuje odborný garant ON.
1.3.2. Výklad této normy zajišťuje odborný garant.
1.3.3. Metodickou kontrolu dodržování pravidel a zásad této normy zajišťuje odborný garant.

2. VYMEZENÍ POJMŮ

2.1. Použité zkratky

BKOM	Brněnské komunikace a.s.
CCTV	Uzavřený televizní okruh (Closed Circuit Television)
CŘD	Centrální řízení dopravy
DMS	Systém pro správu dokumentů (Document Management System)
EPS	Elektrická požární signalizace
EZS	Elektronický zabezpečovací systém
HW	Hardware. Označuje veškeré fyzicky existující technické vybavení počítače.
ICT	Informační a komunikační technologie (Information and Communication Technologies). Označuje veškeré technologie používané pro komunikaci a práci s informacemi.
IMS	Integrovaný systém řízení
IS	Informační systém. Systém pro sběr, udržování, zpracování a poskytování informací a dat.
ISDS	Informační systém datových schránek
ISMS	Systém řízení bezpečnosti informací (Information Security Management System).
ISSTS	Informační systém správy telematických systémů

ISZS	Informační systém základní služby
IT	Informační technologie. Vše, co se týká fungování počítačů po technické stránce.
KB	Kybernetická bezpečnost
MKDS	Městský kamerový dohledový systém
PS KB	Pracovní skupina kybernetické bezpečnosti
PZTS	Poplachové zabezpečovací a tísňové systémy
RPO	Bod obnovy dat (Recovery Point Objective)
RTO	Doba obnovy chodu (Recovery Time Objective)
SHGK	Systém hlavního generálního klíče
SMB	Statutární město Brno
SŘBI	Systém řízení bezpečnosti informací
SSZ	Světelné signalizační zařízení
STS	Správa telematických systémů
SW	Software (programové vybavení) je v informatice sada všech počítačových programů v počítači. Software zahrnuje aplikační software (pracuje s ním uživatel), operační systém (zajišťuje běh programů) a další.
UPS	Zdroj nepřerušovaného napájení (Uninterruptible Power Supply/Source)
VT	Výpočetní technika
VoKB	Vyhláška č. 82/2018 Sb.o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
VŘKB	Výbor pro řízení kybernetické bezpečnosti
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

2.2. Definice

2.2.1. ***Aktivum***
je jakákoli entita, která má pro jednotlivce nebo organizaci hodnotu, která může být zmenšena působením hrozby.

2.2.2. ***Hrozba***
je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu.

2.2.3. ***Riziko***
vyjadřuje míru ohrožení aktiva, míru nebezpečí, že se uplatní hrozba a dojde k nežádoucímu výsledku vedoucímu ke vzniku škody (dopadu hrozby).

2.2.4. ***Analýza rizik***
zahrnuje ohodnocení kombinace hrozby a zranitelnosti s ohledem na aktiva a výpočet finální hodnoty.

2.2.5. ***Bezpečnost informací***
je zajištění důvěrnosti, integrity a dostupnosti informací a dat.

2.2.6. ***Bezpečnostním opatřením***
se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.

2.2.7. ***Dostupnost***
je vlastnost přístupnosti a použitelnosti na žádost oprávněné entity.

2.2.8. ***Důvěrnost***
je vlastnost, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům.

2.2.9. ***Integrita***
je vlastnost přesnosti a úplnosti aktiv.

2.2.10. ***Základní služba***
Je služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v odvětví doprava a činnosti subjektu odpovědného za kontrolu řízení provozu.

2.2.11. ***Informační systém základní služby***
Je informační systém, na kterém je tato služba závislá.

2.2.12. ***Provozovatel základní služby***
Společnost Brněnské komunikace a.s., která poskytuje základní službu a která je určena NÚKIBem podle §22a zákona o kybernetické bezpečnosti.

2.2.13. ***Správce informačního systému základní služby***
Společnost Brněnské komunikace a.s., která určuje účel zpracování informací a podmínky provozování informačního systému základní služby

2.2.14. ***Provozovatel informačního systému základní služby***
Společnost Brněnské komunikace a.s., která zajišťuje funkčnost technických a programových prostředků tvořících informační systém základní služby.

3. SYSTÉM ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

3.1. Cíle, principy a potřeby řízení bezpečnosti informací

Systém řízení bezpečnosti informací je neustálý proces, který je založený na přístupu k rizikům daného informačního systému a stanovení způsobu ustavení, zavádění, provozu, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací v rámci BKOM.
Základním cílem řízení bezpečnosti informací je ochrana informačních aktiv, řízení rizik bezpečnosti informací a jejich zvládání. Prvořadým úkolem je zajištění důvěrnosti, integrity a dostupnosti služeb a informací, primárních aktiv a nepopiratelnosti právních úkonů, při naplnění požadavků a očekávání zainteresovaných stran.
Dlouhodobými cíli v oblasti systému řízení bezpečnosti informací BKOM jsou:

- zachování potřebné kvality a dostupnosti zpracovávaných informací v poskytované základní službě,
- zajištění důvěrnosti, integrity a dostupnosti zpracovávaných informací,
- zajištění ochrany osob v souvislosti se zpracováním jejich osobních údajů,
- udržování souladu s právními a technickými požadavky stanovenými platnými souvisejícími právními předpisy a technickými normami,
- zajistit schopnost předcházet a zvládat nežádoucí události,
- prosazení odpovědnosti zaměstnanců při zajišťování bezpečnosti informací,

- neustálé zlepšování vhodnosti, přiměřenosti a účinnosti systému řízení bezpečnosti informací.

Principy řízení bezpečnosti informací vycházejí z obecně platného pravidla, že jedině u řízené a koordinované činnosti lze očekávat synergický efekt bezpečnostních opatření. Mezi základní principy řízení bezpečnosti informací patří:

- Princip odpovědnosti – prosazování stanovených zásad, pravidel a postupů bezpečnosti informací musí být spojeno s jednoznačně stanovenou odpovědností zaměstnanců za vykonávanou činnost při celkovém zajištění kybernetické bezpečnosti.
- Princip potřeby znát – přístup a rozsah oprávnění zaměstnance nebo dotčené třetí strany musí být odvozen od toho, co potřebuje znát pro výkon své práce.
- Princip formalizace – prosazování a řízení bezpečnosti informací musí být založeno na formalizovaných a jednoznačně definovaných postupech, jejichž uplatňování podléhá dokumentování.
- Princip kompaktnosti a úplného pokrytí – bezpečnost informací musí být tak odolná, jak odolný je její nejslabší článek. Bezpečnost informací musí být navrhována tak, aby působila vyváženě a chránila všechna aktiva. Zásady bezpečnosti informací musí být jednotně prosazovány do všech činností a procesů.
- Princip řízení bezpečnostní dokumentace – postupy a procesy musí být dokumentovány, aby byla zachována jejich přesná opakovatelnost a dohledatelnost. Tato dokumentace je průběžně aktualizována. O bezpečnostních událostech se vedou záznamy.
- Princip kontroly – zavádění a dodržování zásad, pravidel a postupů, prosazování a řízení bezpečnosti informací podléhá pravidelné kontrole, která ověřuje míru a kvalitu skutečné realizace přijatých opatření.
- Princip nejlepší praxe – přijaté postupy a bezpečnostní opatření jsou aplikovány na základě postupů stanovených nejlepší praxí a příslušnými normami.
- Princip řízení rizik – identifikování relevantních hrozeb a zranitelností, průběžné vyhodnocování rizik a stanovování jejich akceptovatelné úrovně. Zaváděním vhodných opatření jsou rizika zvládána tak, aby byla zajištěna kontinuita činností a dosažena požadovaná úroveň bezpečnosti informací.
- Princip řízení změn – identifikování a řízení významných změn, přezkoumávání možných dopadů změn provozovaných v rámci BKOM.
- Princip neustálého rozvoje – je založen na sledování, měření a vyhodnocování efektivnosti systému bezpečnosti, jeho přezkoumávání a soustavném zlepšování. Cílem je neustálý rozvoj a zlepšování kybernetické bezpečnosti, zkvalitňování poskytovaných služeb a zvyšování úrovně zajištění IS.
- Princip bezpečnostního povědomí – poučení o bezpečném nakládání s informacemi, jejich vytváření a zpracování a zajištění dosažení a udržení bezpečnosti informací musí být nedílnou součástí každodenní práce všech zaměstnanců a bezpečnostní hledisko musí být promítnuto do všech činností a procesů.

Potřeby řízení bezpečnosti informací vyplývají z hodnocení aktiv a rizik. V rámci tohoto procesu jsou zhodnoceny hrozby, zranitelnosti a úrovně jednotlivých rizik. Následně jsou definována patřičná nápravná opatření.

3.2. Rozsah a hranice systému řízení bezpečnosti informací (SŘBI)

SŘBI je podmnožinou integrovaného systému řízení (IMS) s jasně vymezenými hranicemi, ve kterých se uplatňují aplikovatelná pravidla a požadavky ČSN EN ISO/IEC 27001 a přiměřeně pravidla a požadavky ZoKB a VoKB a dalších souvisejících právních předpisů, v rozsahu stanoveném řízenou dokumentací.

Rozsah a hranice SŘBI jsou definovány objektovým perimetrem (fyzické hranice) a logickým perimetrem (logické hranice).

Rozsah SŘBI je vymezen primárními a podpůrnými aktivy uvedenými v seznamech primárních a podpůrných aktiv SŘBI a zahrnuje zejména následující oblasti:

- informace zainteresovaných stran spravované a shromažďované v informačních systémech;
- informace o činnostech;
- informace, které jsou duševním vlastnictvím;
- personální a mzdové údaje o zaměstnancích;
- prostory;
- zařízení a vybavení ve vlastnictví a ve správě svěřeného majetku;
- ICT infrastruktura a SW vybavení;
- zaměstnanci;
- dodavatelé.

Fyzické hranice SŘBI se shodují s fyzickými hranicemi IMS, ve kterých jsou zpracovávány informace BKOM nebo třetích stran, a to jak v listinné, tak i elektronické podobě.

Logické hranice bezpečnosti informací jsou dány ICT infrastrukturou BKOM, zahrnující všechny aplikace potřebné pro správu a provoz IS BKOM, pracovní stanice a přenosná zařízení připojené k těmto systémům, pracovní stanice a přenosná zařízení nepřipojené do sítě, na kterých uživatel zpracovává informace.

3.3. Rozsah a hranice informačního systému správy telematických systémů (ISSTS)

ISSTS je specifickou podmnožinou SŘBI s jasně vymezenými hranicemi, ve kterých se přiměřeně uplatňují pravidla a požadavky ZoKB a VoKB a dalších souvisejících právních předpisů.
Rozsah a hranice informačního systému správy telematických systémů je definován objektovým perimetrem (fyzické hranice) a logickým perimetrem (logické hranice).
Rozsah ISSTS je vymezen primárními a podpůrnými aktivy uvedenými v seznamech primárních a podpůrných aktiv ISSTS a zahrnuje zejména služby, zajišťované:

- Oddělením tunelů a organizace dopravy – CTD
- Oddělením parkovacích systémů – PS
- Oddělením městského kamerového dohlížecího systému – MKDS

Hranice ISSTS jsou dány:
Fyzické hranice ISSTS jsou dány perimetrem objektů nebo prostor užívaných BKOM na adrese:

Sídlo firmy:	Renneská tř. 787/1a, Brno-Štýřice
Provozovna:	Masná 7, Brno
Datové centrum Technických sítí Brno:	Barvířská 5, Brno - Zábrdovice

Koncové body ISSTS: Koncovými body jsou chápána koncová zařízení jednotlivých telematických systémů (např. dopravní kamery, parkovací automaty apod.)

Logické hranice ISSTS jsou dány ICT infrastrukturou STS, zahrnující všechny aplikace potřebné pro správu a provoz telematických systémů, pracovní stanice a přenosná zařízení připojené k

těmto systémům, pracovní stanice a přenosná zařízení nepřipojené do sítě, na kterých se zpracovávají informace správy telematických systémů.

3.4. Rozsah a hranice informačního systému základní služby (ISZS)

ISZS je podmnožinou SŘBI s jasně vymezenými hranicemi, ve kterých se striktně uplatňují veškerá pravidla a požadavky ZoKB a VoKB a dalších souvisejících právních předpisů.

Rozsah informačního systému základní služby je stanoven rozsahem základní služby „Činnost subjektu odpovědného za kontrolu řízení provozu.“ Informační systém, na kterém je tato služba závislá, je informačním systémem základní služby. Základní služba je vymezena následujícím primárním aktivem a jeho vlastníkem:

Poř. číslo	Název primárního aktiva	Garant aktiva
1	Centrální řízení dopravy prostřednictvím světelných signalizačních zařízení	vedoucí oddělení SSZ a CŘD, středisko 3330

Podpůrná aktiva jsou uvedena v katalogu podpůrných aktiv ISZS.
BKOM implementoval všechny relevantní požadavky vyhlášky o kybernetické bezpečnosti v rozsahu informačních systémů základní služby.

Hranice informačního systému základní služby jsou dány:

Fyzické hranice ISZS jsou dány perimetrem objektů nebo prostor užívaných BKOM na adrese:
Sídlo firmy: Renneská tř. 787/1a, Brno-Štýřice
Provozovna: Masná 7, Brno
Koncové body SSZ: Koncovými body jsou chápány jednotlivé řadiče na křižovatkách. Seznam koncových bodů je uveden v příloze v katalogu podpůrných aktiv ISZS.

Logické hranice ISZS jsou dány ICT infrastrukturou SSZ, zahrnující všechny aplikace potřebné pro správu a provoz základní služby, pracovní stanice a přenosná zařízení připojené k těmto systémům, pracovní stanice a přenosná zařízení nepřipojené do sítě, na kterých se zpracovávají informace základní služby.

3.5. Pravidla a postupy pro řízení dokumentace

Obecné zásady a postupy pro řízení dokumentace jsou stanoveny v **PIMS-001 Příručka Integrovaného systému řízení.** Nad rámec zásad uvedených v PIMS-001 platí následující zásady:

- Základním řídícím dokumentem SŘBI je tato politika, která stanovuje hlavní zásady SŘBI. Gestorem politiky je Manažer KB, který věcnou stránku zajišťuje ve spolupráci s osobami zastávajícími bezpečnostní role a s příslušnými středisky.
- Aktualizaci této politiky a další bezpečnostní dokumentace zajišťuje Manažer KB. K návrhu změn této politiky se vyjadřují osoby zastávající bezpečnostní role, Garanti primárních aktiv ISZS a participující úseky a střediska, které je mohou připomínkovat.
- Tato politika s další související bezpečnostní dokumentací je uložena v DMS, prostřednictvím kterého se zaměstnanci seznamují se všemi platnými vnitřními předpisy.

3.6. Pravidla a postupy pro řízení zdrojů a provozu SŘBI

Proces přidělování zdrojů v rámci prostředí BKOM zohledňuje potřeby SŘBI dané zejména výstupy analýzy rizik, potřebami organizačních a technických opatření k zajištění preventivní

bezpečnosti informací a reaktivní schopnosti detekovat kybernetické bezpečnostní události a reagovat na vzniklé kybernetické bezpečnostní incidenty.
Zdroji jsou chápány zejména finanční zdroje, lidské zdroje (zaměstnanci a dodavatelé) a dále potřebné technické vybavení (HW, SW, budovy) a informační zdroje (informace o hrozbách a zranitelnostech) sloužící pro zajištění chodu a funkčnosti jednotlivých oblastí SŘBI. Zdroje pro zajištění bezpečného a spolehlivého provozu ISZS mají vždy prioritu.
Zdroje nutné k pokrytí provozních potřeb bezpečnostních opatření SŘBI jsou přidělovány v rámci standardního řízení k zajištění provozních a investičních potřeb IS, a to efektivně a přiměřeně k řešenému riziku. Zdroje k pokrytí provozních potřeb bezpečnostních opatření ISZS jsou formalizovaným postupem vyžadovány po vlastníkovi infrastruktury ISZS, kterým je SMB.
Za řízení SŘBI odpovídá Manažer KB.
Návrh a implementaci bezpečnostních opatření zajišťuje Architekt KB.
Řízení zdrojů v rámci daného IS zajišťuje příslušný Garant aktiva. U IS, které nejsou ve vlastnictví BKOM a které BKOM provozuje na základně smluvního vztahu s příslušným vlastníkem, zajišťuje řízení zdrojů příslušný Garant aktiva vždy v součinnosti s příslušným vlastníkem IS. Požadavky na zajištění zejména finančních zdrojů jsou předkládány Výboru pro řízení kybernetické bezpečnosti, který je po projednání a po schválení předává vlastníkovi IS.
Potřebné lidské zdroje k provozu SŘBI jsou zajištěny pozicemi v rámci organizační struktury, případně externími subjekty a bezpečnostními a dalšími rolemi stanovenými v kapitole Organizační bezpečnost a bezpečnostní role.

3.7. Pravidla a postupy pro provádění auditů SŘBI

Obecné zásady a postupy pro provádění auditů jsou stanoveny v **PIMS-001 Příručka Integrovaného systému řízení a SmGŘ 006 Audity.** Nad rámec zásad uvedených v PIMS-001 platí následující zásady:

- Audit kybernetické bezpečnosti je prováděn externím subjektem nebo zaměstnancem, splňujícím kritéria a požadavky uvedené ve VoKB.
- Audit kybernetické bezpečnosti ověřuje správnost a účinnost zavedených bezpečnostních opatření a jejich shodu s právními předpisy, interními normami, jinými předpisy a smluvními závazky BKOM. Audit kybernetické bezpečnosti musí být prováděn minimálně v intervalu 2 let nebo vždy při významných změnách, a to alespoň v rozsahu těchto změn.
- Manažer KB zpracovává Program auditů kybernetické bezpečnosti, který předkládá ke schválení Výboru pro řízení kybernetické bezpečnosti.
- Mimořádný audit může být iniciován na základě požadavků nebo podnětů ze strany Manažera KB, Architekta KB nebo Garantů aktiv či dalších rolí SŘBI
- V případě, že ISZS nebo některou jeho část provozuje významný dodavatel v roli provozovatele, předkládá tento výsledky jeho auditů Manažeru KB, který je dále předkládá VŘKB
- VŘKB může požadovat a plánovat audity u významných dodavatelů a provozovatelů informačních a komunikačních systémů.

3.8. Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací

Obecné zásady a postupy pro provádění auditů jsou stanoveny v **PIMS-001 Příručka Integrovaného systému řízení.** Nad rámec zásad uvedených v PIMS-001 platí následující zásady:

- Přezkoumání SŘBI hodnotí možnosti zlepšení a potřebu změn, včetně potřeby aktualizovat bezpečnostní dokumentaci, cíle bezpečnosti a hodnocení aktiv a rizik.

- Manažer KB z podkladů a doporučení, získaných z životního cyklu SŘBI, zpracovává a předkládá „Zprávu o přezkoumání SŘBI“ VŘKB jednou ročně.
- Zlepšování SŘBI vychází z nálezů kontrol a nedostatků, z auditů kybernetické bezpečnosti, poznatků převzatých z nejlepší známé praxe v oblasti řízení bezpečnosti informací a zvládání kybernetických bezpečnostních incidentů, trendů vývoje a aktuální situace v oblasti bezpečnostních hrozeb a zranitelností IS.
- Zlepšování SŘBI je zaměřené zejména na snížení rizik v oblasti bezpečnosti informací.
- Navržená nápravná opatření jsou projednána VŘKB, který kontroluje jejich splnění. Jím projednané plány zvládání rizik a nápravných opatření jsou předkládány vedení BKOM ke schválení.
- Po schválení nápravných opatření a návrhů na zlepšení Manažer KB zahájí jejich realizaci.

3.9. Výjimky

Vzhledem ke skutečnosti, že není možné předvídat veškeré možné okolnosti či situace, které bezpečnostní dokumentace pokrývá, lze z jednotlivých ustanovení, požadavků, pravidel a procesů, které jsou stanoveny bezpečnostní dokumentací, udělit v odůvodněných případech výjimku.

Proces udělení výjimky probíhá následovně:

- Zaměstnanec zjistí skutečnost, že není možné odpovídajícím způsobem plnit ustanovení bezpečnostní dokumentace z jakéhokoliv důvodu a tuto skutečnost projedná se svým přímým nadřízeným zaměstnancem, který následně požádá Manažera KB o projednání výjimky.
- Manažer KB projedná požadavek s příslušným Garantem aktiva a v případě, že výjimka představuje pouze přiměřené a akceptovatelné riziko, předloží žádost i s vyhodnoceným rizikem VŘKB, který ji po zvážení schválí nebo zamítne.
- Výjimka musí mít přesně definovaný rozsah:
  - předmět,
  - dotčené aktivum,
  - vyhodnocení rizik,
  - zdůvodnění a
  - platnost.

4. ŘÍZENÍ AKTIV A RIZIK

4.1. Identifikace, hodnocení a evidence aktiv

Manažer KB je odpovědný za identifikaci, hodnocení a centrální evidenci aktiv a dále řízení rizik, kterým jsou identifikovaná aktiva vystavena.

Pravidla řízení aktiv SŘBI zahrnují:

1. Identifikaci, hodnocení a evidenci primárních aktiv:
   i. určení a evidence jednotlivých primárních aktiv včetně určení jejich Garanta,
   ii. hodnocení důležitosti primárních aktiv z hlediska důvěrnosti, integrity, dostupnosti a kritičnosti.
2. Identifikaci, hodnocení a evidenci podpůrných aktiv:
   i. určení a evidence jednotlivých podpůrných aktiv včetně určení jejich Garanta,
   ii. určení vazeb mezi primárními a podpůrnými aktivy.
3. Pravidla ochrany jednotlivých úrovní aktiv:
   i. způsoby rozlišování jednotlivých úrovní aktiv,
   ii. pravidla pro manipulaci a evidenci aktiv podle úrovní aktiv,
   iii. přípustné způsoby používání aktiv.

4. Způsoby spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií.
5. Seznam aktiv musí být udržován aktuální. Za aktuálnost evidence podpůrných aktiv odpovídá Garant primárního aktiva. Současně musí být evidovány vazby mezi aktivy.
6. Minimální rozsah informací evidovaných k primárnímu aktivu ISZS je:
   - jednoznačný identifikátor,
   - název,
   - stručný popis,
   - typ,
   - garant,
   - lokalizace,
   - hodnocení dostupnosti,
   - hodnocení integrity,
   - hodnocení důvěrnosti,
   - podpůrná aktiva, včetně uvedení jejich vazby na primární aktivum.
7. Pravidelně, minimálně 1x ročně, musí být provedeno hodnocení rizik, působících na aktuální aktiva, která patří do rozsahu systému řízení bezpečnosti informací. Při hodnocení rizik a následně v Plánu zvládání rizik jsou zohledněny:
   i. významné změny,
   ii. změny rozsahu systému řízení bezpečnosti informací,
   iii. opatření podle § 11 zákona o kybernetické bezpečnosti a
   iv. kybernetické bezpečnostní incidenty, včetně dříve řešených.

4.2. Plán zvládání rizik

Identifikovaná neakceptovaná rizika, včetně aktuálních hrozeb a zranitelností, které ještě nebyly hodnoceny v rámci analýzy rizik, jsou zapracována do Plánu zvládání rizik, který vede Manažer KB a který zpracovává v součinnosti s Architektem KB a příslušnými Garanty aktiv. Plán předkládá vždy po provedené aktualizaci ke schválení VŘKB.

Plán zvládání rizik zahrnuje následující informace k rizikům:
- ID Opatření,
- Název bezpečnostního opatření,
- Forma realizace bezpečnostního opatření
- Prioritu,
- Očekávané cíle a přínosy zavedení bezpečnostního opatření,
- Zdroje – informační, technické a lidské (interní i externí)
- Plánovaný termín realizace/dokončení
- Odpovědného zaměstnance
- Odpovědnost za realizaci
- Návaznost na rizika,
- Způsob skutečné realizace
- Stav zavedení,
- Garant,
- Metrika pro vyhodnocení.

Manažer KB odpovídá za stav realizace bezpečnostních opatření, a to vždy společně s garantem příslušného opatření. V případě, že dochází k neplnění realizace některého z identifikovaných opatření, projednává tuto skutečnost s VŘKB, který stanovuje opatření k nápravě.

4.3. Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti eviduje přehled zavedených bezpečnostních opatření, včetně uvedení způsobu jejich implementace a předpokládané účinnosti. Současně vymezuje nezavedená bezpečnostní opatření, u kterých vždy uvádí důvod jejich nezavedení.
Za zpracování Prohlášení o aplikovatelnosti odpovídá Manažer KB, který jej v součinnosti s Architektem KB a Garanty aktiv udržuje v aktuálním stavu.

Metodika pro identifikaci, hodnocení a evidenci aktiv a řízení rizik je uvedena v metodickém pokynu **MP – GŘ O39_01 Metodika analýzy rizik kybernetické bezpečnosti**.

4.4. Pravidla pro manipulaci a evidenci aktiv podle úrovní aktiv (Klasifikační schéma)

Je neefektivní chránit všechny informace stejným způsobem. Proto se zavádí klasifikace informací, která rozdělí informace s ohledem na jejich hodnotu, právní požadavky a citlivost. Pro takto rozdělené informace lze definovat ochranná opatření, která se vztahují pouze na příslušnou kategorii, nebo klasifikační úroveň.
Klasifikované informace musí být chráněny před neautorizovaným přístupem, změnou nebo znepřístupněním po celou dobu jejich platnosti. Po skončení doby platnosti (po vypršení termínu skartačního znaku) se informace komisionálně zničí. O tomto zničení musí existovat záznam.
Jednotlivá informační aktiva v listinné i elektronické podobě (pokud je to technicky možné) musí být v okamžiku vzniku, pořízení nebo zpracování označena a evidována na základě jejich klasifikačního stupně.
Stupeň klasifikace informačního aktiva určuje vždy původce nebo příjemce aktiva, v případě že přijme informační aktivum od třetí strany. Stupně klasifikace se mohou v průběhu životního cyklu informačního aktiva měnit a musí být v takovém případě aktualizována. O způsobech označování dokumentů a nosičů médií rozhoduje VŘKB v součinnosti s pracovníkem odpovědným za spisovou službu.

Pro jednotlivé klasifikační úrovně informací jsou definována pravidla pro:
1. přístup k těmto informacím,
2. přenos informací a dat různými komunikačními prostředky,
3. zacházení s informacemi a daty na konci jejich životního cyklu.

Pravidla pro manipulaci s dokumenty a daty jsou stanovena takto:

Klasifikace	Požadavky	Postup při manipulaci
Veřejné (V)	Požadavky pro uchovávání	Informace musí být označeny, tzn. označení musí být umístěno na dokumentech, médiích (pásky, disky, USB, optická média atd.), elektronických zprávách a souborech. V některých případech musí být zajištěna ochrana integrity informace (např. přístupovým oprávněním) – zejména informace zveřejňované na webových stránkách BKOM.
	Požadavky pro přenos	Žádné
	Požadavky pro skartaci a likvidaci	Žádné
Interní Bez označení	Požadavky pro uchovávání	1. Informace a data jsou ukládána v úschovných objektech, kterými mohou být trezory, uzamykatelné schránky, uzamykatelný kancelářský nábytek apod. Za dostatečnou vybavenost úschovnými objekty vždy odpovídá příslušný vedoucí zaměstnanec. Aplikace zpracovávající data BKOM musí být pravidelně

Klasifikace	Požadavky	Postup při manipulaci
		testovány na viry. Integrita systému musí být pravidelně monitorována.
	Požadavky pro přenos	1. U projektů zahrnujících spolupráci s externími dodavateli musí být ve smlouvě ošetřena důvěrnost poskytovaných informací. 2. Informace mohou být přenášeny mimo BKOM a v případě, že se musí přenášet přes veřejné sítě (internet), mohou se přenášet bez šifrování souborů, za předpokladu zabezpečené e-mailové komunikace (protokol SSL). 3. Informace jsou přístupné pouze oprávněným osobám (např. zaměstnancům, dle popisu pracovní náplně; externím dodavatelům, na základě smluvního vztahu apod.).
	Požadavky pro skartaci a likvidaci	1. Informace musí být bezpečně skartovány, pokud nejsou již nadále potřebné (např. dokumenty v listinné podobě skartovány skartovacím přístrojem splňujícím požadavky normy ISO/IEC 21964-1:2018, bezpečnostní stupeň 3 až 5; stará média zničena rozlomením, rozbitím). 2. Likvidace nebo mazání elektronických dat: i. Přenosných paměťových zařízení (flash a externí disky) – několika násobným formátováním paměťového média (min. 2x) ii. Běžné soubory tzv. „na ploše“ – vymazáním souboru bez umístění do koše (klávesová zkratka shift+del).
Chráněné (CH)	Požadavky pro uchovávání	1. Informace musí být označeny, tzn. označení musí být umístěno na dokumentech, médiích (pásky, disky, USB, optická média atd.), elektronických zprávách a souborech. 2. Informace a data jsou ukládány pouze v uložištích BKOM a do příslušných adresářů, dle pokynů Správce ICT. 3. Informace musí být ukládány v zamčených prostorách (např. dokumenty v zamčených skříních, trezoru nebo v zamčených místnostech). 4. Informace musí být uloženy na úložišti s řízeným (omezeným) přístupem, případně v šifrovaných formátech (např. šifrovaný ZIP, šifrovaný disk) na přenosných médiích, které jsou fyzicky chráněny před zneužitím (např. uloženy v trezoru). 5. Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu.
	Požadavky pro přenos	1. Informace mohou být přenášena mimo BKOM pouze ve výjimečných a zdůvodněných případech. Jestliže je potřeba přenášet informace mimo BKOM (přes veřejné přenosové linky – internet), musí být během přenosu šifrovány. 2. Hesla musí být přenášena odděleně.

Klasifikace	Požadavky	Postup při manipulaci
	Požadavky pro skartaci a likvidaci	1. Informace musí být bezpečně skartovány, pokud nejsou již nadále potřebné (např. dokumenty v listinné podobě skartovány skartovacím přístrojem splňujícím požadavky normy ISO/IEC 21964-1:2018, bezpečnostní stupeň 4 až 7, stará média zničena rozlomením, rozbitím). 2. Likvidace nebo mazání elektronických dat: i. Přenosných paměťových zařízení (flash a externí disky) – několikanásobným formátováním paměťového média (min. 3x) nebo použití speciálních skartovacích aplikací (např. DBAN, Disk Wiper, Quickwiper apod.) ii. Běžné soubory tzv. „na ploše“ – vymazáním souboru bez umístění do koše (klávesová zkratka shift+del).

5. ORGANIZAČNÍ BEZPEČNOST A BEZPEČNOSTNÍ ROLE

5.1. Organizační struktura systému řízení bezpečnosti informací

Generální ředitel je vrcholným představitelem společnosti BKOM a navenek zastupuje roli Povinné osoby.

Nejvyšším orgánem v organizační struktuře systému řízení bezpečnosti informací BKOM je Výbor pro řízení kybernetické bezpečnosti ve složení:

a) **Předseda Výboru** – správní ředitel
b) Členové:
   - Manažer KB – místopředseda Výboru – zajištěn dodavatelsky
   - Garant primárního aktiva – vedoucí oddělení SSZ a CŘD
   - Specialista MKDS
   - Koordinátor KB SMB

Výkonným orgánem Výboru pro řízení kybernetické bezpečnosti je Pracovní skupina kybernetické bezpečnosti ve složení:

a) **Vedoucí Pracovní skupiny –** Manažer KB
b) Členové:
   - Architekt KB – zajištěn dodavatelsky
   - Garant fyzické bezpečnosti
   - Garant personální bezpečnosti
   - Vrcholový administrátor IS Světelného signalizačního zařízení
   - Vrcholový administrátor Centrálního technického dispečinku
   - Manažer IMS
   - Vedoucí oddělení VT

K zajištění řízení systému bezpečnosti informací jsou dále ustanoveny tyto bezpečnostní role:

- Manažer KB, který odpovídá za SŘBI;
- Architekt KB, který odpovídá za návrh a implementaci bezpečnostních opatření;
- Auditor KB, který odpovídá za provádění auditu kybernetické bezpečnosti;
- Garant primárního aktiva, který odpovídá za rozvoj, použití a bezpečnost svěřeného primárního aktiva;

- Garant podpůrného aktiva, který odpovídá za rozvoj, použití a bezpečnost svěřeného podpůrného aktiva;
- Gestor primárních aktiv správy telematických systémů, který je v součinnosti s Garanty určených primárních aktiv STS, odpovědný za zajištění rozvoje, použití a bezpečnosti primárních aktiv STS.
- Administrátor, který zajišťuje správu, provoz, použití, údržbu a bezpečnost technického aktiva v jeho správě;
- Uživatel, který je zaměstnancem nebo externím pracovníkem s přístupem k aktivu SŘBI.

Generální ředitel společnosti určuje svým písemným Rozhodnutím jmenovité složení Výboru pro řízení kybernetické bezpečnosti i Pracovní skupiny kybernetické bezpečnosti a dále role Manažera KB, Architekta KB a Auditora KB, včetně jejich zástupců (kmenové zaměstnance zastupují při výkonu výše určených bezpečnostních rolí zaměstnanci, kteří je zastupují v rámci výkonu jejich pracovní funkce).
Výbor pro řízení kybernetické bezpečnosti určuje Garanty primárních aktiv. Garanti primárních aktiv, v součinnosti s Manažerem a Architektem KB určují Garanty podpůrných aktiv.
Vedoucí střediska správy telematických systémů zastává roli Gestora primárních aktiv STS.
Gestor primárních aktiv STS navrhuje Garanty primárních aktiv STS, které následně schvaluje Výbor pro řízení kybernetické bezpečnosti.
Administrátor je určen obsahem své pracovní náplně.
Uživatel je určen obsahem své pracovní náplně spadající do rozsahu SŘBI, která mu umožňuje přístup k aktivům SŘBI.
Působnost, práva a povinnosti VŘKB, PS KB a bezpečnostních rolí jsou stanoveny v **SmGŘ-046 Organizace kybernetické bezpečnosti.**

6. ŘÍZENÍ DODAVATELŮ

Dodavatelé jsou v rámci SŘBI chápáni jako všechny právnické i fyzické osoby podnikající, které pro BKOM zajišťují, na základě smluvního vztahu, služby a dodávky související s provozem, rozvojem, správou, údržbou a bezpečností ICT prostředků a informačních a komunikačních systémů (aktiva), které jsou ve vlastnictví BKOM anebo které BKOM provozuje na základně smluvního vztahu s příslušným vlastníkem.

SŘBI stanovuje následující role dodavatelů:

a) dodavatel – zajišťuje dodávky nebo služby, které jsou poskytovány v hranicích SŘBI, ale nesouvisí s poskytováním základní služby,
b) významný dodavatel – zajišťuje dodávky nebo služby, které jsou poskytovány v hranicích ISZS, základní služba je na nich částečně závislá, ale jejich nedostupnost či přerušení nemůže zásadním způsobem ovlivnit kvalitu a dostupnost poskytované základní služby,
c) významný dodavatel v roli provozovatele informačního systému základní služby – zajišťuje dodávky a služby zajišťující funkčnost technických a programových prostředků ISZS, které jsou poskytovány v hranicích ISZS, základní služba je na nich závislá a jejich nedostupnost či přerušení může zásadním způsobem ovlivnit kvalitu a dostupnost poskytované základní služby BKOM.

Role dodavatelů identifikuje Pracovní skupina KB na základě návrhů Garantů aktiv, Vedoucího oddělení VT a příslušných vedoucích středisek, kteří Manažeru KB předkládají záměry technických specifikací, souvisejících s plánovanou dodávkou nebo službou ICT, která by měla

být poskytovány v hranicích SŘBI. V případě, že plánovaná dodávka nebo služba bude poskytována v rámci SŘBI, ale pro ICT prostředky nebo informační a komunikační systémy, které nejsou ve vlastnictví BKOM, musí být postup identifikace a informování významných dodavatelů projednáván a řešen v součinnosti s vlastníkem aktiva.
Identifikaci rolí dodavatelů následně Manažer KB předkládá ke schválení VŘKB.

Evidenci dodavatelů vede Vedoucí oddělení VT a příslušní vedoucí středisek.
Evidenci významných dodavatelů vede Manažer KB.
Evidence musí být pravidelně aktualizována.

Manažer KB zpracovává podklady pro informování identifikovaných významných dodavatelů o skutečnosti, že jsou vedeni v evidenci významných dodavatelů. Náležitosti informace pro významné dodavatele jsou zpracovávány v rozsahu požadavků VoKB s důrazem na podrobné uvedení všech skutečností, které vedly k jeho identifikaci. Manažerem předložené podklady pro informování významného dodavatele projedná VŘKB a Předseda VŘKB je předává ke schválení Generálnímu řediteli. Generální ředitel tuto informaci zasílá v listinné podobě nebo prostřednictvím ISDS významnému dodavateli.

Pravidla pro řízení dodavatelů jsou uvedena ve směrnici **SmGŘ- 61 Řízení dodavatelů.**

7. BEZPEČNOST LIDSKÝCH ZDROJŮ

7.1. Povinnosti uživatelů

1. Povinnosti zaměstnanců a všech uživatelů, jimž byl přidělen přístup k aktivům SŘBI:
   a) dodržování schválených pravidel kybernetické bezpečnosti daných bezpečnostní dokumentací, (např. odpovědnost za bezpečné nakládání s ICT, dodržování pravidel ochrany informací v souladu s kategorií jejich klasifikace, požadavky na kvalitu a důvěrnost přístupových a autorizačních údajů a prostředků, hlášení zjištěných nedostatků a bezpečnostních událostí);
   b) ochrana osobních údajů dle nařízení GDPR a zákona č. 110/2019 Sb., o zpracování osobních údajů;
   c) dodržování dalších pravidel vyplývajících z popisu pracovního místa.
2. K plnění těchto povinností se uživatelé zavazují svým podpisem pracovní či jiné smlouvy, přičemž jsou prokazatelně seznámeni minimálně s touto Bezpečnostní politikou informací, **SmGŘ-42 Bezpečné chování uživatele, SmGŘ-040 Zvládání kybernetických bezpečnostních incidentů** a další bezpečnostní dokumentací související s jejich pracovním zařazením nebo pracovním či smluvním vztahem. Za prokazatelné seznámení zaměstnanců s výše uvedenou bezpečnostní dokumentací odpovídá vždy příslušný vedoucí zaměstnanec.
3. Každý uživatel je dále povinen:
   a) seznamovat se neprodleně se změnami v bezpečnostní dokumentaci SŘBI, příslušející typu uživatele či jeho roli v systému řízení bezpečnosti informací,
   b) seznamovat se neprodleně se změnami v provozu ICT v SŘBI a v jeho zabezpečení, zveřejněných formou článků na intranetu společnosti, zaslaných mailem apod. a řídit se v nich uvedenými pravidly a doporučeními,
   c) účastnit se určených vzdělávacích akcí v oblasti bezpečnosti ICT.

7.2. Povinnosti oddělení personální a mzdové agendy

K povinnostem oddělení personální a mzdové agendy a vzdělávání patří zejména:

a) zajistit stručné seznámení zaměstnanců na všech úrovních se závaznými opatřeními danými bezpečnostní dokumentací dle osnovy stanovené Manažerem KB, a to v den nástupu do zaměstnání;
b) při výběru a obsazování zaměstnanců do funkcí v souladu s legislativou přihlížet k jejich bezúhonnosti, charakterovým vlastnostem, schopnostem a podle potřeby nakládání s citlivými informacemi vyžadovat další záruky bezpečnosti. Aktuální výpis z rejstříků trestů je vyžadován u zaměstnanců, u kterých je předpoklad, že budou zastávat některou z bezpečnostních rolí uvedenou ve SmGŘ-046 Organizace kybernetické bezpečnosti v rozsahu hranic ISZS. Další případné specifické požadavky na uchazeče jsou upřesněny příslušnými vedoucími zaměstnanci s ohledem na požadovanou funkci;
c) v rámci přijímacího řízení prověřit, v součinnosti s budoucím přímým nadřízeným uchazeče, u relevantních pracovních míst kvalifikační předpoklady, požadavky na znalosti (v oblasti práce s prostředky ICT, práce s operačním systémem MS Windows, kancelářským balíkem MS Office) a bezpečnostní povědomí uchazeče;
d) zajišťovat vzdělávání v oblasti kybernetické bezpečnosti, jako jsou nástupní školení, následné odborné kurzy, pravidelná školení zaměstnanců, vzdělávání a zvyšování bezpečnostní kvalifikace uživatelů potřebné pro práci s aktivy SŘBI. Požadavky na školení stanovují v součinnosti s Manažerem a Architektem KB a dále na základě požadavků vedoucích zaměstnanců a Garantů aktiv. Školení musí být nejméně v rozsahu stanoveném v Plánu zvyšování bezpečnostního povědomí;
e) vést evidenci záznamů o školeních a požadavcích na vzdělávání v oblasti kybernetické bezpečnosti.

7.3. Povinnosti oddělení VT a střediska STS

Oddělení VT a STS aktivně spolupracuje na:

a) neustálém zvyšování povědomí uživatelů o kybernetické bezpečnosti;
b) v součinnosti s Manažerem KB na stanovení osnovy a obsahu školení v oblasti kybernetické bezpečnosti;
c) zajišťování interních seminářů a školení pro seznamování se s novými aplikacemi a technologiemi a zvyšování bezpečnostního povědomí v oblasti užívání a správy ICT;
d) předkládání požadavků vedoucímu oddělení personální a mzdové agendy na zajištění specifických a odborně zaměřených školení formou externích kurzů, konferencí a seminářů, a to na základě posouzení potřeb, požadavků a nabídky.

7.4. Vstupní školení zaměstnanců

1. Všichni zaměstnanci, kteří v rámci výkonu jejich pracovního zařazení budou přistupovat k aktivům SŘBI prostřednictvím přiděleného uživatelského oprávnění, jsou povinni zúčastnit se úvodního vstupního školení ke kybernetické bezpečnosti, které je standardně organizováno jako součást školení BOZP, PO. Školení provádí pověřený zaměstnanec oddělení VT v součinnosti s Manažerem KB.
2. Seznámení s pokyny významnými pro bezpečnou práci v síti a v informačních systémech BKOM (např. přihlašování do systému, používání hesel, šifrování, zásady používání standardních aplikací, přístupových práv, elektronické pošty a www stránek, stahování souborů z internetu, antivirová ochrana, zálohování a archivace dat, nejčastější typy úniků informací, vzory phishingových e-mailů, způsoby hlášení bezpečnostních událostí a incidentů atd.) provádí ve stanoveném rozsahu Vedoucí oddělení výpočetní techniky nebo jím pověřený zaměstnanec.

3. Uživatelé potvrzují proškolení podpisem prezenční listiny nástupního školení, které jsou založeny na oddělení personální a mzdové agendy.
4. Podle pracovního místa, na které je zaměstnanec zařazen, absolvuje nový uživatel také školení pro práci s ostatními aplikacemi, které bude využívat. Toto zaškolení provádí obvykle Garanti primárních aktiv nebo jimi pověřené osoby.

7.5. Pravidelná školení zaměstnanců

1. Manažer KB ve spolupráci s členy Pracovní skupiny KB a oddělením personální a mzdové agendy, připravuje Plán rozvoje bezpečnostního povědomí zaměstnanců. Tento plán je pravidelně upravován jak z hlediska četnosti jednotlivých školení, tak i z hlediska jejich obsahu tak, aby plně pokrýval bezpečnostní potřeby společnosti, která je v roli správce a provozovatele informačního systému základní služby ve smyslu ZoKB.
2. Každý zaměstnanec se pravidelně účastní školení zaměstnanců a svým podpisem v prezenční listině nebo provedením testu v případě e-learningového kurzu potvrzuje, že byl seznámen s daným tématem školení.
3. Formy školení k problematice bezpečnosti informací mohou být osobní (prezenční), nebo „vzdálené“ typu e-learning s automatizovaným vyhodnocením. Prezenční školení mohou být spojená s pravidelným proškolováním zaměstnanců v oblasti PO a BOZP. Pro hodnocení efektivity těchto školení mohou být použity testy, po jejich vyhodnocení jsou probírány otázky a odpovědi, které se vyznačovaly největší chybovostí.
4. Pro zajištění nezbytných informací a znalostí zaměstnanců, kteří mají specifické bezpečnostní role v systému řízení bezpečnosti informací (např. Manažer KB, Architekt KB, administrátoři, Garanti aktiv ISZS, Garanti oblastí bezpečnosti atd.), musí být nad rámec výše uvedené informovanosti a zácviku zajištěna specializovaná školení pro oblast výkonu jejich rolí. Manažer KB předkládá v součinnosti s osobami, zastávajícími bezpečnostní role, návrhy na absolvování specializovaných školení Výboru pro řízení kybernetické bezpečnosti, který je projednává a schvaluje.
5. Rozsah a periodicita jednotlivých kategorií školení je uveden v Plánu rozvoje bezpečnostního povědomí zaměstnanců.
6. Manažer KB v součinnosti s Pracovní skupinou KB pravidelně vyhodnocuje účinnost rozvoje bezpečnostního povědomí a na jeho základě aktualizuje Plán rozvoje bezpečnostního povědomí zaměstnanců.

7.6. Porušení pravidel bezpečnosti

1. Porušení stanovených pravidel kybernetické bezpečnosti zaměstnanci řeší Manažer KB v součinnosti s příslušným vedoucím zaměstnancem a o výsledku informuje příslušného ředitele úseku. Míru zavinění a konkrétního rizika, případně míru dopadu a následků bezpečnostní události či incidentu stanovuje Manažer KB v součinnosti s Pracovní skupinou KB. Konkrétní postih za porušení pravidel bezpečnosti je stanovován na základě tohoto posouzení. Při uplatňování náhrady škody způsobené zaměstnancem se postupuje v souladu se zákoníkem práce a vnitřními předpisy
2. Při závažných nebo opakovaných porušeních bezpečnostních předpisů může Manažer KB nebo Garant primárního aktiva nařídit omezení nebo odejmutí přístupových oprávnění uživateli do doby vyřešení incidentu a zjednání nápravy.
3. Porušení pravidel bezpečnosti třetími osobami s přístupem k aktivům SŘBI na základě smluvního ujednání řeší Výbor pro řízení kybernetické bezpečnosti. Při posuzování porušení třetí osobou se vždy postupuje dle platné smlouvy.
4. Při zjištění bezpečnostní události nebo incidentu je Manažer KB oprávněn za pomocí administrátorů pozastavit platnost kompromitovaného účtu uživatele do doby, než dojde k normalizaci situace a vyšetření důvodů vzniku narušení.

5. V případě porušení bezpečnostních pravidel je postupováno v souladu s **OŘ-D-001-01 Pracovní řád.**
6. Obecná pravidla pro řízení lidských zdrojů jsou uvedena v dokumentu **SmGŘ-005 Řízení lidských zdrojů**

8. ŘÍZENÍ PROVOZU A KOMUNIKACÍ

8.1. Pravomoci a odpovědnosti spojené s bezpečným provozem

Za řízení bezpečného provozu v hranicích SŘBI odpovídá vedoucí oddělení VT v součinnosti s Manažerem a Architektem KB.
Za řízení bezpečného provozu v hranicích ISSTS odpovídá Gestor primárních aktiv STS v součinnosti s Manažerem a Architektem KB.
Za řízení bezpečného provozu v hranicích ISZS odpovídá Garant primárního aktiva ISZS v součinnosti s Manažerem a Architektem KB.
Pravidla uvedená v této kapitole jsou závazná pro řízení bezpečného provozu v hranicích SŘBI, ISSTS a ISZS

8.2. Postupy bezpečného provozu

Pro řízení, správu a monitorování aktiv informačního systému jsou vytvořeny provozní postupy, respektující bezpečnostní zásady, stanovené touto Bezpečnostní politikou a bezpečnostními požadavky, stanovené Architektem KB.
Všechny provozní postupy používané při správě, údržbě a provozu IS jsou dokumentovány v podobě formálních dokumentů, které podléhají pravidelným revizím a jejich změna probíhá prostřednictvím změnového řízení.
Provozní postupy jsou zpracovány v rozsahu plánů, návodů, manuálů a příruček a zahrnují zejména následující postupy:

a) instalace technických aktiv,
b) zálohování,
c) spojení na kontaktní osoby, poskytující podporu v případě vzniku neočekávaných provozních nebo technických problémů,
d) postupy pro spuštění a ukončení chodu systému, restart nebo jeho obnovu v případě selhání systému či jeho nestandardního stavu.

Provozní postupy jsou dostupné všem dotčeným osobám, které je potřebují k výkonu své pracovní činnosti. Za vedení a správu provozních postupů odpovídá vedoucí oddělení VT, Gestor primárních aktiv STS a Garant primárního aktiva ISZS.

Bezpečnostní pravidla jsou stanovena touto Bezpečnostní politikou a metodickými pokyny. Za aktuálnost stanovených pravidel odpovídá Manažer KB v součinnosti s Architektem KB, vedoucím oddělení VT, Gestorem primárních aktiv STS a Garantem primárního aktiva ISZS.

Provozní a komunikační bezpečnost je v SŘBI zajištěna realizací požadavků na bezpečný provoz, kterými jsou především:

a) Provádění pravidelného sledování a analýz technických zranitelností a následné ošetření slabin ICT infrastruktury. Pro proces řízení a správy technických zranitelností jsou určeny role a odpovědnosti.
b) Udržování aktuálního schématu síťové topologie.
c) Pro veškerou infrastrukturu musí být vedená konfigurační databáze, přičemž zálohy konfigurační databáze musí být ukládány v zabezpečeném úložišti.

d) Konfigurační databáze ICT technologií jsou přístupné pouze příslušným administrátorům a Garantům podpůrných aktiv.
e) Je prováděna autentizovaná synchronizace času.
f) Programové vybavení (software a firmware) musí být instalováno v aktuální verzi a mít implementovány aktuální bezpečnostní záplaty pro danou technologii.
g) Komunikace z vnějších sítí je šifrována adekvátním šifrovacím mechanismem, pro přístup jsou používány bezpečné protokoly a jsou zakázány všechny nepoužívané služby/protokoly.
h) Jsou zaznamenávány důležité události, jako jsou přihlášení a odhlášení uživatelů a administrátorů, změny přístupových práv, neprovedené činnosti, varovná a chybová hlášení, přístupy k záznamům apod.
i) Řízení přístupu, pravidelná aktualizace seznamu uživatelů pro vzdálený přístup a zobrazování upozornění o přihlášení a odpovědnosti.

8.3. Řízení kapacity lidských a technických zdrojů

Vedoucí oddělení VT, Gestor primárních aktiv STS a Garant primárního aktiva ISZS, každý v rámci své působnosti:

1. Zajišťují řízení kapacit technických zdrojů nezbytných pro provoz IS SŘBI a jejich pravidelné sledování. V případě nedostatečných kapacit, připravuje požadavky pro nákup dodatečného vybavení a postupuje dle **SmGŘ-061 Řízení dodavatelů**.
   Řízení kapacit technických zdrojů zahrnuje zejména:
   - Pro každou stávající a plánovanou činnost jsou identifikovány kapacitní požadavky.
   - Zvláštní pozornost je věnována zdrojům, které vyžadují delší dobu pro realizaci dodávky nebo obnášejí vysoké náklady.
   - Optimalizace stávajících kapacit se dosahuje např.:
     - odstraněním zastaralých údajů (na disku);
     - vyřazením nevyužívaných aplikací, systémů, databází nebo prostředí;
     - optimalizací dávkových procesů a jejich plánováním;
     - optimalizací aplikační logiky nebo databázových dotazů;
     - zákazem nebo omezením využitelných kapacit pro služby náročné na zdroje.
2. Vedoucí oddělení VT a Gestor primárních aktiv STS odpovídají za pravidelné sledování kapacity lidských zdrojů nezbytných pro zajištění spolehlivého a bezpečného provozu IS SŘBI a IS STS. V případě potřeby zajištění dalších lidských zdrojů předkládají svou žádost nadřízenému řediteli úseku. Garant primárního aktiva ISZS odpovídá za pravidelné sledování kapacity lidských zdrojů nezbytných pro zajištění spolehlivého a bezpečného provozu ISZS. V případě potřeby zajištění dalších lidských zdrojů předkládá svou žádost Výboru pro řízení kybernetické bezpečnosti.

8.4. Pravidla zálohování

1. Zálohování dat je nezbytnou podmínkou pro zachování kontinuity činností BKOM v případě havárie nebo útoku a z ní vyplývající možné ztráty dat. Jsou prováděny dva typy zálohování:
   a) centrální zálohování dat uložených v informačním systému BKOM (data uložená na serverech),
   b) uživatelské zálohování dat – zálohování dat uložených na pracovních stanicích uživatelů.
2. Centrální zálohování dat uložených v IS SŘBI:

a) Veškeré zálohy dat uložených v administrativních informačních systémech BKOM provádějí zaměstnanci oddělení VT, především určený administrátor. Veškeré zálohy dat uložených v provozních informačních systémech střediska STS provádějí určení Garanti podpůrných aktiv STS. Veškeré zálohy dat uložených v informačním systému základní služby provádějí určení Garanti podpůrných aktiv ISZS. Zálohy jsou prováděny pravidelně v potřebných intervalech a kopiích, podle požadavků Garanta primárního aktiva. Minimálně jedna kopie záloh za určené období je uložena vždy mimo budovu, ve které je primární úložiště zálohovaných dat. Pravidla centrálního zálohování jsou podrobně rozepsána v pokynech pro správce zálohování.
b) Oddělení VT, středisko STS a Garant primárního aktiva ISZS dále odpovídá za:
   - zálohy SW vybavení a instalačních médií pro potřeby obnovy systémů a konfigurací;
   - zálohy souborových serverů;
   - obnovu dat ze záloh, testování čitelnosti záložních médií.

3. Požadavky na zálohování a obnovu
   Minimální požadavky na zálohování a obnovu jsou:
   - rozsah zálohování;
   - doba obnovy chodu (Recovery Time Objective – RTO) se rozumí doba, kdy prvky ICT dosáhnou stanovené úrovně poskytovaných služeb;
   - bod obnovy dat (Recovery Point Objective – RPO) se rozumí okamžik, ke kterému jsou zpětně obnovena data.

   Za stanovení požadavků na zálohování odpovídá Vedoucí oddělení VT, Gestor primárních aktiv STS a Garant primárního aktiva ISZS, v součinnosti s Architektem KB a Garantem primárního aktiva.
4. Pravidla a postupy zálohování
   Každý IS musí mít zpracován Plán zálohování, který obsahuje minimálně:
   a) rozsah zálohování;
   b) stanovení RTO a RPO;
   c) předpokládaný objem zálohovaných dat;
   d) určení způsobu zálohy;
   e) dobu uchování (retence) záloh;
   f) popis tvorby záloh;
   g) určení záložního média a způsobu ukládání;
   h) zabezpečení záloh a medií;

   Za zpracování Plánu zálohování odpovídá vedoucí oddělení VT v součinnosti s Garantem primárního aktiva, Gestor primárních aktiv STS a Garant primárního aktiva ISZS.
   O provedení zálohy musí být vypracován záznam obsahující informace zejména o:
   a) zálohovaných datech;
   b) datum a čas zahájení zálohování;
   c) datum a čas ukončení zálohování;
   d) autorovi zálohy a
   e) výsledku (úspěšné provedení zálohy/s chybou apod.).

   Záznam provádí administrátor nebo Garant podpůrného aktiva, který zálohování provedl.
5. Pravidla a postupy obnovy
   Pravidla obnovy obsahují minimálně:
   a) rozsah obnovy;
   b) zdroj obnovy;
   c) cíl obnovy;
   d) test obnovy.

Pravidla obnovy pro jednotlivé systémy stanovuje vedoucí oddělení v součinnosti s Garantem primárního aktiva, Gestor primárních aktiv STS a Garant primárního aktiva ISZS.

O provedení obnovy dat ze zálohy musí být vedeny záznamy obsahující minimálně tyto informace:

a) obnovovaná data;
b) použitá záloha pro provedení obnovy;
c) datum a čas provedení obnovy;
d) kdo obnovu provedl;
e) výsledek obnovy dat.

Záznam provádí administrátor, který obnovu provedl.

8.5. Licenční čistota a řízení zranitelností

1. BKOM používá výhradně legálně držený software a dbá na licenční čistotu. K tomuto účelu evidují pověření pracovníci oddělení VT zakoupené licence a veškerý provozovaný software v IS SŘBI. Pravidla pro používání a instalaci programů, včetně jejich evidence a sledování počtu licencí, jsou v souladu s autorským zákonem definována v provozních postupech. Vedení aktuální evidence je nezbytné pro plánování potřeby nákupu licencí a udržování deklarované licenční čistoty.
2. Uživatelům je zakázáno ukládat, instalovat a nahrávat jakékoliv aplikace nebo programy (mimo centrálně nabízených aplikací oddělením VT). Uživatelé nesmí spouštět a používat software (ani tzv. free SW), který není legálně zakoupen nebo na který BKOM nevlastní příslušnou licenci. Zjištěná porušení těchto pravidel jsou postihována kapitoly 7.4 Porušení pravidel bezpečnosti této politiky, včetně okamžitého odstranění nepovolených aplikací ze systému či pracovní stanice.
3. Instalaci SW musí provádět pouze oprávněné osoby za tímto účelem určené.
4. Evidence programového vybavení (instalovaného software) je vedena v rozsahu:
   a) dodavatele a výrobce programového vybavení;
   b) aktuální nasazenou verzi;
   c) umístění programového vybavení.

   Za evidenci programového vybavení u administrativních informačních systémů SŘBI odpovídá vedoucí oddělení VT. Gestor primárních aktiv STS a Garant primárního aktiva ISZS odpovídá za evidenci programového vybavení v rámci své působnosti.
5. Architekt KB pravidelně (minimálně 1x měsíčně) monitoruje informace o technických zranitelnostech z dostupných zdrojů, identifikuje rizika a navrhuje Manažerovi KB metody řešení. V případě vyhodnocení zranitelnosti jako relevantní a neakceptovatelné, zajistí Architekt KB, prostřednictvím příslušného administrátora či Garanta podpůrného aktiva, instalaci opravných programových balíčků.
6. Testování oprav a nového programového vybavení je realizováno v prostředí odděleném od produkčního prostředí. O případné potřebě testování a následném nasazení do produkčního prostředí rozhoduje Architekt KB.
7. V rámci nasazení oprav programového vybavení do produkčního prostředí jsou vytvořeny body návratu (RPO) a zálohy dat a vytvořeny zálohy předchozích verzí.

8.6. Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů

1. V rámci IS SŘBI jsou aktivně vyhledávány a monitorovány všechny potřebné činnosti a bezpečnostní události, jako např. výskyt počítačových virů, odepření služby (tzv. DoS), nedodržení postupů pro práci s IS SŘBI apod.

2. Oddělení VT se při této činnosti řídí stanovenými pravidly, přičemž má povinnost pravidelně a nepřetržitě (s využitím a nastavením logování v provozovaných aplikacích) zejména:
   a) sledovat provoz sítě;
   b) udržovat přehled o přístupu uživatelů k IS;
   c) zjišťovat možná ohrožení, bezpečnostní incidenty a narušení bezpečnosti;
   d) identifikovat narušitele;
   e) včas přijímat nápravná opatření;
   f) dodržovat zásady pro bezpečné uchovávání systémových záznamů (logů) a přístup k nim pro pozdější vyhodnocení v případě potřeby.
3. Pro zaznamenávání bezpečnostních a provozních událostí oddělení VT zajišťuje:
   a) jednoznačnou síťovou identifikaci zařízení původce, je-li v komunikační síti použit nástroj, který mění jeho síťovou identifikaci,
   b) sběr informací o bezpečnostních a provozních událostech, zejména zaznamenává
      i. datum a čas včetně specifikace časového pásma,
      ii. typ činnosti,
      iii. identifikaci technického aktiva, které činnost zaznamenalo,
      iv. jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,
      v. jednoznačnou síťovou identifikaci zařízení původce a
      vi. úspěšnost nebo neúspěšnost činnosti,
   c) ochranu informací získaných podle bodů a) a b) před neoprávněným čtením a jakoukoli změnou,
   d) zaznamenávání:
      i. přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,
      ii. činností provedených administrátory,
      iii. úspěšné i neúspěšné manipulace s účty, oprávněními a právy,
      iv. neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,
      v. činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému,
      vi. zahájení a ukončení činností technických aktiv,
      vii. kritických i chybových hlášení technických aktiv a
      viii. přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí
4. Záznamy událostí uchovává vedoucí oddělení VT nejméně po dobu 18 měsíců.
5. Oddělení VT za těmito účely používá řadu nástrojů (od automatizovaných skriptů, systémových záznamů až po nástroj pro centralizovanou správu logů), do nichž jsou zapisovány všechny důležité události. Tyto události se zapisují neprodleně a vedoucí oddělení VT kontroluje dodržování stanovených pravidel zpracování a vyhodnocování. Výsledky jsou předávány Architektovi KB.
6. Architekt KB v součinnosti s Manažerem KB vyhodnocuje získané výsledky a posuzuje je ve vztahu k naplnění bezpečnostních cílů a potřeb SŘBI. Při úpravě a optimalizaci nastavení prostředků se bere v úvahu hodnocení výsledků záznamů z hlediska rizik, efektivnosti a účelnosti.
7. Předání výstupů z dohledových systémů vztažených ke konkrétnímu uživateli může Vedoucí oddělení VT poskytnout pouze na základě písemné žádosti, schválené příslušným ředitelem úseku.

Povinnosti vedoucího oddělení VT a oddělení VT při zaznamenávání událostí u ISSTS a ISZS plní Gestor primárních aktiv STS a Garant primárního aktiva ISZS, každý ve své působnosti.

8.7. Požadavky a standardy bezpečného provozu

Vedoucí oddělení VT musí disponovat dokumentovanými provozními postupy a návody pro správu sítě, serverů, aplikací a dalších technologií pro zajištění bezpečného provozu sítě SŘBI.
Síťové zásuvky organizace jsou připojeny a evidovány dle jejich skutečného využití. Nepoužívané zásuvky jsou příslušným administrátorem v rozvaděči odpojeny.
V SŘBI je využíváno vhodné logické dělení sítě na jednotlivé segmenty (tzv. segmentace sítě). Vedoucí oddělení VT odpovídá za nastavení samostatných segmentů sítě jako jsou např. servery a síťové prvky, WI-FI sítě apod.
Všechna zařízení SŘBI (včetně přenosných) jsou centrálně spravována oddělením VT pomocí specializovaných softwarů např. AD apod. Vedoucí oddělení VT ve spolupráci s Manažerem a Architektem KB musí zajistit minimální požadavky na bezpečný provoz sítě SŘBI, kterými jsou především:

- provádění pravidelného sledování a analýz technických zranitelností (např. na webech https://nvd.nist.gov/search,www.nukib.cz apod.), následné ošetření slabin ICT infrastruktury, v souladu s návrhy Architekta KB,
- udržování aktuálního schématu síťové topologie,
- pro veškerou ICT infrastrukturu musí být vedená konfigurační databáze,
- je prováděna automatizovaná synchronizace času,
- programové vybavení (software a firmware) musí být instalováno v aktuální verzi a mít implementovány aktuální bezpečnostní záplaty pro danou technologii,
- komunikace z vnějších sítí je šifrována adekvátním šifrovacím mechanismem, pro přístup jsou používány bezpečné protokoly a jsou zakázány všechny nepoužívané služby/protokoly,
- jsou zaznamenávány důležité události, jako jsou přihlášení a odhlášení uživatelů a administrátorů, změny přístupových práv, neprovedené činnosti, varovná a chybová hlášení, přístupy k záznamům apod.,
- řízení přístupu, pravidelná aktualizace seznamu uživatelů pro vzdálený přístup a zobrazování upozornění o přihlášení a odpovědnosti.

Za realizaci požadavků a standardů bezpečného provozu u ISSST a ISZS odpovídají Gestor primárních aktiv STS a Garant primárního aktiva ISZS, každý ve své působnosti.

8.8. Pravidla bezpečného používání zařízení

U zařízení používaných v SŘBI pro přístup k síti a aplikacím SŘBI musí být dodržena minimálně tato bezpečnostní opatření:

a) pravidelná aktualizace operačního systému zařízení,
b) pravidelná aktualizace antivirového systému zařízení,
c) chránění zařízení za pomocí vstupního hesla,
d) nastaveno automatické uzamknutí zařízení po 10 minutách nečinnosti uživatele,
e) zaměstnanci disponující privilegovaným oprávněním jsou pro běžnou práci povinni používat standardní uživatelský účet. Účet s privilegovaným oprávněním mohou použít pouze v opodstatněných případech k výkonu činností, pro které je toto oprávnění nezbytné, zejména pro autorizaci,
f) přenosná média a zařízení používaná pro práci zaměstnanci jsou evidována a vhodným způsobem chráněna proti neoprávněnému zpřístupnění cizí osobě (např. šifrováním). Před spuštěním jsou zkontrolována antivirovým SW a na pracovních stanicích je zakázáno automatické spouštění souborů.

Vedoucí oddělení VT odpovídá za nastavení zařízení připojujících se k síti a aplikacím SŘBI dle pravidel uvedených výše. V maximální míře se využívají možnosti centrálních nastavení politik prostřednictvím zásad na Active Directory.

Vedoucí oddělení VT v součinnosti s Manažerem a Architektem KB navrhuje pravidla pro centralizovanou správu zařízení, včetně přenosných zařízení, prostřednictvím např. AD, IDM apod. Tato pravidla schvaluje Pracovní skupina KB.
Povinnosti vedoucího oddělení VT a oddělení VT při realizaci pravidel bezpečného používání zařízení u ISSST a ISZS, plní Gestor primárních aktiv STS a Garant primárního aktiva ISZS, každý ve své působnosti.

8.9. Pravidla pro používání přenosných (mobilních) zařízení

Zaměstnanci mají povoleno vykonávat pracovní činnost mimo objekty BKOM pouze po schválení vedoucím zaměstnancem.

U každého mobilního zařízení, přidělenému zaměstnanci, vedoucí oddělení VT eviduje a v případě změny neprodleně aktualizuje následující údaje:

a) jméno odpovědné osoby;
b) e-mailová adresa odpovědné osoby;
c) operační systém;
d) typ identifikátoru;
e) číslo identifikátoru;
f) datum pořízení a datum předání.

U mobilních zařízení používaných v SŘBI pro přístup k síti a aplikacím SŘBI musí být dodržena minimálně tato bezpečnostní opatření:

a) pravidelná aktualizace operačního systému zařízení,
b) pravidelná aktualizace antivirového systému zařízení,
c) nastavena tak, aby se po 10 minutách neaktivity uživatele uzamkla, v případě smartphonu a tabletu po 2 minutách neaktivity,
d) nastavena tak, aby uživatel disponoval pouze účtem s oprávněním „standardní uživatel“,
e) smartphony a tablety chráněny 4místným PINem, biometrickým údajem nebo heslem s alespoň 6 znaky,
f) vybaveny pouze schválenými aplikacemi,
g) pevný disk šifrován, pokud to operační systém umožňuje.

Vedoucí oddělení VT odpovídá za nastavení zařízení připojujících se k síti a aplikacím SŘBI dle pravidel uvedených výše.

8.10. Pravidla pro používání soukromých mobilních zařízení

Zaměstnanec bere na vědomí, že převzetím přístupových oprávnění k síti a aplikacím SŘBI přebírá odpovědnost za zajištění minimální úrovně ochrany soukromých zařízení, kterou je povinen při přístupu zajistit.
Soukromá zařízení, jejímž prostřednictvím zaměstnanec přistupuje k síti a aplikacím SŘBI, musí být:

a) Vybavena pravidelně aktualizovaným operačním systémem.
b) Vybavena pravidelně aktualizovanou antivirovou aplikací.
c) Chráněna za pomoci přihlašovacích údajů uživatele, s:
   i. minimální délkou hesla: 8 znaků a
   ii. použití alespoň 3 ze 4 skupin znaků (malá písmena, velká písmena, číslice nebo speciální znaky).
   iii. Nastavena tak, aby se po 5 minutách neaktivity uživatele uzamknula, v případě smartphonu a tabletu po 2 minutách neaktivity.

iv. Smartphony a tablety chráněny PINem, biometrickým údajem nebo heslem s alespoň 6 znaky.
v. Vybaveny pouze aplikacemi instalovanými z oficiálních obchodů (např. Google Play, Apple store, Galaxy store apod.).

Při používání mobilních a soukromých zařízení pro připojení k aplikacím SŘBI jsou zaměstnanci povinni:

a) Učinit všechna dostupná opatření, která mohou zabránit ztrátě či odcizení zařízení (neponechávají je bez dohledu a/nebo zabezpečení např. v dopravních prostředcích, v ubytovacích zařízeních apod.).
b) Pro připojení k internetu prostřednictvím WI-FI sítě využívat pouze šifrovaného, zabezpečeného připojení (připojení prostřednictvím hesla, důvěryhodný poskytovatel – zaměstnavatel apod., pořadatel školení apod.) a po ukončení práce se odpojit (zásadně nelze využívat např. free WI-Fi v nákupních centrech, hotelích, nádražích apod.).
c) Aktivně zabraňovat odpozorování obrazovky cizí osobou (např. ve vlacích, restauracích, na lavičkách, v prostředcích hromadné dopravy apod.).
d) Neumožnit přístup ke zpracovávaným informacím SŘBI jiné osobě, včetně rodinných příslušníků.

Použití soukromých mobilních zařízení pro připojení do sítě BKOM povoluje vždy příslušný ředitel úseku v součinnosti s příslušným Garantem primárního aktiva a Manažerem KB.

8.11. Evidence vzdálených dohledů dodavatelů

V rámci poskytování služby ICT zpravidla dodavatel v případě závady, kontroly přistupuje vzdáleně na spravovaný prostředek v BKOM přímo do interní sítě BKOM. V případě trvalé diagnostiky má dodavatel na firewallu nastaven trvalý zabezpečený kanál pro odesílání diagnostických dat.

Pokud vyvstal požadavek na toto připojení dodatečně, musí vedoucí oddělení VT, Gestor primárních aktiv STS nebo Garant primárního aktiva ISZS zajistit doplnění potřebných parametrů tohoto přístupu do smlouvy s dodavatelem, a to minimálně v rozsahu:

- popis komunikačních kanálů a přípojných bodů do BKOM:
- název interního prostředku, na nějž dodavatel přistupuje,
- IP adresa zařízení,
- popis provozovaných aplikací na zařízení,
- výčet přípojných bodů dodavatele (adresa pracoviště, IP adresa, kontakt).

8.12. Politika ochrany před škodlivým kódem

Škodlivým kódem je souhrnně označován nežádoucí SW kód, tzv. malware (vir, červ, trojský kůň, spyware, ransomware apod.), který může způsobit nejrůznější škodlivé účinky a dopady.

Vedoucí oddělení VT odpovídá za správné nasazení a nastavení antivirových aplikací na všech zařízeních v SŘBI.

Uživatelé musí být informováni o nebezpečí, které vzniká použitím neschválených programů nebo působením škodlivých programových kódů.

Uživatelé musí být informováni o nebezpečí spočívajícím v rizikovém chování na internetu (např. klikání na různé bannery, otevírání podezřelých příloh e-mailů apod.).

Antivirové aplikace musí být automatizovaně aktualizované.

Použité programové prostředky musí souhrnně zajistit následující možnosti a funkcionalitu:

a) možnost nasazení pro všechna zařízení v SŘBI s centralizovanou správou,

b) možnost on-line kontroly průniku škodlivých kódů z internetu a jiných zdrojů,
c) automatické blokování poškozených souborů s možností jejich opravy,
d) automatické blokování souborů s nepovolenými příponami,
e) zákaz automatického spouštění obsahu výměnných zařízení a datových nosičů,
f) generování výstrah a ukládání auditních záznamů o provedených činnostech,
g) automatická aktualizace virových databází a samotného programu.

Nástroje na ochranu před škodlivým kódem musí provádět stálou kontrolu mezi vnitřní a vnější sítí, u serverů, datových úložišť, pracovních stanic i mobilních zařízení. Používané nástroje musí být automaticky aktualizovány, aby byla zajištěna aktuálnost virové databáze i samotného SW.
Pro jednotlivé nástroje jsou určeni odpovědní zaměstnanci oddělení VT, ISSTS a ISZS, dle jejich nasazení (síť, servery, pracovní stanice apod.).
Za definici rozsahu konkrétních opatření odpovídá Architekt KB v součinnosti s vedoucím oddělení VT, Gestorem primárních aktiv STS a Garantem primárního aktiva ISZS.

9. ŘÍZENÍ PŘÍSTUPU

9.1. Princip minimálních oprávnění/potřeba znát

1. Řízení přístupových práv musí být realizován podle principu „minimálních oprávnění“.
2. Pravidla pro řízení přístupových oprávnění:
   a) Každý uživatel má přístup pouze k těm aktivům, která nezbytně potřebuje k výkonu své práce, určené pracovní náplní.
   b) Základní rozsah oprávnění k jednotlivým aktivům je definován jako minimum potřebného pro činnosti, které uživatel potřebuje. Oprávnění jsou členěna do uživatelských rolí.
   c) Změna rozsahu přístupových oprávnění je řízena a schvalována.
   d) Přístupy k aktivům musí být nejdříve zakázány a následně jednotlivě uživatelům povolovány podle jejich pracovní pozice a role, při respektování principu „potřeba znát“, který určuje, že uživatel nesmí mít přístup k aplikaci nebo datům, které nepotřebuje k výkonu své pracovní pozice.

9.2. Požadavky na řízení přístupu

Každý zaměstnanec (uživatel) využívající výpočetní techniku organizace používá pro připojení k operačním systémům a aplikacím SŘBI, ISSTS a ISZS jedinečné uživatelské jméno a heslo, které s nikým nesdílí.
Uživatelé získávají ke svému účtu základní oprávnění, odpovídající pracovnímu zařazení, vykonávané práci a zásadě potřeby znát.
Společné, projektové či jinak sdílené uživatelské účty jsou zakázány. Výjimkou jsou technické účty, které spravuje určený zaměstnanec oddělení VT, střediska STS a určený Garnat podpůrného aktiva ISZS.
Všem zaměstnancům BKOM jsou přidělovány pouze účty s oprávněním „standardní uživatel“.
Je prováděna pravidelná kontrola řízení přístupových práv a stanovených pravidel pro řízení přístupových práv.
Kontrola přidělených přístupových oprávnění je prováděna při každé významné změně a minimálně jednou za rok a za její realizaci odpovídají Garanti primárních aktiv v součinnosti s vedoucím oddělení VT. Za kontrolu přidělených přístupových oprávnění u ISSTS a ISZS odpovídá Gestor primárních aktiv STS a Garant primárního aktiva ISZS, každý ve své působnosti.

Je vedena evidence o uskutečněných přístupech a o pokusech o přístup k OS nebo aplikaci SŘBI, ISSTS a ISZS.
Primárním nástrojem pro řízení uživatelů SŘBI je AD.
Pro přístup k ISZS se využívá vícefaktorová autentizace, pokud je to technicky možné.
Garanti primárních aktiv jsou odpovědní za řízení všech přístupových oprávnění zaměstnanců k SŘBI, ISSTS a ISZS ve své odpovědnosti.

9.3. Řízení přístupových oprávnění

Je zavedena aktuální evidence uživatelských účtů pro lokální i vzdálený přístup interních i externích uživatelů. Za vedení této evidence odpovídá vedoucí oddělení VT, Gestor primárních aktiv STS a Garant primárního aktiva ISZS, každý ve své působnosti.
Uskutečněné přístupy a pokusy o přístup k OS a aplikacím SŘBI, ISSTS a ISZS musí být automaticky zaznamenávány a monitorovány prostřednictvím záznamu událostí pro další využití.
Je nastaveno časové omezení platnosti přihlašovací relace, po jehož vypršení následuje automatické ukončení přihlášení k IS.
Je nastaveno řízení počtu možných neúspěšných pokusů o přihlášení, které jsou automaticky zaznamenávány a monitorovány prostřednictvím záznamu událostí.
Nástroj pro ověření identity uživatelů, administrátorů a aplikací automatizovaně vynucuje následující pravidla:

- minimální délka hesla: 12 znaků u standardních účtů,
- minimální délka hesla: 17 znaků u privilegovaných účtů,
- heslo musí obsahovat alespoň 3 ze 4 skupin znaků (malá písmena, velká písmena, číslice nebo speciální znaky),
- maximální platnost hesla: 12 měsíců,
- minimální platnost hesla: 24 hodin,
- historie hesel: 3 hesla,
- maximální počet neúspěšných pokusů o přihlášení: 5,
- doba zablokování účtu po neúspěšných pokusech o přihlášení: 30 minut,
- vynucení bezodkladné změny výchozího hesla po jeho prvním použití.

9.4. Přidělení přístupového oprávnění

1. Personalista na základě podpisu pracovní smlouvy nebo jiné pracovně právní smlouvy zadá žádost o přidělení přístupových oprávnění k IS SŘBI a ISSTS, kde uvede následující informace o zaměstnanci do aplikace Podepisto:
   - jméno a příjmení zaměstnance,
   - pracovní zařazení,
   - termín nástupu,
   - osobní číslo,
   - organizační jednotka (středisko, oddělení, …).
2. Žádost je přidělena příslušnému vedoucímu zaměstnanci, který určí rozsah přidělených přístupových oprávnění s ohledem na předpokládanou pracovní náplň zaměstnance a žádost schválí.
3. Žádosti o přidělení přístupových oprávnění k ISZS se podávají prostřednictvím HelpDesku ISZS a schvaluje je Garant primárního aktiva ISZS.
4. Na základě této schválené žádosti zřídí příslušný zaměstnanec oddělení VT, střediska STS a ISZS uživatelský účet pro uvedeného zaměstnance a zajistí nastavení přístupových oprávnění do informačních systémů a aplikací dle schváleného rozsahu.

5. Zaměstnanec, který zřídil přístupové oprávnění pro nového zaměstnance se schváleným rozsahem, provede záznam o rozsahu přidělených přístupových oprávnění do evidence přístupových oprávnění. K záznamu přiloží seznam všech schválených požadavků na rozsah přístupového oprávnění.
6. Za evidenci přístupových oprávnění odpovídá vedoucí oddělení VT, Gestor primárních aktiv ISSTS a Garant primárního aktiva ISZS, každý ve své působnosti.

9.5. Změna přístupového oprávnění

1. Změna přístupového oprávnění je prováděna na základě žádosti, kterou schvaluje vedoucí zaměstnanec zaměstnance, jehož se změna uživatelských oprávnění týká. Schválenou žádost zasílá e-mailem vedoucímu oddělení VT anebo Gestorovi primárních aktiv STS. Žádost o změnu přístupových oprávnění u ISZS se vkládá do HelpDesku a schvaluje ji Garant primárního aktiva.
2. Žádost musí obsahovat identifikaci zaměstnance, požadovanou změnu rozsahu přístupového oprávnění, důvod změny a informaci, zda se jedná o trvalou změnu či dočasnou. V případě, že se jedná o dočasnou změnu, žádost musí obsahovat také přesné určení období, po které mají být přístupová oprávnění změněna.
3. Zaměstnanec oddělení VT, střediska STS a ISZS, který bude změnu realizovat, nejdříve zruší u příslušného zaměstnance veškerá přidělená přístupová oprávnění a teprve potom nastaví rozsah nového přístupového oprávnění.
4. O změně přístupového oprávnění provede záznam do evidence přístupových oprávnění.

9.6. Zrušení přístupového oprávnění

1. V případě ukončení pracovněprávního vztahu se společností BKOM zasílá vedoucí oddělení personální a mzdové agendy vedoucímu oddělení VT, Gestorovi primárních aktiv a Garantovi primárního aktiva ISZS, informaci o ukončení pracovněprávního vztahu (na základě této informace provede pracovník oddělení VT, střediska STS a ISZS změnu přístupového hesla k tomuto účtu k datu ukončení pracovněprávního vztahu) a příslušný vedoucí zaměstnanec zašle požadavek na odebrání přístupových oprávnění (Výstupní list ICT-žádost, příloha č.3 SmGŘ-005-c). Tento požadavek musí obsahovat:
   - identifikaci zaměstnance,
   - datum, ke kterému mají být uživatelská oprávnění deaktivována a uživatelské účty smazány,
   - případné požadavky na nestandardní opatření (přesměrování emailové schránky, zřízení zálohy apod.).
2. Zaměstnanci musí být nejpozději v den odchodu zrušena veškerá přístupová oprávnění.
3. V případě řešení bezpečnostní události či incidentu, může požádat o dočasné zablokování přístupových oprávnění i Garant primárního aktiva (příslušný vedoucí zaměstnanec) nebo Manažer KB.
4. O zrušení či pozastavení platnosti uživatelských oprávnění provede zaměstnanec oddělení VT, střediska STS a ISZS, který zrušení či pozastavení realizoval, záznam do evidence přístupových oprávnění.
7. Za vedení a aktuálnost evidence přístupových oprávnění odpovídá vedoucí oddělení VT, Gestor primárních aktiv ISSTS a Garant primárního aktiva ISZS, každý ve své působnosti.

9.7. Řízení privilegovaných přístupových oprávnění

Privilegovaným oprávněním se rozumí přístupové oprávnění k účtu, které umožnuje v jednotlivém prvku ICT minimálně jednu z níže uvedených možností:

a) vykonávat činnosti nad rámec běžného uživatele IS;
b) provádět změny v nastavení IS;

c) měnit rozsah přidělených oprávnění jednotlivých rolí a uživatelů;
d) vykonávat servisní činnosti bez přítomnosti uživatele.

Použití privilegovaných oprávnění je řízeno a je striktně odděleno od standardních uživatelských oprávnění.

Vedoucí oddělení VT přiděluje privilegovaná oprávnění pouze těm zaměstnancům oddělení VT, kteří jej ke své práci prokazatelně potřebují (např. administrátoři aplikací). Pokud je žádáno o zřízení privilegovaného oprávnění pro zaměstnance, který není zaměstnancem oddělení VT, musí být žádost schválena a odůvodněna příslušným ředitelem úseku.
Zaměstnanci s privilegovanými oprávněními jsou si plně vědomi vyšších bezpečnostních požadavků spojených s tímto typem oprávnění. Přístupové heslo pro tato oprávnění musí splňovat všechny požadavky uvedené v bodě 9.3 Řízení přístupových oprávnění.
Každý uživatel privilegovaného oprávnění musí udržovat heslo v tajnosti. Privilegovaná oprávnění se oprávněným zaměstnancům vytvářejí jako samostatné uživatelské účty, které jsou jednoznačně odděleny od standardního účtu uživatele.

Zaměstnanci disponující privilegovaným oprávněním jsou pro běžnou práci povinni používat standardní uživatelský účet. Účet s privilegovaným oprávněním mohou použít pouze v opodstatněných případech k výkonu činností, pro které je toto oprávnění nezbytné.

Vedoucí oddělení VT vede seznamy zaměstnanců, kteří disponují privilegovaným oprávněním. Povinnosti vedoucího oddělení VT při řízení privilegovaných přístupových oprávnění u ISSST a ISZS, plní Gestor primárních aktiv STS a Garant primárního aktiva ISZS, každý ve své působnosti.
Manažer KB, ve spolupráci s odpovědnými zaměstnanci, tyto seznamy přezkoumává z hlediska aktuálnosti a potřebnosti minimálně 1x do roka.

9.8. Přidělení, změny a rušení přístupových oprávnění externích subjektů

1. Veškeré přidělení a změny uživatelských oprávnění pro externí subjekty musí být schváleny příslušným ředitelem úseku, do jehož kompetence spadá smlouva s externím subjektem.
2. Žádost o zřízení a změny uživatelských oprávnění externího subjektu k IS SŘBI a ISSTS je zasílána elektronicky vedoucímu oddělení VT a Gestorovi primárních aktiv STS.
3. Žádost o zřízení a změny uživatelských oprávnění externího subjektu k ISZS se podává prostřednictvím HelpDesku. Garant primárního aktiva ISZS odpovídá za zřízení přístupu k HelpDesku pro žádající extérní subjekty a schvaluje zřízení či změny uživatelských oprávnění externích subjektů.
4. Přesná definice rozsahu uživatelských oprávnění musí být součástí smlouvy uzavřené mezi externím subjektem a BKOM. Změny je možné provádět formou uzavření dodatku ke smlouvě.
5. V případě ukončení smlouvy s externím subjektem je za zrušení přidělených přístupových oprávnění odpovědná osoba, která je odpovědná za smluvní vztah s dodavatelem.
6. Vedoucí oddělení VT, Gestor primárních aktiv STS a Garant primárního aktiva ISZS vede evidenci přístupů pro externí subjekty.

10. ŘÍZENÍ ZMĚN

Všechny významné změny prvků ICT SŘBI, Telematických systémů STS a ISZS, včetně změn v nastavení provozních a bezpečnostních parametrů, aktualizací apod., jsou plánovány a řízeny.
Změny jsou rozděleny do dvou skupin:

1. Změna IS – stávající změna IS,
2. Významná změna IS – změna IS, která má nebo může mít vliv na kybernetickou bezpečnost a představuje vysoké riziko, které je určeno analýzou rizik.

Pro každou významnou změnu musí být stanoven postup pro návrat do původního stavu před provedenou změnou.
Před rozhodnutím o realizaci významné změny jsou zejména vzata v úvahu následující opatření:

a) plánování změny, spočívající ve stanovení plánovaného rozsahu změny a zpracování a vyhodnocení plánu a harmonogramu životního cyklu změny,
b) zhodnocení rizik, spočívající v provedení analýzy rizik u aktiv, která souvisí s plánovanou změnou,
c) zhodnocení potenciálních dopadů (včetně dopadů na bezpečnost informací) takových změn a zavedení opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami, spočívající v posouzení závěrů z provedené analýzy rizik s cílem posoudit možné dopady v oblastech:
   - dopadů na funkčnost a kvalitu poskytované základní služby v případě, že se jedná o významnou změnu v hranicích ISZS,
   - dopadů na funkčnost a kvalitu poskytovaných služeb v případě, že se jedná o významnou změnu v hranicích SŘBI a STS,
   - finanční náročnosti změny.

Významné změny musí být testovány. Plán testování významných změn musí obsahovat:

a) definici rozsahu a druhy testů;
b) časový harmonogram testování;
c) rozsah rolí určených pro testování;
d) školení rolí určených pro testování;
e) testovací scénáře;
f) metriky testování;
g) vyhodnocení testů.

Významné změny musí být dokumentovány. Dokumentace změny musí obsahovat:

a) závěry z provedené analýzy rizik;
b) výsledek přezkoumání dopadů významné změny;
c) rozhodnutí o realizaci významné změny;
d) stanovení osob a jejich odpovědnosti za realizaci významné změny;
e) plán nasazení významné změny;
f) požadavky na projektovou, provozní a bezpečnostní dokumentaci;
g) plán testování významné změny;
h) akceptaci významné změny.

Manažer KB je odpovědný za případnou aktualizaci bezpečnostní politiky a bezpečnostní dokumentace. Garant primárního aktiva ISZS, Gestor primárních aktiv STS a vedoucí oddělení VT jsou odpovědni za provedení změn v provozní dokumentaci ISZS, ISSTS a SŘBI.

Manažer KB ve spolupráci s Architektem KB, vedoucím oddělení VT a Gestorem primárních aktiv STS odpovídá za řízení změn v hranicích SŘBI.
Manažer KB ve spolupráci s Architektem KB a Garantem primárního aktiva ISZS odpovídá za řízení změn v hranicích ISZS. Významné změny, mající zásadní dopad na poskytování a kvalitu základní služby, projednává vždy Pracovní skupina KB a schvaluje VŘKB, který schválenou změnu následně projednává s vlastníkem infrastruktury ISZS, který změnu schvaluje a stanovuje způsob financování.

11. AKVIZICE, VÝVOJ A ÚDRŽBA

Proces akvizice, vývoje a údržby je plánován, řízen a dokumentován. Vedení BKOM odpovídá za určení a poskytnutí ICT prostředků potřebných pro:

a) udržování souladu se zákonnými a dalšími požadavky a dodržování bezpečnostních závazků, uvedených ve smlouvách,
b) vybudování, zavedení, provoz, monitorování, udržování a zlepšování systému řízení bezpečnosti informací,
c) udržování odpovídající úrovně bezpečnosti informací správnou aplikací všech zavedených opatření.

11.1. Odpovědnosti za akvizici, vývoj a údržbu

Garant primárního aktiva:

a) definuje funkční požadavky na akvizici a vývoj jednotlivých prvků,
b) zajišťuje hodnocení aktiva,
c) navrhuje pravidla přístupu k aktivu.

Architekt KB navrhuje implementaci bezpečnostních opatření na úrovni:

a) bezpečnosti vývojového a testovacího prostředí,
b) kontrolních bodů bezpečnosti v projektu,
c) bezpečného úložiště,
d) řízení verzí,
e) identifikaci zranitelností a návrhu opatření.

Garant podpůrného aktiva definuje požadavky na provoz a údržbu prvku ICT.

Manažer KB ve spolupráci s Architektem KB a Garantem primárního aktiva ISZS odpovídá za plánování akvizic v hranicích ISZS. Požadavky na akvizici projednává vždy Pracovní skupina KB a záměr akvizice schvaluje VŘKB, který plánovanou akvizici následně projednává s vlastníkem infrastruktury ISZS, který ji schvaluje a stanovuje způsob financování.

11.2. Životní cyklus projektu akvizice, vývoje a údržby

Životní cyklus projektu akvizice obsahuje bezpečnostní požadavky a bezpečnostní opatření v závislosti na platné bezpečnostní politice, identifikovaných rizicích a požadavcích Architekta KB a Garantů aktiv.
Životní cyklus projektu akvizice, vývoje a údržby se dělí na tyto na sebe navazující fáze:

1. Stanovení požadavku, spočívající v identifikaci požadavku na nový, nebo změnu stavu stávajícího IS.
2. Akvizice, spočívající v definici podrobného rozsahu požadavku a provedení:
   a) Identifikace a hodnocení rizik požadavku.
   b) Stanovení bezpečnostních opatření.

3. Vývoj, spočívající v procesu změny ze stavu aktuálního do stavu plánovaného akvizicí a procesu testování, realizovaného výhradně v odděleném vývojovém a testovacím prostředí od produkčního a za použití pouze anonymizovaných či smyšlených dat.
4. Údržba, spočívající v provádění činností stanovených provozní dokumentací.

Vývoj, změny a údržba aktiv jsou prováděny v souladu s pravidly uvedenými v této politice a stanovenými procesy, které zohledňují zásady bezpečného vývoje a řízení změn, testování v rámci odděleného prostředí.
Za účelem neustálého zlepšování je prováděna pravidelná kontrola účinnosti procesu akvizice, vývoje a údržby alespoň jednou za rok. Kontrola účinnosti je zaměřena na:

a) Provádění identifikace a hodnocení rizik požadavku.
b) Promítnutí bezpečnostních požadavků do projektové dokumentace.
c) Dodržování požadavku bezpečného vývoje a údržby.

Výsledkem kontroly účinnosti procesu akvizice, vývoje a údržby je zpráva o účinnosti, která obsahuje zjištění a doporučení pro zlepšení celého procesu.
Zpráva o účinnosti je jedním ze vstupních zdrojů informací pro celkové vyhodnocení účinnosti řízení systému řízení bezpečnosti informací prostřednictvím přezkoumání a její výsledky musí být zohledněny v plánu zvládání rizik kybernetické bezpečnosti při plánování na další období.
Za vyhodnocení účinnosti procesu akvizice, vývoje a údržby odpovídá Manažer KB.
V případě, že se v rámci akvizice jedná o významnou změnu stávajícího IS, musí být zohledněny požadavky pravidel stanovených v kapitole „Řízení změn“.

11.3. Řízení zranitelností v projektu akvizice, vývoje a údržby

Proces řízení zranitelností aktiv je plánován, dokumentován a řízen. Je založen na:

- identifikaci zranitelností;
- řešení zranitelností dle priorit;
- kontrole aplikovaných opatření.

Technické přezkoumání aplikací po změnách provozní platformy jednotlivých prvků ICT vyžaduje alespoň:

- přezkoumání postupů řízení a integrity aplikací a zabezpečení dat k zajištění, že nebyly změnami provozních platforem kompromitovány;
- zajištění včasného oznámení změn provozních platforem, aby bylo před implementací umožněno provedení příslušných testů a přezkoumání;
- zajištění provedení příslušných změn v plánech kontinuity činností.

Změny programového vybavení jsou omezeny na nezbytné změny a všechny jsou řízeny. V případě, že je nutno programové vybavení upravit, jsou posuzovány následující body:

- rizika navrhovaných opatření a procesů zajišťujících integritu;
- dodržení licenční politiky;
- součinnost s dodavatelem při aktualizaci programového vybavení;
- kompatibilita s dalším používaným programovým vybavením.

Manažer KB ve spolupráci s Architektem KB vedoucím oddělení VT a Gestorem primárních aktiv STS odpovídá za řízení zranitelností v hranicích SŘBI a ISSTS.
Manažer KB ve spolupráci s Architektem KB a Garantem primárního aktiva ISZS odpovídá za řízení zranitelností v hranicích ISZS.

12. BEZPEČNOST KOMUNIKAČNÍCH SÍTÍ

12.1. Pravidla a postupy pro zajištění bezpečnosti sítě

1. Pro prvky komunikační sítě je definován účel, provozní a technické parametry, postupy pro správu a údržbu.
2. Každá část komunikační sítě musí být dokumentovaná ve fyzické a logické vrstvě. Za vedení dokumentace odpovídá vedoucí oddělení VT, Gestor primárních aktiv STS a Garant primárního aktiva ISZS, každý ve své působnosti.
3. Správa sítě a síťových prvků je oddělena od správy pracovních stanic a serverů.
4. Síť je segmentována a logicky oddělena za účelem zajištění bezpečnosti prvků ICT systémů a odolnosti vůči případným útokům.
5. Za správu komunikačních sítí odpovídá vedoucí oddělení VT, Gestor primárních aktiv STS a Garant primárního aktiva ISZS, každý ve své působnosti. V rámci komunikační sítě musí být nastaveno řízení přístupů.
6. Musí být zajištěna ochrana přenosu ztráty paketů i možného odposlechu.
7. Pro ochranu komunikační sítě se využívají bezpečnostní opatření technického charakteru, minimálně v rozsahu:
   a) Segmentace komunikační sítě.
   b) Řízení komunikace v rámci komunikační sítě a perimetru komunikační sítě.
   c) Pomocí kryptografie zajištění důvěrnosti a integrity dat při vzdáleném přístupu, vzdálené správě nebo při přístupu do komunikační sítě pomocí bezdrátových technologií.
   d) Blokace nežádoucí komunikace.
   e) Využívání nástroje, který zajistí ochranu integrity komunikační sítě.
   f) Oddělení interní a externí sítě pomocí firewallu a proxy serveru.
   g) Musí být nastaveno monitorování sítě a vyhodnocování provozních záznamů.
8. V rámci komunikační sítě ISZS musí být navíc zajištěn provoz nástroje, zajišťujícího ochranu integrity sítě.
9. V rámci ochrany integrity vnitřní sítě ISZS musí být prováděno zrcadlení dat na druhou linii serverů.

12.2. Určení práv a povinností za bezpečný provoz sítě

1. Všechny části a prvky komunikačních sítí musí být přiřazeny Garantům podpůrných aktiv.
2. Garant podpůrného aktiva je odpovědný za efektivní využití všech dostupných bezpečnostních funkcí používaných technologií a odpovídá za správu bezpečnosti sítě.
3. Architekt KB posuzuje nastavení a změny bezpečnosti provozu sítě a navrhuje opatření k zajištění bezpečného provozu sítě.

12.3. Pravidla a postupy pro řízení přístupů v rámci sítě

1. Do sítě interní sítě LAN lze připojovat pouze prostředky ICT, které jsou v majetku a správě BKOM anebo které BKOM provozuje pro jiného vlastníka.
2. Pravidla jsou aplikovatelná na všechny komunikační sítě BKOM alespoň v rozsahu:
   a) interní sítě LAN;
   b) externí sítě WAN a MAN;
   c) propojení na externí sítě (Internet).
3. Pro přístupy uživatelů a administrátorů do vnitřní sítě jsou použity nástroje pro správu a ověření identity.
4. Pro přístupy technických prostředků do vnitřní sítě jsou použity nástroje pro správu přístupu technických prostředků.

5. V rámci uspořádání síťových topologií komunikační infrastruktury musí být vždy od sebe vzájemně odděleny segmenty, které jsou určeny pro logické umístění:
   a) Segmentů uživatelských stanic a mobilních zařízení.
   b) Zařízení pro přístup a práci s privilegovanými oprávněními.
   c) Vývojové, testovací a provozní prostředí.
6. Přístupy jsou řízeny v jednotlivých prvcích ICT na základě stanovených skupin a rolí.

12.4. Pravidla a postupy pro ochranu vzdáleného přístupu k síti

1. V rámci vzdáleného přístupu do komunikační sítě musí být pro přenos informací používány prostředky a postupy zajišťující bezpečnost, funkčnost a spolehlivost na základě provedeného hodnocení aktiv a rizik. Pro zajištění dostupnosti a důvěrnosti musí být aplikováno:
2. Vzdálený přístup uživatelů k sítím je řízen prostřednictvím odpovídajících technických prostředků.
3. Vzdálený přístup je možný jen prostřednictvím komunikačního kanálu chráněného kryptografickými prostředky.
4. Musí být evidovány, aktualizovány a spravovány všechny příslušné autentizační prostředky pro vzdálený přístup k síti.
5. Ověření identity žadatele o vzdálený přístup do sítí ISZS je provedeno formou vícefaktorové autentizace.
6. Vzdálený přístup se automaticky ukončí při neaktivitě tohoto přístupu, která je delší než 30 min.
7. Přístup z externích sítí do sítí ISZS je možný jen do demilitarizovaných zón navržených tak, aby případný vnější útok neohrozil bezpečnost interní sítě.
8. Vzdálené připojení dodavatelů je možné jen na základě oboustranné dohody, zakotvené ve smluvním vztahu.

12.5. Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů

1. Komunikační sítě musí obsahovat monitorovací a bezpečnostní prvky, které umožňují včasnou detekci provozního nebo bezpečnostního selhání, popř. chybné funkce její součásti.
2. Všechny síťové prvky musí pravidelně synchronizovat čas.
3. Veškeré síťové prvky, které to umožňují, musí být trvale monitorovány.
4. U sítě ISZS musí být navíc zajištěno:
   - Všechny aktivity, události a informace o provozu jsou zaznamenávány v provozním deníku.
   - U síťových prvků jsou pořizovány provozní záznamy.
   - Záznamy událostí prvků ICT jsou uchovávány nejméně po dobu 24 měsíců.
   - Záznamy událostí jsou zajištěny před neoprávněným přístupem a neoprávněnou modifikací.

13. FYZICKÁ BEZPEČNOST

13.1. Pravidla pro ochranu objektů

Za návrh, realizaci a kontrolu pravidel k zajištění fyzické bezpečnosti objektů je odpovědný pověřený zaměstnanec do role Garanta fyzické bezpečnosti a současně člen Pracovní skupiny kybernetické bezpečnosti v součinnosti s Manažerem KB.

Prostory, ve kterých jsou umístěna podpůrná ICT aktiva (serverovny, místnosti s aktivními prvky atd.), musí být chráněny proti vniknutí nepovolaných osob některým z níže uvedených prostředků a systémů, nebo jejich kombinací:

a) Instalací vhodných mechanických zábranných prostředků, zejména:
   i. mříže,
   ii. závory,
   iii. venkovní rolety,
   iv. bezpečnostní okenní fólie,
   v. zámkové mechanismy,
   vi. vstupní turnikety.

Tyto prostředky musí svou konstrukcí a mechanickou odolností splňovat stanovené bezpečnostní funkce.

a) Instalací elektronických zabezpečovacích systémů, jimiž jsou:
   i. poplachový zabezpečovací a tísňový systém (PZTS),
   ii. elektrická požární signalizace (EPS).

Za pravidelnou kontrolu funkčnosti mechanických zábranných prostředků a za zajištění pravidelných revizí elektronických zebezpečovacích systémů je odpovědný určený Garant fyzické bezpečnosti, který je povinen vést:

a) provozní knihu PTZS, EPS,
b) plán revizí a evidenci revizních zpráv.

13.2. Pravidla pro kontrolu vstupu osob

V hranicích SŘBI jsou stanovena:

a) pravidla pro vstup do objektů pro zaměstnance, návštěvy a dodavatele,
b) pravidla pro vstup osob do objektů:
   i. v pracovní dobu,
   ii. v mimopracovní dobu, ve dnech pracovního volna a pracovního klidu,
c) odpovědné osoby za kontrolu osob vstupujících do objektů v roli recepčních,
d) pravidla pro pohyb osob po budově:
   i. osobám z řad veřejnosti je vstup do kanceláří umožněn pouze v přítomnosti zaměstnanců – uživatelů příslušné kanceláře,
   ii. zaměstnancům je vstup do kanceláří umožněn podle pracovního zařazení, případně výkonu jiných činností, na základě předání klíče od příslušné kanceláře,
   iii. soukromé návštěvy lze na pracovišti přijímat se souhlasem nadřízeného a pouze na dobu nezbytně nutnou,
e) pravidla pro vstup do režimových prostor:
   i. vstup je povolen pouze Garantům podpůrných aktiv, která jsou uložena a provozována v daném režimovém prostoru,
   ii. každý vstup je monitorován a zaznamenán,
   iii. případní dodavatelé ICT služeb mohou vstupovat jen v doprovodu příslušného Garanta podpůrného aktiva.

13.3. Pravidla zabezpečení dokumentů určených ke skartaci a archivaci

Za bezpečnost vyřízených dokumentů po dobu jejich skartační lhůty a dokumentů určených k archivaci odpovídá určený zaměstnanec. Odpovědná osoba a její povinnosti musí být uvedena ve Spisovém a skartačním řádu.

Dokumenty musí být zabezpečeny tak, aby bylo minimalizováno riziko jejich ztráty, krádeže, zničení, poškození nebo zpřístupnění nepovolaným osobám.

Odpovědný zaměstnanec vede:

a) Evidenci uložených dokumentů,

b) Evidenci zapůjčených a vrácených dokumentů.

Dokumenty personální a mzdové povahy a jiné dokumenty obsahující důvěrné informace musí být ukládány odděleně od ostatních uložených dokumentů, a to v uzamykatelných úschovných objektech z nehořlavých materiálů (např. kovové skříně a registratury). Klíčem od tohoto úschovného objektu disponuje pouze odpovědný zaměstnanec, duplikát klíče je uložen v zapečetěném obalu u osoby, která duplikáty klíčů disponuje.

Pokud je k ukládání dokumentů vyhrazena samostatná místnost (spisovna), platí pro ni následující pravidla:

a) Do místnosti má přístup pouze zaměstnanec odpovědný za vedení spisovny. Ostatní zaměstnanci nebo cizí osoby mohou do spisovny vstupovat pouze v doprovodu odpovědného zaměstnance.
b) Zabezpečení vnitřního prostoru spisovny je zajištěno těmito opatřeními nebo jejich kombinací:
   i. PZTS,
   ii. je-li ve spisovně vestavěno okno přístupné např. z přízemí, římsy, balkonu apod.:
   – instalace detektoru tříštění skla,
   – instalace okenní bezpečnostní fólie nebo bezpečnostní mříže,
   iii. kouřové čidlo,
   iv. ruční hasící přístroj.
c) Splnění dalších požadavků dle § 68 odst. 4 vyhlášky č. 645/2004 Sb., kterou se provádí zákon o archivnictví a spisové službě.
d) V případě, že je archivace či skartace zajišťována prostřednictvím dodavatele, platí pro zajištění obou činností pravidla uvedená v **SmGŘ-061 Řízení dodavatelů**. Pravidla se uplatňují přiměřeným způsobem pro daný druh a podmínky poskytované služby.

13.4. Pravidla klíčového režimu (manipulace s klíči, čipy a čipovými kartami)

Za evidenci vydaných přístupových/docházkových čipů je odpovědný pověřený zaměstnanec Oddělení personální a mzdové agendy.

Garant fyzické bezpečnosti odpovídá za naprogramování přístupových oprávnění na čip přidělený zaměstnanci v rozsahu písemného požadavku, schváleného příslušným vedoucím zaměstnancem, který určí rozsah přidělených přístupových oprávnění s ohledem na předpokládanou pracovní náplň zaměstnance.

Za evidenci vydaných klíčů je odpovědný zaměstnanec určený Garantem fyzické bezpečnosti.

Zaměstnancům jsou předávány klíče, čipy a čipové karty oproti podpisu.

Je stanoven režim pořizování, vydávání a ukládání duplikátů klíčů. Duplikáty klíčů jsou ukládány v zapečetěných obalech, opatřeny podpisem odpovědného zaměstnance, případně datem vydání duplikátu klíče a datem opětovného zapečetění obalu s duplikátem klíče. Duplikáty klíčů jsou ukládány v uzamykatelných objektech u stanoveného odpovědného zaměstnance.

V případě existence SHGK je vedena průkazná evidence hlavních a generálních klíčů. Za evidenci přidělených a vrácených klíčů systému SHGK je odpovědný zaměstnanec určený Garantem fyzické bezpečnosti.

13.5. Pravidla úklidu

Garant fyzické bezpečnosti odpovídá za stanovení pravidel úklidu:

a) v pracovní době – zaměstnanec plně odpovídá za jím zpracovávané informace a data BKOM,
b) v mimopracovní době – zaměstnanec musí zajistit uzamčení všech interních případně chráněných dokumentů do úschovných objektů,

c) v režimových prostorech – úklid probíhá pouze za přítomnosti oprávněného zaměstnance.

13.6. Pravidla pro zajištění fyzické bezpečnosti zařízení

Fyzická bezpečnost zařízení je zajištěna těmito opatřeními:

a) Pracovní stanice je vždy umístěna v uzamykatelné místnosti/kanceláři s řízeným přístupem prostřednictvím čipové karty.
b) Je-li vnější strana dveří kanceláře vybavena dveřní koulí, je uživatel kanceláře při jejím krátkodobém opuštění povinen místnost uzavřít, není-li provedena instalace dveřní koule, kancelář se při jejím opuštění uzamyká.
c) Při dlouhodobém opuštění kanceláře nebo po ukončení pracovní doby je zaměstnanec při odchodu povinen zkontrolovat uzavření oken a kancelář uzamknout.

Servery a další důležité technologie, které jsou uloženy v místnostech, musí být zabezpečeny následujícím způsobem:

a) Kancelář je chráněna za pomoci instalace bezpečnostního zámku a kování kategorie RC3 dle ČSN EN 1627.
b) Server je uložen v uzamykatelné rackové skříni.
c) Klíčem od rackové skříně disponuje správce ICT.
d) Kabeláž serveru je chráněna proti poškození.

Servery a další důležité technologie, které jsou uloženy na chodbách či jiných přístupných prostorách, musí být zabezpečeny některým z následujících způsobů:

a) Server je uložen v uzamykatelné rackové skříni.
b) Klíčem od rackové skříně disponuje pouze Garant příslušného podpůrného aktiva.
c) Kabeláž serveru je chráněna proti poškození.
d) V rackové skříni je, dle reálných možností, provedena instalace elektronického zabezpečení, signalizujícího násilné vniknutí do rackové skříně, nebo

K provozování a bezpečnému uchování datových úložišť, serverů a dalších zařízení na podporu IT sítě je vyhrazena samostatná místnost (serverovna).

V serverovně jsou servery a další důležité technologie umístěny výhradně do rackových skříní. Skříně musí být vždy uzamčeny. Odstraňování (bočních a zadních) stěn z rackové skříně je zakázáno, není-li jejich dočasná demontáž nezbytně nutná k provedení servisního zásahu nebo jiného úkonu.

Vstup do serverovny je zajištěn některým z těchto opatření nebo jejich kombinací:

a) instalace bezpečnostního zámku a kování kategorie RC3 dle ČSN EN 1627,
b) instalace mechatronického/elektromechanického zámku s pamětí,
c) instalace jiného elektronického přístupového systému.

Zabezpečení rackové skříně je zajištěno těmito opatřeními nebo jejich kombinací:

a) zajištěním kontroly vstupu,
b) instalací bezpečnostních čidel:
    i. dveřní magnetické čidlo,
    ii. otřesové čidlo,
    iii. teplotní čidlo.

Zabezpečení vnitřního prostoru serverovny je zajištěno těmito opatřeními nebo jejich kombinací:

a) PZTS,
b) kamerový systém (CCTV),
c) je-li v serverovně vestavěno okno přístupné např. z přízemí, římsy, balkonu apod.:
    i. instalace detektoru tříštění skla,
    ii. instalace okenní bezpečnostní fólie nebo bezpečnostní mříže,
d) kouřové čidlo,

e) stabilní hasící zařízení (plynové),
f) ruční hasící přístroj pro hašení elektronických zařízení,
g) uložením kabeláže do krycích lišt.

K zajištění neporuchového a kontinuální provozu zařízení v serverovně je provedena:

a) instalace účinné klimatizace,
b) instalace krátkodobého záložního zdroje elektrické energie UPS,
c) napojení na dlouhodobý záložní zdroj (např. motorgenerátor).

13.7. Detekce narušení fyzické bezpečnosti

V případě detekce narušení objektu, vybaveného PZTS a EZS, musí být vždy zajištěna odpovídající reakce v reálném čase. Toto opatření je zajištěno těmito variantními řešeními, kdy poplachový signál PZTS a EPS je:

a) přenesen na pult centralizované ochrany provozovaný např. Městskou policií, Policií ČR, bezpečnostní agenturou, Hasičským záchranným sborem atd.,
b) přenesen na pracoviště ostrahy objektu, která vyrozumí určeného zaměstnance, který přijme další nezbytná opatření,
c) přenesen dle odst. a) a dále formou notifikace (např. SMS) je vyrozuměn určený zaměstnanec, který přijme další nezbytná opatření.

14. DETEKCE KYBERNETICKÝCH BEZPEČNOSTNÍCH UDÁLOSTÍ

V rámci SŘBI je implementován nástroj pro monitoring, sběr a detekci kybernetických bezpečnostních událostí, který zajišťuje monitoring, sběr a zaznamenávání bezpečnostních a provozních událostí u důležitých aktiv informačního a komunikačního systému a ochranu získaných informací před neoprávněným využitím nebo jejich změnou.

Rozsah monitorovaných aktiv navrhuje Architekt KB v součinnosti s vedoucím oddělení IT, Gestorem primárních aktiv SST, Garantem primárního aktiva ISZS a Garanty podpůrných aktiv.

Nástroj zajišťuje v rámci komunikační sítě, jejíž součástí jsou informační a komunikační systémy SŘBI, STS a ISZS:

a) ověření a kontrolu přenášených dat v rámci komunikační sítě a mezi komunikačními sítěmi;
b) ověření a kontrolu přenášených dat na perimetru komunikační sítě,
c) blokování nežádoucí komunikace.

1. V rámci provozování nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí musí být zaznamenávány tyto události:
   a) datum a čas včetně specifikace časového pásma;
   b) typ činnosti;
   c) identifikace technického aktiva, které činnost zaznamenalo;
   d) jednoznačnou identifikaci účtu, pod kterým byla činnost provedena;
   e) jednoznačnou síťovou identifikaci zařízení původce;
   f) úspěšnost nebo neúspěšnost činnosti.
2. V rámci zaznamenávaných událostí zejména shromažďuje tyto informace:
   a) přihlášení a odhlášení ke všem účtům, a to včetně neúspěšných pokusů;
   b) činnosti provedené administrátory;
   c) úspěšné i neúspěšné manipulace s účty, oprávnění a právy;
   d) neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,

e) činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému,
f) zahájení a ukončení činností technických aktiv,
g) kritické i chybové hlášení technických aktiv a
h) přístupy k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí.

Nástroj musí poskytovat informace, pro určené provozní a bezpečnostní role, o detekovaných bezpečnostních událostech, včetně včasného varování.
Proces řešení kybernetických bezpečnostních událostí a incidentů je dokumentován a řízen v souladu se **SmGŘ-040 Zvládání kybernetických bezpečnostních událostí a incidentů.**
V rámci ISZS musí být zajištěno zpracování a analyzování informací z nástrojů pro detekci kybernetických bezpečnostních událostí. Reakce na ně musí probíhat dle stanoveného procesu.

1. Za účelem neustálého zlepšování musí být prováděna pravidelná kontrola účinnosti nástroje pro detekci kybernetických bezpečnostních událostí a minimálně jednou ročně musí být zpracována analýza informací z nástrojů pro detekci kybernetických bezpečnostních událostí pro VŘKB, která obsahuje oblasti:
   a) optimálnost nastavení procesů detekce kybernetických bezpečnostních událostí;
   b) optimálnost nastavení citlivosti a rozsahu nástrojů detekce kybernetických bezpečnostních událostí;
   c) efektivitu detekce kybernetických bezpečnostních událostí jednotlivých technických opatření;
   d) nastavení uživatelských rolí, práv a pověření;
   e) četnost, periodicitu a nebezpečnost opakujících se bezpečnostních událostí;
   f) dle zjištěných nedostatků navrhuje příslušná a přiměřená bezpečnostní opatření.
2. Na základě výsledků zpracovaných analýz musí být prováděna aktualizace a optimalizace nástroje pro detekci kybernetických bezpečnostních událostí, a to minimálně 1x ročně.
3. Výsledkem kontroly účinnosti procesu nástroje pro detekci kybernetických bezpečnostních událostí je zpráva o účinnosti, která obsahuje zjištění a doporučení pro zlepšení celého procesu. Výsledky účinnosti musí být zohledněny v plánu zvládání rizik KB při plánování na další období.
4. Za optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí je odpovědný Garant primárního aktiva ISZS ve spolupráci s Architektem KB a Manažerem KB.

15. KRYPTOGRAFICKÁ OCHRANA

Úroveň ochrany s využitím kryptografického algoritmu je dokumentována a řízena pro každý prvek ICT. Architekt KB odpovídá za výběr a návrh vhodných kryptografických prostředků.
Úroveň kryptografické ochrany musí být stanovena v odpovídajícím rozsahu v závislosti na posouzení rizik v souladu s bezpečnostními potřebami s ohledem na:

- požadavky na důvěrnost a integritu informací primárních aktiv,
- použití přenosového média,
- typ a sílu kryptografického algoritmu.

V případě, že dojde k prolomení kryptografického algoritmu, tak musí být změněn ve všech systémech, které jej používají.

15.1. Pravidla kryptografické ochrany informací

Pro zajištění důvěrnosti a integrity vybraných aktiv, na základě jejich hodnocení, je nastavena ochrana minimálně na úrovni doporučených kryptografických algoritmů ze strany NÚKIB.

Při výběru algoritmů a vhodných kryptografických technik je vhodné zohledňovat rovněž doporučení uznávaných národních nebo mezinárodních bezpečnostních autorit, publikujících reporty a doporučení.

Před použitím kryptografického programového vybavení musí dojít k jeho schválení v rámci procesu stanového pravidly akvizice, vývoje a údržby.

Architekt KB vede seznam doporučených a aplikovaných kryptografických postupů a technik.

Pro vybrané prvky ICT, dle doporučení Manažera a Architekta KB, jsou používána kryptografická opatření za účelem zajištění, dle technických možností, zejména:

- identifikačních a autentizačních prostředků,
- autorizačních prostředků,
- přenosu informací mezi prvky ICT,
- šifrování souborů,
- zabezpečení elektronické pošty a přístupu k internetu.

Kryptografické ochrany při přenosu informací po komunikačních sítích se řídí prostřednictvím klasifikace informací, které jsou komunikačními sítěmi přenášeny tak, že se použije kryptografická ochrana odpovídající úrovni nejpřísněji klasifikované informace, která je komunikační sítí přenášena.

Opatření kryptografické ochrany informací jsou implementována vždy při přenosu po komunikačních sítích:

- mezi segmenty sítí,
- při přístupu do vnitřní sítě z vnějšího prostředí.

Kryptografické ochrana při uložení informací na mobilní zařízení nebo vyměnitelné technické nosiče dat se řídí klasifikací informací, které jsou na nich ukládány tak, že se použije kryptografická ochrana odpovídající úrovni nejpřísněji klasifikované informace, která je na takové zařízení ukládána.

Opatření kryptografické ochrany informací jsou implementována při uložení souborů na mobilní zařízení nebo vyměnitelné technické nosiče dat a je použita jedna z těchto metod:

- šifrování na úrovni celých disků,
- šifrování na úrovni souborů.

Vedoucí zaměstnanci v součinnosti s vedoucím oddělení VT odpovídají za ochranu šifrováním pevných disků u mobilních zařízení zaměstnanců, včetně notebooků (např. za pomoci BitLockeru, VeraCrypt apod.) vynášených mimo hranice SŘBI.

Vedoucí oddělení VT odpovídá za realizaci kryptografické ochrany v rámci SŘBI, Gestor primárních aktiv STS odpovídá za realizaci kryptografické ochrany v rámci služeb zajišťovaných střediskem a Garant primárního aktiva ISZS za realizaci kryptografické ochrany v rámci ISZS.

15.2. Systém správy klíčů

Správa kryptografických klíčů zahrnuje zejména:

- generování a evidenci klíčů pro různé kryptografické metody a systémy,
- získávání a evidenci certifikátů veřejných klíčů,
- bezpečnou distribuci klíčů uživatelům včetně způsobu jejich aktivace,
- bezpečné uložení klíčů včetně zajištění přístupu pouze oprávněným uživatelům,
- změny a aktualizace klíčů včetně pravidel pro tyto činnosti,
- adekvátní reakce na kompromitace klíčů,

- deaktivace klíčů v případě odchodu zaměstnance nebo kompromitaci klíče.

Pravidla pro správu navrhuje Pracovní skupina KB a schvaluje VŘKB.

16. SOUVISEJÍCÍ DOKUMENTY

16.1. Dokumenty nadpodnikové úrovně

Identifikace zákonných, podzákonných a technických norem souvisejících s realizací bezpečnosti informací

- Zákon č. 89/2012 Sb., Občanský zákoník, v platném znění
- Zákon č. 65/1965 Sb., Zákoník práce, v platném znění
- Zákon č. 121/2000 Sb., o právu autorském, v platném znění
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, v platném znění
- Zákon č. 563/1991 Sb., o účetnictví, v platném znění
- Zákon č. 181/2014 Sb. o kybernetické bezpečnosti, v platném znění
- Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), v platném znění
- EN ISO/IEC 27001:2013 - Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky
- EN ISO/IEC 27002:2022 - Informační technologie – Bezpečnostní techniky – Soubor postupů pro management bezpečnosti informací
- ČSN EN ISO 9001 Systémy managementu kvality – Požadavky
- ČSN EN ISO 14001 Systémy environmentálního managementu – Požadavky s návodem pro použití
- ČSN ISO 45001 Systémy managementu bezpečnosti a ochrany zdraví při práci – Požadavky s návodem k použití
- ČSN 01 0391 Systém managementu společenské odpovědnosti organizací – Požadavky

16.2. Podnikové dokumenty

PIMS-001	Příručka Integrovaného systému řízení
SmGŘ-046	Organizace kybernetické bezpečnosti
SmGŘ-061	Řízení dodavatelů
SmGŘ-042	Bezpečné chování uživatele
SmGŘ-040	Zvládání kybernetických bezpečnostních událostí a incidentů
SmGŘ-041	Řízení kontinuity činností ICT
SmGŘ-035	Ochrana osobních údajů
Mp-GŘ039-01	Metodika analýzy rizik kybernetické bezpečnosti

17. ZÁVĚREČNÁ USTANOVENÍ

17.1. Účinnost

Tato směrnice nabývá účinnosti dnem 01.02.2023.

17.2. Rozdělovník

Zaměstnanci s uživatelským účtem obdrží ON v systému DMS. Zaměstnanci bez tohoto přístupu jsou seznámeni s dokumentací v její listinné podobě, uložené u správce řízené dokumentace.

Bezpečné chování uživatele

(SmGŘ-042)

1. vydání ze dne 26.01.2023 Účinnost ode dne 01.02.2023

Číslo revize	Čísla revidovaných stránek	Zaznamenal a zařadil Jméno	Datum	Podpis
1				
2				
3				
4				
5				

	Odborný garant	Formálně ověřil	Vydavatel	Schválil
Úsek	SŘ	GŘ	SŘ	GŘ
Funkce	Manažer kybernetické bezpečnosti	Správce řízené dokumentace	Předseda výboru pro řízení kybernetické bezpečnosti	Generální ředitel
Jméno	Ing. Igor Prosecký (I3 Consultants s.r.o.)	Ing. Pavel Burian	Ing. Roman Nekula, MBA	Ing. Luděk Borový
Datum	26.01.2023	26.01.2023	26.01.2023	26.01.2023
Podpis				

Obsah směrnice
(SmGŘ-042)

1. ÚVODNÍ USTANOVENÍ

1.1. Účel

Tato směrnice stanoví pravidla bezpečného chování uživatelů v rámci systému řízení bezpečnosti informací BKOM.

1.2. Závaznost

Tento dokument je závazný pro všechny zaměstnance společnosti BKOM a současně pro všechny externí subjekty a jejich zaměstnance, kteří jsou na základě smlouvy oprávněni přistupovat k aktivům BKOM.

1.3. Správa normy

1.3.1. Sběr připomínek a případné změnové řízení zajišťuje odborný garant ON.

1.3.2. Výklad této normy zajišťuje odborný garant.

1.3.3. Metodickou kontrolu dodržování pravidel a zásad této normy zajišťuje odborný garant.

2. VYMEZENÍ POJMŮ

2.1. Použité zkratky

BKOM	Brněnské komunikace, a.s.
DMS	Systém pro správu dokumentů (Document Management System)
HW	Hardware – označuje veškeré fyzicky existující technické vybavení počítače
ICT	Informační a komunikační technologie (Information and Communication Technologies) - označuje veškeré technologie používané pro komunikaci a práci s informacemi
IS	Informační systém. Systém pro sběr, udržování, zpracování a poskytování informací a dat
ISSTS	Informační systém správy telekomunikačních systémů
ISZS	Informační systém základní služby
NTB	Notebook (přenosné zařízení)
ON	Organizační norma
PIN	Osobní identifikační číslo (Personal Identification Number)
SŘBI	Systém řízení bezpečnosti informací
SW	Software (programové vybavení) je v informatice sada všech počítačových programů v počítači – software zahrnuje aplikační software (pracuje s ním uživatel), operační systém (zajišťuje běh programů) a další
VPN	Virtuální privátní síť
VT	Výpočetní technika

2.2. Definice

2.2.1. ***Aktivum***

je jakákoli entita, která má pro jednotlivce nebo organizaci hodnotu, která může být zmenšena působením hrozby. V podmínkách BKOM se typicky jedná např. o informace BKOM, informace a služby poskytované BKOM, ICT prostředky a síťová infrastruktura BKOM, programové vybavení, zaměstnanci a objekty BKOM, dodavatelé ICT služeb pro BKOM apod.

2.2.2. ***Uživatel***
je zaměstnanec BKOM nebo zaměstnanec třetí strany, který má přístup k aktivům SŘBI, obvykle prostřednictvím přiděleného ICT zařízení a přístupového oprávnění.

2.2.3. ***Služební zařízení***
je ICT prostředek, kterým je obvykle pracovní stanice, samostatný počítač, tiskárna, kopírka, scanner a další případná HW zařízení, vždy vybavená potřebným programovým vybavením a přidělená uživateli k plnění pracovních povinností zaměstnavatelem.

2.2.4. ***Přenosné zařízení***
je služební mobilní zařízení. V podmínkách BKOM se obvykle jedná o notebook, tablet, smartphone, čtečka dat apod.

2.2.5. ***Vyměnitelné médium***
je přenosné elektronické paměťové médium (datový nosič), kterým je např. magnetické, optické nebo polovodičové zařízení, které lze vložit nebo připojit k počítačovému zařízení a vyjmout z něj, či odpojit od něj. Slouží k ukládání textových, obrazových a zvukových záznamů a informací. V podmínkách BKOM se obvykle jedná o pevné disky, USB disk, flash disky, externí disky, paměťové karty, CD, DVD).

3. PRAVIDLA PRO BEZPEČNÉ NAKLÁDÁNÍ S AKTIVY

3.1. Uživatelé a jejich aktiva

Uživatelé jsou odpovědní za zabezpečení informací a služeb ve své působnosti, a to zejména za zajištění důvěrnosti, dostupnosti a integrity zpracovávaných informací a poskytovaných služeb.
Bezpečným nakládáním s aktivem je myšlen celý jeho životní cyklus, tj. především přidělení aktiva uživateli, jeho užívání, včetně manipulace a jeho odebrání, evidence a likvidace. Aktivy svěřenými uživateli jsou zejména:

- identifikační a přístupové prostředky sloužící pro přístup do objektů BKOM (např. přístupové čipové karty, klíče od místností a prostor objektu),
- výpočetní technika a mobilní zařízení (např. pracovní stanice, notebook, mobilní telefon, tablet),
- výměnná média (např. USB disk, flash disk, externí disk, paměťové karty, CD, DVD),
- prostředky pro přístup do vnitřní sítě BKOM a k informacím a službám informačních systémů SŘBI (např. uživatelské jméno a přístupové heslo, interní či kvalifikovaný certifikát, VPN token).

3.2. Přidělení aktiv uživateli a jejich evidence

Aktiva jsou uživateli svěřena na základě oprávněné potřeby. Svěřené technické vybavení je evidováno na osobní kartě zaměstnance v případě, že se jedná o hmotný majetek. V případě aktiva, které nepodléhá evidenci v majetku, eviduje dané aktivum příslušný Garant aktiva. Přidělování přístupových oprávnění uživateli se řídí pravidly uvedenými v **SmGŘ – 039 Bezpečnostní politika informací.**

3.3. Bezpečné užívání a manipulace s aktivy

Při manipulaci a správě aktiv musí být dodržována pravidla odpovídající klasifikaci aktiva. Přesná pravidla pro manipulaci s aktivy jsou uvedena v **SmGŘ – 039 Bezpečnostní politika informací.**

Uživatelé jsou povinni se seznámit se všemi bezpečnostními dokumenty, které jsou relevantní pro činnosti, které vykonávají. Přehled dokumentů, se kterými jsou povinny se jednotlivé role seznámit, je uveden v kapitole „9. Související dokumenty“.

4. OBECNÁ PRAVIDLA BEZPEČNÉHO CHOVÁNÍ UŽIVATELE

BKOM je jako zaměstnavatel, z důvodu zajištění kybernetické bezpečnosti, oprávněn k monitoringu užívání informačních a komunikačních technologií na pracovišti prostřednictvím auditních záznamů používaných aplikací, informací o využití elektronické pošty, obsahu zpráv pracovní povahy a statistik navštívených webových stránek zaměstnancem/uživatelem.

Uživatel je povinen:

- vzít na vědomí, že porušení pravidel uvedených v tomto dokumentu může být kvalifikováno jako porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci,
- převzít zodpovědnost za veškeré úkony, skutky a aktivity prováděné pod jemu svěřenými přístupovými oprávněními (přidělené uživatelské jméno a přístupové heslo),
- pro přístup k operačním systémům a aplikacím používat pouze své přidělené přístupové jméno a heslo,
- při prvním přihlášení k aplikacím změnit přidělené výchozí heslo,
- zachovávat jedinečnost a důvěrnost přístupového hesla, tj. nikomu heslo nesdělovat (včetně kolegů, vedoucích zaměstnanců, zaměstnanců oddělení VT apod.), nikde a nijak jej nezaznamenávat. (*Pozn.: zaměstnanec oddělení VT, ředitel, vedoucí zaměstnanec, ani asistentka nepotřebují pro svou práci znát heslo uživatele),*
- zajistit při zadávání přístupového hesla nemožnost jeho odpozorování druhou osobou,
- při přihlašování k aplikacím prostřednictvím webového prohlížeče nevyužívat funkci „zapamatovat heslo“,
- používat instalované programové vybavení pouze k plnění pracovních povinností a v souladu s ním a v souladu s účelem, ke kterému je určeno,
- při používání čipové karty s identifikačním certifikátem nikdy PIN nenechávat veřejně dostupný, ani neponechávat kartu bez dohledu uživatele,
- dodržovat pravidla pro tvorbu přístupového hesla k aplikacím:
  - minimální délka hesla: 12 znaků u standardních účtů,
  - minimální délka hesla: 17 znaků u privilegovaných účtů,
  - heslo musí obsahovat alespoň 3 ze 4 skupin znaků (malá písmena, velká písmena, číslice nebo speciální znaky),
- respektovat a, pokud není automatizovaně vynuceno, dodržovat další pravidla pro použití hesel, kterými jsou zejména:
  - maximální platnost hesla: 12 měsíců,
  - minimální platnost hesla: 24 hodin,
  - historie hesel: 3 hesla,
  - maximální počet neúspěšných pokusů o přihlášení: 5,
  - doba zablokování účtu po neúspěšných pokusech o přihlášení: 30 minut,
  - přístupové heslo do aplikací nesmí obsahovat jméno uživatelského účtu (osobní číslo uživatele),
  - je zakázáno používání osobních údajů uživatele a jiných lehce odhalitelných hesel (jako jsou datum narození, jména členů rodiny, názvy předmětů v blízkosti počítače, běžných jednoduchých slov umožňujících tzv. slovníkový útok, apod),
  - Je zakázáno sdílet stejné přístupové heslo pro více aktiv,

- před opuštěním pracoviště, i krátkodobém (např. na toaletu), zabezpečit zařízení BKOM uzamčením pracovní plochy nebo odhlášením se od zařízení BKOM (např. pomocí kláves ⊞+L nebo ctrl+alt+del),
- dodržovat pravidlo „čistého stolu“, to znamená, že všechny dokumenty obsahující interní nebo chráněné informace, které se v danou chvíli nezpracovávají, jsou uloženy v uzamykatelných skříních,
- v případě jakéhokoliv podezření na kompromitaci hesla nebo jeho zneužití změnit okamžitě heslo a tuto informaci, v případě uživatelů IS SŘBI a ISSTS okamžitě nahlásit vedoucímu zaměstnanci a zapsat do aplikace „Nahlasto“. V případě uživatelů ISZS tuto skutečnost okamžitě zapsat do aplikace HelpDesk ISZS.
- důsledně kontrolovat doručenou elektronickou poštu a v případě podezření, že se jedná o závadný e-mail (podvodný e-mail apod.), takovou zprávu neotvírat a vždy se zamyslet, zda:
  - znám odesílatele, zda působí věrohodně,
  - je text e-mailu srozumitelný,
  - očekávám mail tohoto typu (neznámé faktury, výhry, výzvy bankovních institucí apod.),
  - je odkaz uvedený v mailu shodný s adresou (kontrola najetím myší na odkaz),
  - v případě, že se jedná pravděpodobně o podvodný e-mail, neprodleně tuto skutečnost zapsat do aplikace „Nahlasto“,
- v případě zasílání e-mailů s šifrovanou přílohou předat heslo příjemci jinou cestou (např. telefonicky, SMS apod.). Heslo nikdy nesmí být součástí odesílaného e-mailu. Hesla k jednotlivým souborům se řídí stejnými pravidly jako hesla k uživatelským účtům,
- neprodleně hlásit ztrátu jakéhokoliv přiděleného zařízení, včetně přenosného datového nosiče, vedoucímu zaměstnanci a do aplikace „Nahlasto“,
- ukládat informace na místa určená k zálohování a brát na vědomí, že informace uložené mimo určené adresáře nejsou zálohovány, tj. takové informace nebude možné případně obnovit,
- absolvovat v řádném termínu povinná školení zaměřená na zvyšování bezpečnostního povědomí v oblasti kybernetické bezpečnosti.

Uživatel nesmí:

- instalovat žádné programové vybavení na služební zařízení BKOM,
- stahovat žádné spustitelné soubory z neautorizovaných stránek,
- jakkoli zasahovat do zařízení BKOM a jejich konfigurací,
- připojovat žádné technické vybavení, které mu nebylo svěřeno k užívání v rámci plnění pracovních povinností, včetně vybavení, které umožňuje připojení k vnitřní síti BKOM (např. modemy, switche, huby atd.),
- kopírovat, ukládat, přenášet jakákoliv data BKOM mimo prostory BKOM (mimo povolené postupy popsané ve směrnici **SmGŘ -039 Bezpečnostní politika informací**),
- připojovat k zařízením BKOM jakékoliv soukromé či neznámé datové nosiče (např. CD, flash disky, externí HDD). Výjimku tvoří pouze datové nosiče, předané klienty nebo třetími strany pro účely konkrétního řízení. Tyto nosiče jsou vždy nejdříve prověřeny antivirovým programem a zařízení má v operačním systému vypnutou funkci „Přehrát automaticky“,
- navštěvovat rizikové internetové stránky a klikat na reklamní bannery na webových stránkách a v e-mailech,
- tisknout data z aplikací BKOM pro jiné než pracovní účely a vytištěné dokumenty ponechávat bez dozoru na tiskárně/kopírce,
- pokoušet se vypínat nainstalovaný antivirový systém.

5. PRAVIDLA POUŽÍVÁNÍ SLUŽEBNÍCH A SOUKROMÝCH PŘENOSNÝCH (MOBILNÍCH) ZAŘÍZENÍ

5.1. Pravidla pro ochranu a používání služebních přenosných zařízení

Zaměstnanci mají povoleno vykonávat pracovní činnost mimo objekty BKOM pouze po schválení nadřízeným zaměstnancem.

U přenosných zařízení používaných v SŘBI pro přístup k síti a aplikacím SŘBI musí být dodržena minimálně tato bezpečnostní opatření:

a) pravidelná aktualizace operačního systému zařízení,
b) pravidelná aktualizace antivirového systému zařízení,
c) nastavena tak, aby se po 10 minutách neaktivity uživatele uzamkla, v případě smartphonu a tabletu po 2 minutách neaktivity,
d) nastavena tak, aby uživatel disponoval pouze účtem s oprávněním „standardní uživatel“,
e) smartphony a tablety chráněny 4místným PINem, biometrickým údajem nebo heslem s alespoň 6 znaky,
f) vybaveny pouze schválenými aplikacemi,
g) pevný disk šifrován, pokud to operační systém umožňuje.

Vedoucí oddělení VT odpovídá za nastavení zařízení připojujících se k síti a aplikacím SŘBI dle pravidel uvedených výše.

5.2. Pravidla pro používání soukromých přenosných zařízení

Zaměstnanec bere na vědomí, že převzetím přístupových oprávnění k síti a aplikacím SŘBI přebírá odpovědnost za zajištění minimální úrovně ochrany soukromých zařízení, kterou je povinen při přístupu zajistit.
Soukromá zařízení, jejímž prostřednictvím zaměstnanec přistupuje k síti a aplikacím SŘBI, musí být:

a) Vybavena pravidelně aktualizovaným operačním systémem.
b) Vybavena pravidelně aktualizovanou antivirovou aplikací.
c) Chráněna za pomoci přihlašovacích údajů uživatele, s:
    i. minimální délkou hesla: 8 znaků a
    ii. použití alespoň 3 ze 4 skupin znaků (malá písmena, velká písmena, číslice nebo speciální znaky).
    iii. Nastavena tak, aby se po 5 minutách neaktivity uživatele uzamknula, v případě smartphonu a tabletu po 2 minutách neaktivity.
    iv. Smartphony a tablety chráněny PINem, biometrickým údajem nebo heslem s alespoň 6 znaky.
    v. Vybaveny pouze aplikacemi instalovanými z oficiálních obchodů (např. Google Play, Apple store, Galaxy store apod.).

Při používání přenosných a soukromých zařízení pro připojení k aplikacím SŘBI jsou zaměstnanci povinni:

a) Učinit všechna dostupná opatření, která mohou zabránit ztrátě či odcizení zařízení (neponechávají je bez dohledu a/nebo zabezpečení např. v dopravních prostředcích, v ubytovacích zařízeních apod.).
b) Aktivně zabraňovat odpozorování obrazovky cizí osobou (např. ve vlacích, restauracích, v prostředcích hromadné dopravy apod.).

c) Neumožnit přístup ke zpracovávaným informacím SŘBI jiné osobě, včetně rodinných příslušníků.

Použití soukromých přenosných zařízení pro připojení do sítě BKOM povoluje vždy příslušný ředitel úseku v součinnosti s příslušným Garantem primárního aktiva a Manažerem KB.

5.3. Pravidla pro ochranu a používání výměnných médií (přenosných datových nosičů)

Připojování soukromých přenosných datových nosičů k zařízením BKOM je zakázáno.
Používání zaměstnavatelem přidělených přenosných datových nosičů pro soukromé účely je zakázáno.
Zaměstnavatelem přidělené přenosné datové nosiče jsou evidovány a vhodným způsobem chráněny proti neoprávněnému zpřístupnění cizí osobě (např. šifrováním). Před spuštěním na služebním zařízení jsou zkontrolována antivirovým SW.

6. BEZPEČNÉ CHOVÁNÍ NA SOCIÁLNÍCH SÍTÍCH

V případě, kdy BKOM disponuje vlastním profilem na sociálních sítích, je zajištěno:

a) Přístupovými oprávněními k oficiálnímu profilu disponují pouze oprávnění zaměstnanci určení příslušným ředitelem úseku.
b) Oprávnění zaměstnanci musí být proškoleni ve způsobech administrace profilu a dále pravidlech pro zveřejňování informací.
c) Oprávnění zaměstnanci jsou povinni důsledně ověřovat jakéhokoliv odkazy zasílané prostřednictvím aplikací na sociálních sítích, včetně různých výzev k provedení nějakých činností (např. „Zjistěte, kdo se dívá na váš profil!“ apod.). Takovéto odkazy je zakázáno používat.

Zaměstnancům je zakázáno vytvářet profily na sociálních sítích, které by mohly vzbuzovat dojem, že se jedná o oficiální profily BKOM.
Zaměstnanci nesmí nikdy sdělovat na osobních profilech na sociálních sítích informace pracovní povahy.
Oprávnění zaměstnanci berou na vědomí, že:

- Sociální sítě údaje z profilů nabízejí třetím stranám.
- Vše, co napíší, či vloží do sociální sítě, se stává majetkem provozovatelů sociálních sítí a ve většině případů je nelze vzít zpět.

7. BEZPEČNÉ POUŽITÍ ELEKTRONICKÉ POŠTY

V rámci BKOM je provozována firemní elektronická pošta. Elektronická pošta je uživateli dostupná v programovém vybavení Microsoft Outlook. Uživatelé, kterým byla pro výkon jejich činnosti, na žádost nadřízeného, zřízena uživatelská emailová schránka, k elektronické komunikaci v rámci firmy i mimo ni, musí respektovat tato pravidla:

- elektronická pošta je určena pouze k plnění pracovních povinnost a v souvislosti s nimi,
- při zasílání klasifikovaných informací je povinnost se řídit pravidly uvedenými **v SmGŘ-039 Bezpečnostní politika informací**,
- pro pracovní účely je zakázáno použití soukromých poštovních schránek (včetně přeposílání služebních mailů do těchto soukromých schránek),
- v případě plánované nepřítomnosti, delší než 3 pracovní dny, zapíná uživatel v Microsoft Outlooku volbu automatické odpovědi Mimo kancelář a nastavuje volbu tak,

aby byl případný odesílatel e-mailu informován, že na jeho e-mail nebude v době nepřítomnosti uživatele reagováno, případně doplní, na jaký jiný e-mail je možné se obrátit,
- e-mailové schránky jsou na serveru BKOM,
- o provedení archivní zálohy e-mailové schránky lze požádat prostřednictvím nadřízeného,
- při podezření na závadný e-mail tento neotvírat a ohlásit jej nadřízenému a zapsat tuto bezpečnostní událost do aplikace „Nahlasto“,
- při ukončení pracovního poměru uživatel musí odhlásit uživatelskou e-mailovou adresu ze všech konferencí, aplikací a jiných procedur, které na tuto adresu zasílají e-mailové zprávy.

8. BEZPEČNÉ POUŽITÍ PŘÍSTUPU NA INTERNET

Uživatelé jsou povinni v rámci přístupu na internet dodržovat tato pravidla:
- používat internet zejména pro plnění pracovních činností a v souvislosti s nimi,
- nepoužívat internetové připojení BKOM k nezákonným aktivitám,
- nediskutovat a neukládat na veřejně přístupná úložiště (např. uloz.to) informace klasifikované stupněm důvěrnosti vyšší než veřejné nebo tyto sdílet v sociálních sítích a na diskusních fórech, a to ani v zašifrované formě,
- zakazuje se stahovat spustitelné soubory z nedůvěryhodných zdrojů a navštěvovat webové stránky s rizikovým nebo závadným obsahem jako např. warez fóra.

Pro přístup k internetu pomocí prostředků mimo firemní síť je nutno mít na paměti, že komunikace přes tyto body může být sledována a ovlivňována. Důrazně se doporučuje v takovém případě použití VPN, u mobilních telefonů je nutné zvážit k jakým informačním zdrojům přistupovat. Pro zpracování služebních informací zásadně nelze využívat např. free Wi-Fi v nákupních centrech, hotelích, nádražích apod. K internetu je možné přistupovat i přes hotspot mobilního telefonu.

9. SOUVISEJÍCÍ DOKUMENTY

9.1. Dokumenty nadpodnikové úrovně

Identifikace zákonných, podzákonných a technických norem souvisejících s realizací bezpečnosti informací:

Zákon č. 181/2014 Sb.	o kybernetické bezpečnosti
Vyhláška č. 82/2018 Sb.	o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
ČSN EN ISO 9001	Systémy managementu kvality – Požadavky
ČSN EN ISO/IEC 27001	Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací - Požadavky

9.2. Podnikové dokumenty

PIMS-001	Příručka Integrovaného systému řízení
SmGŘ-039	Bezpečnostní politika informací
SmGŘ-039	Politika bezpečnosti informací
SmGŘ-061	Řízení dodavatelů
SmGŘ-040	Zvládání kybernetických bezpečnostních událostí a incidentů
SmGŘ-041	Řízení kontinuity činností ICT
Mp-GŘ039-01	Metodika analýzy rizik kybernetické bezpečnosti

10. ZÁVĚREČNÁ USTANOVENÍ

10.1. Účinnost

Tato směrnice nabývá účinnosti dnem 01.02.2023.

10.2. Seznam příloh

10.3. Rozdělovník

Zaměstnanci s uživatelským účtem obdrží ON v systému DMS. Zaměstnanci bez tohoto přístupu jsou seznámeni s dokumentací v její listinné podobě, uložené u správce řízené dokumentace.

Směrnice pro správu a uživatele CTD

(SmGŘ-044)

2. vydání ze dne 31.07.2017 Účinnost ode dne 01.08.2017

Číslo revize	Čísla revidovaných stránek	Zaznamenal a zařadil Jméno	Datum	Podpis
1				
2				
3				
4				
5				

	Odborný garant	Formálně ověřil	Vydavatel	Schválil
Úsek	GŘ	GŘ	EŘ	GŘ
Funkce	Manažer IMS	Správce řízené dokumentace	Představitel managementu	Generální ředitel
Jméno	Ing. Pavel Burian	Ing. Pavel Burian	Ing. Ivan Točev, MBA	Ing. Luděk Borový
Datum	31.07.2017	31.07.2017	31.07.2017	31.07.2017
Podpis				

Obsah směrnice
(SmGŘ-044)

1. ÚVODNÍ USTANOVENÍ

1.1. Účel

Tato směrnice definuje postupy a povinnosti zaměstnanců Správního úseku společnosti BKOM.

1.2. Závaznost

1.2.1. Tento dokument je závazný pro všechny zaměstnance Správního úseku společnosti BKOM a současně pro všechny externí subjekty a jejich zaměstnance, kteří jsou na základě smlouvy oprávněni využívat CTD prostředků BKOM.

1.2.2. Veškeré prostředky CTD (HW a SW) jsou určeny výhradně pro plnění pracovních povinností zaměstnanců případně pro potřeby organizace. Ostatní osoby nemají přístup povolen, výjimkou jsou zaměstnanci dodavatelských firem, kteří mohou provádět instalace a servisní zásahy pod dohledem zaměstnanců Správního úseku.

1.2.3. Uživatel nesmí vyvíjet takovou činnost, která by poškozovala prostředky CTD, nebo která by ostatním uživatelům škodila nebo bránila v řádném užívání prostředků CTD.

1.2.4. Zaměstnanec je povinen řádně hospodařit s prostředky CTD a chránit je před ztrátou, poškozením či zničením.

1.2.5. Každý uživatel je odpovědný za všechny úkony provedené na uživatelské stanici a v infrastruktuře CTD, které byly autorizovány jeho jménem a heslem, a to i v případě, že tyto úkony byly provedeny jinou osobou s využitím kompromitace přihlašovacích údajů uživatele.

1.2.6. Porušení jakéhokoliv bodu tohoto dokumentu se považuje zejména za porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci dle zákoníku práce.

1.3. Správa normy

1.3.1. Sběr připomínek a případné změnové řízení zajišťuje odborný garant organizační normy

1.3.2. Výklad organizační normy zajišťuje odborný garant.

1.3.3. Metodickou kontrolu dodržování pravidel a zásad této normy zajišťuje odborný garant.

2. VYMEZENÍ POJMŮ

2.1. Použité zkratky

BKOM	-	společnost Brněnské komunikace a.s.
CTD	-	centrální technický dispečink
DMS	-	systém pro správu dokumentů (Document Management System)
DMZ	-	demilitarizovaná zóna
HW	-	hardware; označuje veškeré fyzicky existující technické vybavení počítače
IMS	-	integrovaný systém řízení
IS	-	informační systém; systém pro sběr, udržování, zpracování a poskytování informací a dat
LAN	-	lokální počítačová síť (Local Area Network)
ON	-	organizační norma (y)
Sw	-	software (programové vybavení) je v informatice sada všech počítačových programů v počítači; software zahrnuje aplikační software (pracuje s nimi uživatel), operační systém (zajišťuje běh programů) a další
WPN	-	virtuální privátní síť

2.2. Definice

2.2.1. CD-ROM
Nepřepisovatelné optické záznamové médium.

2.2.2. CD-RW
Mají všechny vlastnosti jako CD-ROM, navíc však umožňují smazání jejich obsahu a nahrání nového.

2.2.3. Doména
Jednoznačné jméno (identifikátor) počítače nebo počítačové sítě, které jsou připojené do internetu.

2.2.4. DVD-ROM
Digitální optický datový nosič.

2.2.5. DVD-RW
Digitální optický datový nosič pro zápis i čtení.

2.2.6. Firewall
Ochrana počítačové sítě.

2.2.7. Flash disk
Paměťové zařízení, používané převážně jako náhrada diskety. Data se do disku nahrávají přes sběrnici USB.

2.2.8. NTP protokol
Protokol pro synchronizaci vnitřních hodin počítačů.

2.2.9. RAM
Paměť využívaná v počítačích a dalších el. zařízeních.

2.2.10. Server
Zařízení poskytující sítové služby.

2.2.11. Technický specialista
Osoba odpovědná za provoz prostředků CTD.

3. SPRÁVA CTD

3.1. Proces řízení přístupu

3.1.1. Zřízení přístupu

- Personalista na základě podpisu pracovní smlouvy nebo jiné pracovně právní smlouvy zašle emailem na emailové adresy technických specialistů Správního úseku informaci o novém zaměstnanci. Email musí obsahovat tyto informace:
  - jméno a příjmení zaměstnance,
  - pracovní zařazení,
  - termín nástupu.

- Na základě této informace navrhnou techničtí specialisté rozsah oprávnění pro uvedeného zaměstnance a tento návrh zašlou ke schválení řediteli Správního úseku.
- Ředitel následně zváží rozsah přidělených uživatelských oprávnění s ohledem na předpokládanou pracovní náplň zaměstnance a zašle ho zpět technickým specialistům k realizaci.
- Techničtí specialisté následně provedou úpravy nastavení uživatelských oprávnění. Přístupy budou aktivní až ke dni nástupu nového zaměstnance.

3.1.2. Změny uživatelských oprávnění

- Změna uživatelských oprávnění je prováděna na základě žádosti. Žádost zasílá emailem řediteli Správního úseku vedoucí pracovník zaměstnance, jehož se změna uživatelských oprávnění týká.
- Žádost musí obsahovat identifikaci zaměstnance, požadovanou změnu nastavení uživatelských oprávnění, důvod změny a informaci, zda se jedná o trvalou změnu či dočasnou. V případě, že se jedná o dočasnou změnu, žádost musí obsahovat také přesné určení období, po které mají být uživatelská oprávnění změněna.
- Ředitel Správního úseku posoudí a případně schválenou žádost předá technickým specialistům, kteří provedou změnu nastavení uživatelských oprávnění. O změně provedou záznam do evidence uživatelských oprávnění včetně kopie žádosti o změnu nastavení uživatelských oprávnění.
- O změně informují dotčeného vedoucího pracovníka.

3.1.3. Odebrání uživatelských oprávnění

- V případě ukončení pracovněprávního vztahu se společností BKOM zasílá personalista na e-mailové adresy technických specialistů požadavek na odebrání uživatelských oprávnění. Tento požadavek musí obsahovat:
  - jasnou identifikaci zaměstnance,
  - datum, ke kterému mají být uživatelská oprávnění deaktivována a uživatelské účty smazány,
  - případné požadavky na nestandardní opatření (ponechání emailové schránky, ponechání obsahu síťové složky apod.
- V naléhavých případech (zejména při ohrožení bezpečnosti informací apod.) je oprávněn podat žádost o zrušení či pozastavení také vedoucí pracovník zaměstnance, jehož uživatelská oprávnění mají být zrušena nebo bezpečnostní manažer.
- O zrušení či pozastavení platnosti uživatelských oprávnění provedou zaměstnanci záznam do evidence uživatelských oprávnění.

3.1.4. Přidělení, změny a rušení uživatelských oprávnění externích subjektů

- Veškeré přidělení a změny uživatelských oprávnění pro externí subjekty musí být schváleny příslušným ředitelem Správního úseku.
- Žádost a zřízení uživatelských oprávnění externího subjektu je zasílána elektronicky na emailové adresy technických specialistů.
- Přesná definice rozsahu uživatelských oprávnění musí být součástí smlouvy uzavřené mezi externím subjektem a společností BKOM. Změny je možné provádět formou uzavření dodatku ke smlouvě.

- Jakákoli změna uživatelských oprávnění musí být v souladu se smlouvou s externím subjektem. Změny je možné provést pouze na základě žádosti o změnu uživatelských oprávnění externího subjektu.
- V případě ukončení smlouvy s externím subjektem je za zrušení přidělených uživatelských oprávnění osoba odpovědná za uvedený smluvní vztah.
- Techničtí specialisté vedou evidenci přístupů pro externí subjekty.
- V případě ukončení činnosti pro BKOM jsou pracovníci třetích stran povinni vrátit veškeré prostředky ve vlastnictví BKOM, poskytnuté třetí straně k výkonu činnosti.

3.2. Základní bezpečnostní pravidla používání CTD

V rámci používání prostředků CTD a dle technických možností použitých technologií jsou všichni zaměstnanci či externí subjekty a jejich zaměstnanci povinni:

- při využívání CTD pracovat pouze pod jemu přidělenou uživatelskou identitou a dodržovat pravidla používání hesel uvedená v kapitole 5,
- chránit data a prostředky CTD před neoprávněným přístupem nepovolaných osob, před úmyslnými nebo náhodnými změnami, destrukcí nebo únikem dat, bránit jejich zneužití či krádeží.
- zajistit ochranu pracovní stanice nebo jiného zařízení pro zpracování informací tak, aby nemohlo dojít k jejímu zneužití jiným zaměstnancem, případně cizí neoprávněnou osobou. Tato povinnost zahrnuje:
  - uživatel nesmí nechat bez dozoru aktivní stanici nebo jiné zařízení pro zpracování informací,
  - při opuštění pracoviště uzamknout stanici,
  - při odchodu ze zaměstnání se odhlásit od pracovní stanice.
- respektovat pokyny vydávané technickými specialisty ohledem na zajištění bezproblémového provozu CTD,
- nahlásit technickým specialistům jakékoliv podezření na nesprávné fungování stanice, napadení počítačovým virem, případně jakékoli podezření na narušení bezpečnosti CTD,
- zkontrolovat před použitím proti virům antivirovým programem veškerá data z cizích zdrojů a veškerá vyměnitelná média (s důrazem na přepisovatelná média – flash disky, CD-RW, DVD-RW,…).

Při používání prostředků CTD, a pokud to technické možnosti těchto prostředků umožňují, je zaměstnancům společnosti BKOM i externím subjektům a jejich zaměstnancům zakázáno:

- používat jinou, než přidělenou uživatelskou identitu,
- používat hesla v rozporu s Pravidly používání hesel uvedených v Kapitole 3.3.,
- zasahovat do HW a SW konfigurace počítače. Tyto zásahy provádí pouze techničtí specialisté,
- instalovat a spouštět na stanici jakýkoli software bez souhlasu nadřízeného a souhlasu technických specialistů. Instalace HW i SW provádí výhradně technický specialista, uživatel nesmí instalovat jakýkoliv CTD prostředek, za porušování autorského práva SW je v organizaci zodpovědný každý uživatel na přiděleném zařízení IS, který úmyslně autorské právo porušil vlastním jednáním,
- používat nebo ukládat osobní data nebo nelegální obsah (SW, mp3, video) na prostředky CTD ve vlastnictví BKOM.

3.3. Pravidla používání hesel

V případě, že to technické možnosti prostředků CTD umožňují, jsou při používání hesel platná pravidla:

- Technický specialista sděluje uživatelům přístupové informace vhodnou formou (nejlépe ústně), aby nemohlo dojít k jejich zneužití. Heslo si uživatel změní ihned po prvním přihlášení.
- Uživatelé jsou povinni zachovávat mlčenlivost o svých přístupových informacích, aby nemohlo dojít k jejich zneužití. Za zneužití svých přístupových informací odpovídá uživatel, nebo ten, kdo uživateli tuto přístupovou informaci poskytl.
- Všichni uživatelé sítě LAN musí dodržovat následující kritéria pro hesla:
  - udržovat heslo v tajnosti,
  - nezaznamenávat hesla na papír, do souboru nebo do příručních výpočetních prostředků, pokud není uložení provedeno bezpečným způsobem (šifrovaně),
  - měnit heslo pokaždé, kdy je možná kompromitace hesla,
  - heslo nesmí být založeno na skutečnosti, kterou může někdo snadno odhadnout nebo ji získat z osobních informací (jméno, datum narození, telefonní číslo apod.),
  - nezačleňovat hesla do jakýchkoli automatizovaných přihlášení (např. uložená v makru nebo pod funkční klávesou apod.),
  - nesdílet individuálně přidělená hesla,
  - minimální délka hesla je 6 znaků,
  - heslo musí obsahovat alespoň 3 ze 4 dále uvedených skupin znaků:
    - malá písmena bez diakritiky (a – z),
    - velká písmena bez diakritiky (A – Z),
    - číslice (0 – 9),
    - speciální znaky (! @ # $ % & * ( ) =).
  - minimální délka stáří hesla je 1 den,
  - maximální délka stáří hesla je 12 měsíců.

3.4. Dokumentace a provozní postupy

3.4.1. Dokumentace provozních postupů IS

Za celkové řádné vedení provozní (bezpečnostní) dokumentace odpovídá vedoucí střediska 3310, nebo jím pověřená osoba. Záznamy v rámci provozní dokumentace provádějí příslušní správci systémů.

Účelem provozní dokumentace je zaznamenat informace o změnách IS, událostech v jeho provozu a informace, které s provozem IS souvisí. Provozní dokumentace nebo její část může být, je-li to vhodné, vedena pro více IS nebo částí společně.

Tato dokumentace se může vést jak v listinné tak i v elektronické podobě.

Provozní deník

Jedním z důležitých dokumentů provozní dokumentace je Provozní deník tvořený záznamy s následující strukturou:

- datum a čas záznamu,
- název události či informace,
- technologické zařízení,
- popis události či informace,

- autor záznamu,
- jednoznačná identifikace autora (např. Jméno a příjmení, číslo zaměstnance).

Pokud se vyskytne v Provozním deníku záznam týkající se bezpečnosti IS popřípadě událost (incident bezpečnosti informací, bezpečnostní slabina, zjištění pokusu průniku, apod.), která má na tuto oblast dopad, musí být o tomto informován bezpečnostní správce, který rozhodne o dalším postupu.

Provozní dokumentace je dále tvořena:
- záznamy o chybách a nestandardních stavech,
- záznamy o změnách,
- záznamy o kontrolách a auditech,
- záznamy o bezpečném mazání a likvidaci médií,
- kontaktními informacemi na subjekty spojené se správou a provozem zařízení.

3.4.2. Záznamy o činnostech a zásazích na serverech

Každý server musí mít založen provozní deník, do kterého se budou zaznamenávat všechny zásahy a změny, které byly na serveru provedeny, a to jak z hlediska HW i z hlediska SW.
Každý záznam musí obsahovat následující údaje:
- datum a čas přihlášení,
- jméno osoby provádějící zásah,
- druh zásahu a jeho popis,
- případné poznámky a komentáře k zásahu.

Záznam vždy provede zaměstnanec, který změnu na serverech prováděl.

Pokud se vyskytne v provozním deníku záznam týkající se bezpečnosti IS popřípadě událost (incident bezpečnosti informací, zjištění pokusu průniku, apod.), která má na tuto oblast dopad, musí být o tomto informován bezpečnostní správce, který rozhodne o dalším postupu.

3.4.3. Sledování a audit síťových služeb a serverů

Na řadiči domény je nastaveno logování následujících událostí:
- lokální přihlášení úspěšné/neúspěšné,
- management uživatelských skupin a účtů úspěšné/neúspěšné,
- změny politik úspěšné/neúspěšné,
- privilegované operace úspěšné/neúspěšné,
- systémové události úspěšné/neúspěšné.

Dále může být na požadavek garanta logován přístup ke konkrétním souborům a adresářům.

Logovací soubory budou na serverech uchovávány po dobu 30 dní, poté budou přesunuty na centrální úložiště logovacích souborů, kde budou uchovány po dobu minimálně 6 měsíců. Archivaci logovacích souborů provádí bezpečnostní správci jednotlivých serverů.
Bezpečnostní správci jednotlivých serverů jsou povinni nejpozději jednou za 14 dní provést vyhodnocení logů serveru a v případě zjištění podezřelých záznamů ihned provést prošetření situace.

3.4.4. Pravidla pro posouzení nového IS, akceptace nového IS

Při výběru nového informačního systému musí daný IS splňovat z hlediska bezpečnosti následující požadavky:

- musí umožňovat členit uživatele dle rolí a přístupových práv do skupin,
- musí vyžadovat uživatelské jméno a heslo,
- musí mít možnost vynucení délky, složitosti, maximálního a minimálního stáři hesla,
- musí mít nástroj na prověření konzistentnosti databází,
- musí obsahovat nástroj na automatické zálohování databází,
- musí logovat vybrané uživatelské a všechny privilegované funkce.

Při plánování nasazení nového IS musí být vyhodnoceny požadavky nového IS na hardware a v případě zjištění nedostatečných parametrů stávající infrastruktury musí být před nasazením takového IS naplánována a provedena změna parametrů infrastruktury.

3.4.5. Údržba sítě LAN

Údržba počítačové sítě (HW i SW) je prováděna technickými specialisty, kteří provádí údržbu podle pokynů dodaných výrobci jednotlivých komponentů sítě nebo podle pokynů dodaných výrobci jednotlivých programových produktů.

3.5. Politika užívání síťových služeb

Uživatelé musí mít povolen přístup pouze ke službám, k jejichž užití byli oprávněni.

Interní komunikační infrastruktura musí být oddělena od jiných sítí, zejména od veřejných prostředí (Internet apod.). Povolené výjimky musí být řádně dokumentovány a ověřovány a musí být schváleny bezpečnostním manažerem. Povolené výjimky musí poskytovat dostatečné záruky a být řešeny tak, že jejich prostřednictvím nedojde k narušení systému řízení přístupu.

3.5.1. Autentizace uživatele externího připojení

Vzdálený přístup uživatele je realizován prostřednictvím VPN spojení nebo tenkého klienta vždy šifrovaným komunikačním kanálem.

Součástí předání vzdáleného přístupu k síti je i předání přístupového certifikátu a hesla uživateli, pomocí kterého se uživatel autentizuje prostředkům vzdáleného přístupu. Pro toto heslo platí stejné podmínky jako pro běžná uživatelská hesla.

3.5.2. Autentizace síťových připojení

Pro autentizaci připojení z konkrétního zařízení je zajištěna automatická identifikace zařízení pomocí certifikátu a šifrovacího klíče. Tento certifikát a klíč je generován pro každé zařízení jako jedinečný a nesmí být použit na žádném jiném zařízení. Použití terminálů pro více uživatelů je zakázáno.

3.5.3. Ochrana portů pro vzdálenou diagnostiku a konfiguraci

Fyzický přístup k aktivním síťovým zařízením musí být zabezpečen tak, aby k těmto zařízením měli přístup pouze odpovědní techničtí specialisté.

Logický přístup k portům musí být povolen pouze z vybraných pracovních stanic (administrátorské stanice, dohledové servery), přičemž komunikace musí být zabezpečena pomocí šifrování (ssh, https…). Vlastní nastavení provádí techničtí specialisté.

3.5.4. Princip oddělení v sítích, řízení směrování sítě

Interní informační infrastruktura (síť LAN) je oddělena pomocí firewallu od DMZ, DMZ je následně oddělena firewallem od veřejné sítě (internet).

Komunikace mezi jednotlivými zónami je směrována a omezena tak, aby byla na nejmenší možnou míru eliminována možnost neoprávněného přístupu ke službám a částem IS.

Veškerá povolená komunikace přes firewally (povolené porty, cílové/zdrojové IP adresy) je evidována na CTD.

3.5.5. Identifikace zařízení v sítích

Pro autentizaci připojení ze specifické lokality nebo specifického zařízení musí být zajištěna automatická identifikace zařízení. Použití terminálů pro více uživatelů je zakázáno, případné výjimky musí být dokumentovány a schváleny vlastníkem aktiva, ke kterému se tímto terminálem přistupuje.

Identifikátor zařízení musí jasně definovat, ke které síti může být zařízení připojeno.

3.6. Řízení služeb poskytovaných třetími stranami

3.6.1. Ochrana informací při styku se třetími stranami

Třetí strany, které pracují s daty a informacemi BKOM, se musí smluvně zavázat k zajištění ochrany informací. Požadavky na zajištění ochrany informací se zapracovávají do textu smlouvy, jsou součástí dodatku smlouvy nebo jsou zpracovány formou samostatné smlouvy. Ve smlouvách s dodavateli musí být vždy uplatněny bezpečnostní požadavky stanovené v bezpečnostní politice informací a bezpečnostní dokumentaci informačního systému. Smlouvy jsou před uzavřením posouzeny bezpečnostním správcem.

3.6.2. Smlouva se třetí stranou

Zaměstnanec odpovědný za uzavření smlouvy s třetí stranou uvádí do smlouvy následující:

- závazek dodržovat povinnosti vyplývající z ISMS,
- závazek třetí strany ochránit informace poskytované v rámci plnění smluvního vztahu.

Smlouva řešící přístup externí strany k informacím nebo do zabezpečených oblastí je před uzavřením schválena představitelem vedení BKOM.¨

3.6.3. Sledování a vyhodnocování služeb poskytovaných třetí stranou

Služby poskytované třetími stranami musí být pravidelně (průběžně) monitorovány a kontrolovány. Jsou hodnoceny následující požadavky:

- monitoring úrovně kvality služeb poskytovaných třetí stranou, kontrola shody se smlouvou,
- evidence incidentů bezpečnosti informací, jejich kontrola pracovníky Správního úseku i třetí stranou podle podmínek ve smlouvě,

- řešení a řízení všech identifikovaných problémů.

3.6.4. Řízení změn služeb poskytovaných třetí stranou

Změny v poskytování služeb třetí stranou musí být smluvně ošetřeny.

Každé změně musí předcházet analýza, kde jsou brány v úvahu informace jako kritičnost produkčních systémů, odhady rizik atd.

Tyto změny řídí techničtí specialisté ve spolupráci s ředitelem Správního úseku a garantem aktiva (jedná se o stejný postup jako v případě pořizování služeb, popřípadě uzavírání smluv).

3.7. Mobilní výpočetní prostředky a práce na dálku

3.7.1. Mobilní výpočetní prostředky a komunikace

Současné připojení mobilních výpočetních prostředků do vnitřní sítě a do veřejných sítí je zakázáno.

Pro zabezpečení mobilních výpočetních prostředků je stanoveno následující:

- prostředky musí být vybaveny vlastním programovým vybavením zajišťujícím antivirovou ochranu a ochranu před škodlivými programy (spyware, atd.). Konfigurace tohoto programového vybavení musí zajistit provedení automatické aktualizace při každém připojení do veřejné sítě,
- zabezpečení neveřejných informací klasifikačního stupně „citlivé informace“ kryptografickými prostředky (vhodné se jeví využívat minimálně standardní kryptografický prostředek zabudovaný v operačním systému - MS Windows XP).

3.7.2. Práce na dálku

Práce na dálku je povolena pouze pro specifické skupiny zaměstnanců v odůvodněných případech.
Zaměstnanci je možné zřídit vzdálený přístup do sítě BKOM na základě schváleného Protokolu o předání vzdáleného.
Žádost zaměstnance o přidělení vzdáleného přístupu posuzuje a schvaluje ředitel správního úseku.
Vzdálený přístup do sítě zřizuje a eviduje technický specialista.
Vzdálený přístup do sítě přes Internet musí být chráněn šifrováním přenášených dat.

4. SOUVISEJÍCÍ DOKUMENTY

4.1. Dokumenty nadpodnikové úrovně

ČSN EN ISO 9001	Systémy managementu kvality – Požadavky
ČSN EN ISO 14001	Systémy environmentálního managementu – Požadavky s návodem pro použití
ČSN ISO 45001	Systémy managementu bezpečnosti a ochrany zdraví při práci – Požadavky s návodem k použití
ČSN ISO/IEC 27001	Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky

4.2. Podnikové dokumenty

PIMS-001	Příručka Integrovaného systému řízení
SmGŘ-039	Bezpečnostní politika informací
OŘ-ŘD 001	Organizační řád

4.3. Vystavené dokumenty

Nejsou.

5. ZÁVĚREČNÁ USTANOVENÍ

5.1. Účinnost

Tato směrnice nabývá účinnosti dnem 01.08.2017.
Tímto vydáním ON se ruší veškerá předchozí vydání a úpravy.

5.2. Seznam příloh

Přílohy nejsou.

5.3. Rozdělovník

Zaměstnanci s uživatelským účtem obdrží ON v systému DMS. Zaměstnanci bez tohoto přístupu jsou seznámeni s dokumentací v její listinné podobě, uložené u správce řízené dokumentace.

Organizace kybernetické bezpečnosti

(SmGŘ-046)

1. vydání ze dne 26.01.2023 Účinnost ode dne 01.02.2023

Číslo revize	Čísla revidovaných stránek	Zaznamenal a zařadil Jméno	Datum	Podpis
1				
2				
3				
4				
5				

	Odborný garant	Formálně ověřil	Vydavatel	Schválil
Úsek	SŘ	GŘ	SŘ	GŘ
Funkce	Manažer kybernetické bezpečnosti	Správce řízené dokumentace	Předseda výboru pro řízení kybernetické bezpečnosti	Generální ředitel
Jméno	Ing. Igor Prosecký (I3 Consultants s.r.o.)	Ing. Pavel Burian	Ing. Roman Nekula, MBA	Ing. Luděk Borový
Datum	26.01.2023	26.01.2023	26.01.2023	26.01.2023
Podpis				

Obsah směrnice

(SmGŘ-046)

1. ÚVODNÍ USTANOVENÍ

1.1. Účel

Tento dokument stanovuje základní pravidla organizace kybernetické bezpečnosti společnosti Brněnské komunikace a.s., a stanovení působnosti určených orgánů a bezpečnostních rolí v rámci systému řízení bezpečnosti informací.
Pravidla stanovená tímto dokumentem obsahují postupy, které vycházejí z požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), navazující vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) a bezpečnosti informací, zejména dle ČSN EN ISO/IEC 27001.

1.2. Závaznost

Tato směrnice je závazná pro všechny zaměstnance společnosti a třetí strany, mající přístup k aktivům společnosti.

1.3. Správa normy

1.3.1. Sběr připomínek a případné změnové řízení zajišťuje odborný garant ON.

1.3.2. Výklad této normy zajišťuje odborný garant.

1.3.3. Metodickou kontrolu dodržování pravidel a zásad této normy zajišťuje odborný garant.

2. VYMEZENÍ POJMŮ

2.1. Použité zkratky

BKOM	Brněnské komunikace a.s.
DMS	Systém pro správu dokumentů (Document Management System)
GovCERT/CSIRT	Speciální vládní skupina zabývající se poskytováním bezpečnostních rad (Government Computer Emergency Response Team)/Skupina pro reakci na počítačové bezpečnostní události (Computer Security Incident Response Team)
GŘ BKOM	Generální ředitelství Brněnských komunikací a.s.
ICT	Informační a komunikační technologie (Information and Communication Technologies). Označuje veškeré technologie používané pro komunikaci a práci s informacemi.
IMS	Integrovaný systém řízení
ISSTS	Informační systém správy telematických systémů
ISZS	Informační systém základní služby
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OD SMB	Odbor dopravy Statutárního města Brna
ON	Organizační norma(y)
PS KB	Pracovní skupina kybernetické bezpečnosti
SŘBI	Systém řízení bezpečnosti informací
STS	Správa telematických systémů

VoKB	Vyhláška č. 82/2018 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)
VŘKB	Výbor pro řízení kybernetické bezpečnosti
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

2.2. Definice

2.2.1. ***Systém řízení bezpečnosti informací***
je podmnožinou integrovaného systému řízení (IMS) s jasně vymezenými hranicemi, ve kterých se uplatňují aplikovatelná pravidla a požadavky ČSN EN ISO/IEC 27001 a přiměřeně pravidla a požadavky ZoKB a VoKB a dalších souvisejících právních předpisů, v rozsahu stanoveném řízenou dokumentací.

2.2.2. ***Informační systém správy telematických systémů***
je specifickou podmnožinou SŘBI s jasně vymezenými hranicemi v rámci střediska správy telematických systémů, ve kterých se přiměřeně uplatňují pravidla a požadavky ZoKB a VoKB a dalších souvisejících právních předpisů.

2.2.3. ***Informační systém základní služby***
je podmnožinou SŘBI a jeho rozsah je stanoven rozsahem základní služby „Činnost subjektu odpovědného za kontrolu řízení provozu.“ Základní služba je vymezena činnostmi souvisejícími s centrálním řízení dopravy prostřednictvím světelných signalizačních zařízení. V informačním systému základní služby se striktně uplatňují veškerá pravidla a požadavky ZoKB a VoKB a dalších souvisejících právních předpisů.

3. ORGANIZAČNÍ BEZPEČNOST A BEZPEČNOSTNÍ ROLE

3.1. Organizační struktura systému řízení bezpečnosti informací

Nejvyšším orgánem v organizační struktuře systému řízení bezpečnosti informací BKOM je Výbor pro řízení kybernetické bezpečnosti. Generální ředitel společnosti určuje svým písemným Rozhodnutím jmenovité složení Výboru pro řízení kybernetické bezpečnosti i Pracovní skupinu kybernetické bezpečnosti a dále role Manažera KB, Architekta KB a Auditora KB, včetně jejich zástupců.
Výbor pro řízení kybernetické bezpečnosti určuje Garanty primárních a podpůrných aktiv a významné dodavatele.

3.2. Výbor pro řízení kybernetické bezpečnosti

Výbor pro řízení kybernetické bezpečnosti odpovídá za celkové řízení a rozvoj systému řízení bezpečnosti informací BKOM.
Jednání Výboru se mohou zúčastnit, v případě potřeby, i další osoby. Tyto osoby nemají hlasovací právo a mají pouze poradní hlas.
Výbor se pravidelně schází zpravidla min. jednou za 3 měsíce, nebo dle potřeby, přičemž zápis z jednání Výboru je ukládán u Předsedy Výboru a Manažera KB.

Výbor ve své působnosti odpovídá zejména za:

a) řízení a rozvoj kybernetické bezpečnosti v rámci povinné osoby (informačního systému základní služby) a celého systému řízení bezpečnosti informací BKOM;
b) tvorbu rámce kybernetické bezpečnosti zahrnující stanovení strategických, dlouhodobých i krátkodobých cílů v oblasti kybernetické bezpečnosti, jejich prosazování a směřování rozvoje kybernetické bezpečnosti dle aktuálních hrozeb a potřeb;
c) definici rolí a odpovědností v rámci systému řízení bezpečnosti informací;
d) definici požadavků na podávání zpráv a kontrolu systému řízení bezpečnosti informací.

Mezi klíčové činnosti VŘKB patří zejména:

a) kontrola aktuálního stavu kybernetické bezpečnosti v rámci povinné osoby a zjišťování, zda dochází k naplňování plánovaných cílů;
b) řízení dodavatelů ISZS;
c) projednání legislativních dopadů v oblasti kybernetické bezpečnosti na SŘBI a vydání potřebných stanovisek a opatření;
d) schválení zásad, pravidel, rozsahu a způsobu implementaci bezpečnostních opatření SŘBI;
e) stanovení povinností a odpovědností jednotlivých bezpečnostních rolí systému řízení bezpečnosti informací, včetně jejich aktualizací a u vybraných rolí, včetně návrhů jejich personálního obsazení a zastupitelnosti;
f) určení Garantů primárních aktiv;
g) stanovení a kontrola postupů při předávání působnosti jednotlivých bezpečnostních rolí SŘBI;
h) pravidelné přezkoumání a vyhodnocení systému řízení bezpečnosti informací, vzhledem k naplňování stanovených cílů s projednáním a schválením opatření ke zlepšení a nápravě;
i) příprava, schválení a předložení vedení BKOM zprávy o stavu kybernetické bezpečnosti BKOM s návrhy opatření;
j) plánování a řízení auditu systému řízení bezpečnosti informací, a to s frekvencí minimálně jednou za 2 roky nebo při významných změnách, v rozsahu těchto změn;
k) řízení rizik;
l) schvalování a aktualizace Plánu zvládání rizik;
m) schvalování závěrů z řešení bezpečnostních událostí a incidentů;
n) projednávání plánů testování zranitelností, které předkládá ke schválení GŘ BKOM. Plán testování zranitelností ISZS předkládá GŘ BKOM ke schválení OD SMB;
o) projednávání a schvalování návrhu bezpečnostní architektury bezpečnosti informací;
p) prosazování požadavků na kybernetickou bezpečnost do procesů nákupu a implementace technických a programových prostředků.

Práva VŘKB:

a) vyžadovat součinnost od všech zaměstnanců v SŘBI;
b) přizvat další osoby na zasedání VŘKB;
c) rozhodnout o zrušení přístupu k aktivům;
d) vyžádat v případě potřeby mimořádný audit KB;
e) jednat jménem BKOM s významnými dodavateli i dodavateli v oblasti kybernetické bezpečnosti;
f) projednání a schvalování výjimek ze stanovených pravidel v oblasti kybernetické bezpečnosti, včetně stanovení jejich platnosti.

3.3. Pracovní skupina kybernetické bezpečnosti:

Pracovní skupina kybernetické bezpečnosti je výkonný orgánem Výboru pro oblast kybernetické bezpečnosti u BKOM. Na jednání Pracovní skupiny mohou být přizvány, v případě potřeby, další osoby. Pracovní skupina se schází dle potřeby a svolává ji Manažer KB.

Pracovní skupina ve své působnosti odpovídá zejména za:

a) přípravu podkladů pro jednání Výboru;
b) přípravu návrhů bezpečnostní architektury SŘBI;
c) návrh bezpečnostních opatření SŘBI, včetně zásad, pravidel, způsobu a rozsahu jejich implementace;
d) tvorbu a aktualizaci rozsahu odpovědnosti dodavatelů ICT služeb, sloužícího jako základní podklad pro řízení dodavatelů;
e) návrhy úrovně poskytovaných ICT služeb;
f) řešení kybernetických bezpečnostních událostí a incidentů;
g) projednání aktuálních zranitelností s cílem posoudit jejich relevantnost a možné dopady.

Mezi klíčové činnosti Pracovní skupiny KB patří zejména:

a) sledovat a analyzovat aktuální stav bezpečnostních potřeb v oblastech:
   - řízení provozu a komunikací,
   - řízení přístupových oprávnění,
   - řízení kontinuity činností,
   - fyzické bezpečnosti,
   - správě a ověřování identit,
   - ochrany před škodlivým kódem,
   - zaznamenávání událostí,
   - detekce, sběru a vyhodnocování kybernetických bezpečnostních událostí,
   - aplikační bezpečnosti,
   - kryptografické ochrany;
b) navrhovat přiměřená bezpečnostní opatření;
c) plánovat a koordinovat implementaci bezpečnostních opatření.

Práva Pracovní skupiny KB:

a) vyžadovat součinnost od všech zaměstnanců v SŘBI;
b) přizvat další osoby na zasedání PS KB;
c) vyžádat v případě potřeby mimořádný audit KB;
d) požadovat provedení testování zranitelností u vybraných primárních aktiv;
e) navrhovat a požadovat po VŘKB provedení změn v požadavcích na úroveň a kvalitu poskytovaných ICT služeb;
f) navrhovat výjimky ze stanovených pravidel v oblasti kybernetické bezpečnosti, včetně zrušení přístupu k aktivům a předkládat je VŘKB k projednání.

3.4. Bezpečnostní role

Pro řízení systému řízení bezpečnosti informací jsou zavedeny následující bezpečnostní role:

i. Manažer KB,

ii. Architekt KB,
iii. Garant primárního aktiva,
iv. Garant podpůrného aktiva,
v. Gestor primárních aktiv správy telematických systémů
vi. Auditor KB,
vii. Administrátor,
viii. Uživatel.

3.5. Práva a povinnosti bezpečnostních rolí

*3.5.1. **Manažer KB***

Manažer KB je odpovědný za řízení systému řízení bezpečnosti informací a je hlavní řídící prvek systému řízení bezpečnosti informací u BKOM.

Manažer KB ve své působnosti odpovídá zejména za:

a) tvorbu, úpravy a revize dokumentace systému řízení bezpečnosti informací;
b) zajištění a řízení procesu řízení aktiv a rizik;
c) zpracování a předkládání Zpráv o hodnocení aktiv a rizik, Plánu zvládání rizik a Prohlášení o aplikovatelnosti Výboru pro řízení kybernetické bezpečnosti;
d) návrhy vhodných bezpečnostních opatření, v součinnosti s Architektem KB, a po jejich schválení za metodické řízení jejich implementace, kontrola, vyhodnocení a návrh opatření ke zlepšení a vyhodnocování vhodnosti a účinnosti bezpečnostních opatření;
e) přípravu a projednání pravidelných hlášení o stavu kybernetické bezpečnosti pro vedení BKOM;
f) poskytnutí metodické pomoci a podpory pro zajištění bezpečnosti informací při vytváření, hodnocení, výběru, řízení a ukončení dodavatelských vztahů v oblasti ICT;
g) komunikaci s GovCERT/CSIRT;
h) reakci na opatření vydané NÚKIB, neprodleně projednat jejich obsah s Architektem KB a další příslušnými bezpečnostními rolemi. V případě potřeby svolává VŘKB a Pracovní skupinu KB;
i) řízení vyšetřování a zvládání bezpečnostních událostí a incidentů v rámci SŘBI.

Manažer KB je dále povinen:

a) zajišťovat a koordinovat provedení posouzení rizik systému řízení bezpečnosti informací alespoň 1x za rok nebo vždy v případech významných změn systému řízení bezpečnosti informací;
b) řídit realizaci nápravných opatření systému řízení bezpečnosti informací;
c) vést evidenci významných dodavatelů;
d) monitorovat zveřejněné hrozby a zranitelnosti. Následně, v součinnosti s Architektem KB, zpracovat jejich analýzu a doporučení pro další postup, doporučení postoupit k projednání VŘKB a Pracovní skupině;
e) v součinnosti s Architektem KB předkládat Výboru k projednání bezpečnostní požadavky na nově pořizované informační a komunikační systémy;
f) zajistit hlášení na NÚKIB v případě kybernetického bezpečnostního incidentu v ISZS;
g) zajistit předání odpovědností v případě ukončení nebo změny pracovního poměru Architekta kybernetické bezpečnosti a Garantů aktiv;

h) v případě ukončení a předání bezpečnostní role Manažera KB je povinen předat svému nástupci minimálně následující:
   i. veškerou aktuální dokumentaci k řízení aktiv a rizik, včetně aktuálního Plánu zvládání rizik,
   ii. evidenci bezpečnostních událostí a incidentů,
   iii. zprávy z auditů kybernetické bezpečnosti,
   iv. aktuální Zprávu o přezkoumání systému řízení bezpečnosti informací,
   v. Prohlášení o aplikovatelnosti,
   vi. dokumentaci k řízení dodavatelů, včetně Evidence identifikovaných významných dodavatelů,
   vii. aktuální přehled plánovaných významných změn,
   viii. Předání a převzetí role Manažera KB se hlásí písemně Předsedovi Výboru a GŘ BKOM.

Práva Manažera KB:
a) vyžádat si zasedání Výboru;
b) vyžádat si provedení mimořádného auditu nebo kontroly shody;
c) vyžádat zrušení přístupu k aktivům;
d) přizvat další osoby na zasedání Výboru;
e) vyžádat si nezbytnou součinnost od příslušných vedoucích a ostatních zaměstnanců;
f) vyžádat si metodickou pomoc a podporu od NÚKIB.

Manažer KB nemůže současně vykonávat role odpovědné za provoz informačního a komunikačního systému a další řídící či provozní role.

Manažer KB musí splňovat kvalifikační předpoklady stanovené VoKB rozsahem znalostí, zkušeností, vzděláním a certifikací.

*3.5.2. **Architekt KB***

Architekt KB je odpovědný za návrh a zajištění implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura.

Architekt KB ve své působnosti odpovídá zejména za:
a) analýzu architektury SŘBI, jeho jednotlivých komponent, včetně vzájemných vazeb a za tvorbu a údržbu procesně-organizačního a aplikačního modelu architektury bezpečnosti informací;
b) monitoring a analýzu možných dopadů aktuálních hrozeb a zranitelností, zveřejňovaných NÚKIB a dalšími odbornými fóry;
c) provádění kontrol, hodnocení a testování funkčnosti zavedených bezpečnostních opatření;
d) vytváření testovacích postupů a odpovídajících kritérií jejich akceptace;
e) definici bezpečnostních požadavků na návrh, vývoj, testování a implementaci nových informačních a komunikačních systémů a změnu stávajících;
f) tvorbu a aktualizaci rozsahu odpovědností dodavatelů ICT služeb.

Architekt KB je dále povinen:

a) zajišťovat architekturu bezpečnosti s cílem zajištění bezpečnosti primárních aktiv, tj. jejich důvěrnosti, dostupnosti a integrity;
b) posuzovat zajištění bezpečnosti prvků, které tvoří podpůrná aktiva ve vazbě na primární aktiva;
c) určovat klíčové podmínky, principy a modely architektury informačních a komunikačních systémů, posuzovat a vybírat technologie a stanovovat koncepci bezpečnostního rozvoje informačních a komunikačních systémů;
d) řídit, koncepčně vést a VŘKB předkládat ke schválení bezpečnostní architekturu informačních a komunikačních systémů včetně podpůrných technických aktiv;
e) definovat požadavky na nástroje pro zajištění technických opatření kybernetické bezpečnosti;
f) vytvářet a udržovat model architektury kybernetické bezpečnosti (procesní model, aplikační architekturu, technologie atd.);
g) VŘKB navrhovat změny architektury kybernetické bezpečnosti;
h) předkládat návrh implementace technických opatření;
i) navrhovat a optimalizovat opatření a procesy řešení bezpečnostních událostí a incidentů;
j) spolupracovat s Manažerem KB a předkládat návrhy změn bezpečnostní dokumentace SŘBI;
k) dohlížet na implementaci bezpečnostních opatření;
l) ve spolupráci s Manažerem KB a Garanty aktiv navrhovat opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu;
m) poskytovat součinnost dalším bezpečnostním rolím;
n) spolupracovat na zajištění trvalé ochrany aplikací a informací informačních a komunikačních systémů dostupných z vnější sítě;
o) spolupracovat při aplikaci používání kryptografických prostředků a systému správy klíčů.

Práva Architekta KB:

a) vyžádat si zasedání Pracovní skupiny KB;
b) navrhnout provedení testování zranitelností u vybraného informačního nebo komunikačního systému;
c) požádat VŘKB o zrušení přístupu k aktivům;
d) přizvat další osoby na zasedání Pracovní skupiny KB;
e) vyžádat si nezbytnou součinnost od příslušných zaměstnanců a Garantů primárních a podpůrných aktiv.

Architekt KB nemůže současně vykonávat role odpovědné za provoz informačního a komunikačního systému.

Architekt KB musí splňovat kvalifikační předpoklady stanovené VoKB rozsahem znalostí, zkušeností, vzděláním a certifikací.

3.5.3. Garant primárního aktiva

Garant primárního aktiva je odpovědný za zajištění rozvoje, použití a bezpečnosti svěřeného primárního aktiva.

Garant primárního aktiva ve své působnosti odpovídá zejména za:

a) definici určení účelu informačního nebo komunikačního systému, resp. svěřeného primárního aktiva a návrhy podmínek jeho provozování a užívání, včetně stanovení závazných parametrů;
b) schvalování a řízení přístupu k aktivu, v případě primárního aktiva zajišťujícího provoz ISZS a ISSTS;
c) návrh rozsahu a způsobu řízení přístupu k svěřenému primárnímu aktivu a podpůrným aktivům, na kterých je primární aktivum závislé.
d) hodnocení svěřeného primárního aktiva z hlediska důvěrnosti, integrity, dostupnosti a kritičnosti;
e) zajištění zdokumentování svěřeného primárního aktiva za metodické podpory Manažera KB a Architekta KB, včetně identifikace podpůrných aktiv a definice vazeb mezi primárním a podpůrnými aktivy, prostřednictvím kterých se primární aktivum realizuje;
f) identifikaci a sledování legislativních a dalších požadavků relevantních pro primární aktivum.

Garant primárního aktiva je dále povinen:

a) spolupracovat na zajištění a realizaci operativních opatření vydaných Manažerem KB, resp. pro jejich provedení poskytnout veškerou součinnost;
b) průběžně zajišťovat sledování identifikovaných rizik svěřeného primárního aktiva včetně jejich vyhodnocování z pohledu závažnosti jejich možných dopadů;
c) v případě změn s dopadem na svěřené primární aktivum se aktivně podílet na:
    i. věcné části zadání na provedení změn,
    ii. přípravě testovacích dat a organizaci testování,
    iii. zkušebním a ověřovacím provozu a zátěžových a bezpečnostních testech,
    iv. přípravě a organizaci akceptačního řízení a na akceptaci jako takové;
d) podílet se na tvorbě nebo připomínkování:
    i. provozních pravidel včetně Havarijních plánů,
    ii. plánu zvládání rizik, který kromě bezpečnostních opatření pro zvládání rizik zahrnuje i určení osob zajišťujících jejich zavedení a správu,
    iii. pravidel pro dodavatele;
e) navrhovat požadavky na kvalitu a úroveň služeb ICT zajišťovaných dodavatelsky pro zajištění provozu svěřeného primárního aktiva;
f) zajistit součinnost při provádění kontrolních auditů a interních kontrol;
g) zajistit součinnost při řešení kybernetických bezpečnostních událostí a incidentů;
h) v případě podezření na porušování stanovených pravidel při použití aktiva neprodleně toto oznámit Manažerovi KB;
i) posoudit a schválit navržené odstávky podpůrného aktiva, na kterém je primární aktivum závislé;
j) v případě ukončení a předání bezpečnostní role Garanta aktiva je povinen předat svému nástupci minimálně následující:
    i. dokumentaci primárního aktiva,
    ii. aktuální přehled podpůrných aktiv a jejich hodnocení,
    iii. aktuální přehled požadavků na ochranu aktiva,
    iv. pokud existují, informace o plánovaném rozvoji nebo změně aktiva,
    v. přehled aktuálních přístupů k aktivu.

Předání a převzetí role Garanta primárního aktiva se hlásí písemně Předsedovi VŘKB.

Práva Garanta primárního aktiva:

a) vyžádat si účast na zasedání Pracovní skupiny KB;
b) navrhnout provedení testování zranitelností u podpůrného aktiva, na němž je jemu svěřené primární aktivum závislé;
c) požádat VŘKB o zrušení vybraných přístupů k svěřenému primárnímu aktivu;
d) kontrolovat plnění stanovené kvality a úrovně služeb primárního aktiva;
e) vyjadřovat se k prioritám realizace bezpečnostních opatření, vztahujících se k svěřenému primárnímu aktivu;
f) požadovat od Garanta podpůrného aktiva poskytování zpráv o jím identifikovaných zranitelnostech, bezpečnostních událostech a incidentech, včetně jejich vyhodnocení;
g) požadovat od Garanta podpůrného aktiva informace o identifikovaných rizicích podpůrných aktiv a hodnocení důsledků rizik z vazeb mezi primárními a podpůrnými aktivy;
h) vyjadřovat se k pravidlům řízení přístupu k svěřenému primárnímu aktivu a provádět kontroly přístupů.

Garant primárního aktiva musí mít zásadní znalosti svěřeného primárního aktiva.

3.5.4. Garant podpůrného aktiva

Garant podpůrného aktiva je odpovědný za zajištění provozu a rozvoje svěřeného podpůrného aktiva v rozsahu, který umožňuje spolehlivé a bezpečné použití primárního aktiva, dle parametrů stanovených Garantem aktiva a bezpečnostními pravidly SŘBI.

Garant podpůrného aktiva ve své působnosti odpovídá zejména za:

a) hodnocení svěřeného podpůrného aktiva z hlediska důvěrnosti, integrity, dostupnosti a kritičnosti;
b) aktuálnost evidence svěřeného aktiva;
c) v součinnosti s Manažerem a Architektem KB identifikaci a hodnocení rizik podpůrného aktiva a v součinnosti s Architektem KB navrhovat přiměřená bezpečnostní opatření;
d) realizaci stanovených bezpečnostních opatření u svěřeného aktiva a provádění analýz jejich vhodnosti a efektivnosti;
e) sledování identifikovaných rizik u svěřeného aktiva a jejich vyhodnocování z hlediska závažnosti jejich možných dopadů.

Garant podpůrného aktiva je dále povinen:

a) informovat Garanta primárního aktiva o plánovaných technologických odstávkách svěřeného podpůrného aktiva a vyžádat si jeho souhlas;
b) analyzovat úrovně a kvalitu poskytovaných služeb ICT a Garantovi primárního aktiva podávat návrhy na případné změny;
c) podílet se na tvorbě a aktualizaci bezpečnostní dokumentace svěřeného aktiva;
d) poskytnout veškerou součinnost při řešení kybernetických bezpečnostních incidentů vyžádanou Manažerem KB, a to bez ohledu na pracovní dobu;
e) realizovat operativní bezpečnostní opatření uložená Manažerem KB;

f) na vyžádání Manažera KB nebo Architekta KB vypracovat stanoviska a připomínky k návrhům změn daného svěřeného podpůrného aktiva a k případným ICT službám, které předpokládají sdílení některých komponent svěřeného podpůrného aktiva;
g) na vyžádání Architekta KB poskytnout veškerou požadovanou součinnost při výkonu jeho činnosti;
h) vyžadovat od Garanta primárního aktiva předložení účelu, podmínek a závazných parametrů pro používání primárního aktiva;
i) podílet se na tvorbě nebo připomínkování:
    i. zadávací dokumentace veřejných zakázek, které se týkají svěřeného podpůrného aktiva,
    ii. testovacích scénářů týkajících se svěřeného podpůrného aktiva,
    iii. migrace ICT služeb,
    iv. přípravy a organizace akceptačního řízení;
k) v případě ukončení a předání bezpečnostní role Garanta podpůrného aktiva je povinen předat svému nástupci minimálně následující:
    i. dokumentaci podpůrného aktiva,
    ii. hodnocení podpůrného aktiva,
    iii. přehled aktuálních požadavků na ochranu aktiva a implementovaných bezpečnostních opatření,
    iv. pokud existují, informace o plánovaném rozvoji nebo změně aktiva,
    v. přehled aktuálních přístupů k aktivu.

Předání a převzetí role Garanta podpůrného aktiva se hlásí písemně Garantovi primárního aktiva.

Práva Garanta podpůrného aktiva:
a) vyžádat si účast na zasedání Pracovní skupiny KB;
b) navrhnout provedení testování zranitelností u podpůrného aktiva;
c) kontrolovat plnění stanovené kvality a úrovně služeb aktiva;
d) vyjadřovat se k výsledkům kontrol zavedených bezpečnostních opatření;
e) vyjadřovat se k obsahu školení uživatelů ICT služby z pohledu rozvoje bezpečnostního povědomí;
f) předložit Manažerovi KB požadavek na přehodnocení:
    i. přijatelnosti identifikovaných kybernetických bezpečnostních rizik,
    ii. priorit realizace bezpečnostních opatření.

Garant podpůrného aktiva musí mít zásadní znalosti svěřeného podpůrného aktiva.

3.5.5. Gestor primárních aktiv správy telematických systémů

Gestor primárních aktiv správy telematických systémů je, v součinnosti s Garanty určených primárních aktiv STS, odpovědný za zajištění rozvoje, použití a bezpečnosti primárních aktiv STS. Navrhuje Garanty primárních aktiv STS, které předkládá ke schválení VŘKB.

Gestor primárních aktiv ve své působnosti odpovídá zejména za:
a) Schválení definice určení primárních aktiv STS a návrhů jejich změn.
b) Schvalování předložení návrhů řízení přístupů k primárním aktivům STS.

c) Identifikaci a sledování legislativních a dalších požadavků relevantních pro primární aktivum.

Gestor primárních aktiv STS je povinen zajistit realizaci bezpečnostních opatření, stanovených touto politikou a dalšími vnitřními předpisy u ISSTS a to včetně pokynů vydaných VŘKB.

Práva Gestora primárních aktiv STS:
a) vyžádat si účast na zasedání Pracovní skupiny KB a VŘKB;
b) kontrolovat plnění stanovené kvality a úrovně služeb aktiva;
c) vyjadřovat se k výsledkům kontrol zavedených bezpečnostních opatření;
d) vyjadřovat se k obsahu školení uživatelů ISSTS z pohledu rozvoje bezpečnostního povědomí;
e) předložit Manažerovi KB požadavek na přehodnocení:
   i. přijatelnosti identifikovaných kybernetických bezpečnostních rizik,
   ii. priorit realizace bezpečnostních opatření.

*3.5.6. **Auditor KB***

Auditor KB je odpovědný za provádění auditů kybernetické bezpečnosti s cílem provést nezávislé hodnocení správnosti a účinnosti zavedených bezpečnostních opatření.

Odpovědnost a povinnosti Auditora KB jsou uvedeny v **SmGŘ-006 Audity IMS**.

Závěrečný protokol z auditu KB předává Auditor KB VŘKB k projednání a přijetí opatření. Předseda VŘKB seznamuje, společně s Auditorem KB, vedení společnosti s výsledky auditu KB.

Audity SŘBI jsou plánovány VŘKB v rozsahu požadavků normy ČSN EN ISO/IEC 27001 s frekvencí jedenkrát za rok.

Audity ISZS jsou plánovány VŘKB v rozsahu požadavků ZoKB a VoKB s frekvencí minimálně jednou za 2 roky a při každé významné změně v ISZS, alespoň v rozsahu této významné změny.

Audity SŘBI jsou prováděny externím pracovníkem akreditovaného certifikačního orgánu.

Audity ISZS jsou prováděny externím dodavatelem vybraného prostřednictvím veřejné zakázky, nebo vlastním zaměstnancem, který současně nesmí být pověřen výkonem jiných bezpečnostních rolí a rolí odpovědnou za provoz ICT nebo zajištění fyzické či personální bezpečnosti. Současně nesmí auditor KB zastávat roli Manažera a Architekta KB, Garanta primárního a podpůrného aktiva a nesmí být členem VŘKB.

Auditor KB musí splňovat kvalifikační předpoklady stanovené VoKB rozsahem znalostí, zkušeností, vzděláním a certifikací.

*3.5.7. **Administrátor***

Administrátor je osoba odpovědná za správu, provoz, použití, údržbu a bezpečnost technického aktiva v jeho správě. V podmínkách BKOM se jedná obvykle o zaměstnance

zařazené na funkcích specialista ICT, samostatný technik. Role administrátorů určuje u SŘBI vedoucí oddělení VT a u ISZS Garant primárního aktiva.

Povinnosti administrátorů jsou stanoveny Pracovní náplní zaměstnance a povinnostmi Garanta podpůrného aktiva.

3.5.8. ***Uživatel***

Uživatel je zaměstnanec BKOM nebo externí pracovník, který má přístup k aktivům BKOM v rozsahu SŘBI a ISZS.

Povinnosti uživatelů jsou stanoveny platnými vnitřními předpisy BKOM.

4. SOUVISEJÍCÍ DOKUMENTY

4.1. Dokumenty nadpodnikové úrovně

ČSN EN ISO 9001	Systémy managementu kvality – Požadavky
ČSN EN ISO 14001	Systémy environmentálního managementu – Požadavky s návodem pro použití
ČSN ISO 45001	Systémy managementu bezpečnosti a ochrany zdraví při práci – Požadavky s návodem k použití
ČSN ISO/IEC 27001	Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky
Zákon č. 181/2014 Sb.	o kybernetické bezpečnosti
Vyhláška č. 82/2018 Sb.	o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

4.2. Podnikové dokumenty

PIMS-001	Příručka Integrovaného systému řízení
SmGŘ-039	Politika bezpečnosti informací
SmGŘ-061	Řízení dodavatelů
SmGŘ-042	Bezpečné chování uživatele
SmGŘ-040	Zvládání kybernetických bezpečnostních událostí a incidentů
SmGŘ-041	Řízení kontinuity činností ICT
Mp-GŘ039-01	Metodika analýzy rizik kybernetické bezpečnosti

5. ZÁVĚREČNÁ USTANOVENÍ

5.1. Účinnost

Tato směrnice nabývá účinnosti dnem 01.02.2023.
Tímto vydáním ON se ruší veškerá předchozí vydání a úpravy.

5.2. Rozdělovník

Zaměstnanci s uživatelským účtem obdrží ON v systému DMS. Zaměstnanci bez tohoto přístupu jsou seznámeni s dokumentací v její listinné podobě, uložené u správce řízené dokumentace.

Předpis pro vyhotovení geodetické dokumentace skutečného provedení staveb

(Mp-SÚ3200-01)

6. vydání ze dne 28.11.2016 Účinnost ode dne 01.12.2016

Číslo revize	Čísla revidovaných stránek	Zaznamenal a zařadil Jméno	Datum	Podpis
1	str. 10, 15	Burian	21.06.2017	
2				
3				
4				
5				

	Odborný garant	Formálně ověřil	Vydavatel	Schválil
Úsek	SŘ	GŘ	SŘ	SŘ
Funkce	Vedoucí oddělení geodézie	Správce řízené dokumentace	Vedoucí střediska	Správní ředitel
Jméno	Ing. Marek Chlup	Ing. Pavel Burian	Ing. Marek Hořejš	Ing. Roman Nekula, MBA
Datum	28.11.2016	28.11.2016	28.11.2016	28.11.2016
Podpis				

Obsah směrnice
(Mp-SÚ3200-01)

1. ÚVODNÍ USTANOVENÍ

1.1. **Účel**

Předpis popisuje vyhotovení geodetické dokumentace skutečného provedení staveb pro společnost Brněnské komunikace a.s.

1.2. **Závaznost**

Tento Mp platí pro zhotovitele geodetické dokumentace skutečného provedení staveb.

1.3. **Správa normy**

1.3.1. Sběr připomínek a případné změnové řízení zajišťuje odborný garant ON.
1.3.2. Výklad této normy zajišťuje odborný garant.
1.3.3. Metodickou kontrolu dodržování pravidel a zásad této normy zajišťuje odborný garant.

2. VYMEZENÍ POJMŮ

2.1. **Použité zkratky**

BKOM	-	Brněnské komunikace a.s.
Bpv	-	výškový systém – baltský po vyrovnání
CŘD	-	centrální řízení dopravy
DGN	-	označení výkresů systému MicroStation
Mp	-	metodický pokyn
PBPP	-	pevné body podrobného polohového pole
Sm	-	směrnice
S-JTSK	-	souřadnicový systém – Jednotné trigonom. sítě katastrální
SSZ	-	světelné signalizační zařízení
2D	-	dvourozměrný
3D	-	třírozměrný

2.2. **Definice**

Vyhotovení geodetické dokumentace skutečného provedení staveb pro společnost BKOM.

2.3. **Odborné funkce**

Zodpovědný geodet
je zástupce BKOM, pověřený přejímáním geodetické dokumentace skutečného provedení staveb.

Zhotovitel
je geodet, geodetická firma dodávající BKOM geodetickou dokumentaci skutečného provedení staveb. Zhotovitel musí splňovat požadavky plynoucí ze Zákona č.200/1994 Sb. § 3, odst. (3) a (4).

3. VYHOTOVENÍ GEODETICKÉ DOKUMENTACE SKUTEČNÉHO PROVEDENÍ STAVEB

3.1. **Rozsah geodetických prací a geodetické části dokumentace skutečného provedení stavby**

3.1.1. Rozsah prací – měření

3.1.1.1. Obecné podmínky

- souřadnicový systém S-JTSK
- výškový systém Bpv
- účelová mapa ve 3. třídě přesnosti - podle ČSN 01 3410
- měřítko mapování 1:250

3.1.1.2. Zaměření skutečného provedení komunikace

- Měření bude provedeno **v příčných profilech po 20 m včetně výšek v ose vozovky a výšek obrubníků**. Účelová mapa novostavby bude zaměřena za hranici silničního tělesa, i s objekty do vzdálenosti min. 10 m. Zpracovatel si před zahájením měřických prací zjistí stav okolí v pasportu BKOM. V případě, že navazuje na již zaměřené stavby, zpracuje zaměření v návaznosti na tyto již provedené stavby. Pokud je stavbou chodník, parkoviště, zastávka, vjezd, nebo jedná – li se o opravu povrchů, bude provedeno pouze zaměření realizace (stavby) bez návaznosti na okolní objekty.
- Je-li podél komunikace vyznačeno rozhraní parcel plotem nebo zídkou ohraničující soukromý majetek, **je nutno zaměřit** toto rozhraní a zakreslit typ tohoto rozhraní uživatelskou čarou. Situace za ploty a zídkami (evidentně soukromý majetek) se neměří.
- Je nutno zaměřit všechny povrchové znaky podle **ČSN 01 3411**.
- Zaměří se všechny hranice mezi různými povrchy a materiál každého povrchu se vyznačí popisem.
- Zaměří se nezpevněné plochy kolem stromů.
- Zaměří se osy kolejí a rozhraní tramvajového tělesa a vozovky. V případě, že není jasné rozhraní mezi tram. tělesem a vozovkou, kreslí se čára (vrstva 13) ve vzdálenosti 0,50m od kolejnice.
- Při mimoúrovňovém křížení komunikací se druhá komunikace vyznačí obrysem.
- U podchodů se zaměří část pod komunikací včetně odvodnění.
- U oblouků se měří 3 body, u větších poloměrů po 5m, přímý úsek maximálně po 20m.
- U všech ploch bude vyznačen povrch geodetickou značkou, u zpevněných ploch textem.
- Textem budou dále označeny popisy objektů, orientační čísla domů, názvy ulic, výšky obrubníků, materiál obrubníků, materiál vodících proužků a přídlažby.
- Není-li jednoznačné využití plochy, je třeba označit, zda jde o vozovku, chodník, parkoviště ap.
- U schodiště se měří začátek a konec podesty, stupně se vykreslí dle skutečnosti.
- U zábradlí, svodidel a zídek se uvede materiál a výška.
- U propustků se zaměří vtok, výtok a křídla a uvede se průměr a materiál potrubí.
- Zaměří se podobrubníkové vpusti.
- Svislé a vodorovné dopravní značky se uvedou podle vyhlášky č. 30/2001 Sb. ve znění pozdějších předpisů.
- Zaměří se úchyt svislé dopravní značky včetně značek na objektech. Zákres se provede podle **ČSN 01 3411**.
- U podélné čáry přerušované se zaměří změna kadence, u vodorovných stínů se zaměří směr čar.

3.1.1.3. Zaměření skutečného provedení kanalizace

- Zaměřuje se **dešťová kanalizace včetně přípojek**, která přejde do správy BKOM.
- Zaměření podrobných částí dešťové kanalizace je nutno zaměřit zásadně **před záhozem**.
- Měří se polohy a výšky šachet, vpustí, lomů, míst napojení a ostatních objektů na kanalizaci.

- U šachet, vpustí a ostatních objektů se uvádí výšky dna, výšky poklopu (mříže), výšky vyústění a výšky zaústění.
- U kanalizačního potrubí se uvádí materiál a průměr potrubí, spád v promilích a délka mezi šachtami a přípojkami.
- Délka přípojky se uvádí v metrech na 2 desetinná místa.
- U kanalizačních šachet, vpustí a přípojek se zakótují oměrné míry nejméně na dva pevné předměty měření.
- Součástí dodávky skutečného provedení zaměření kanalizace je tabulka uličních vpustí, tabulka kanalizačních šachet, podélný profil dešťové kanalizace, výkres atypických objektů kanalizace. Situaci kanalizace v tištěné podobě, tabulky a podélné profily předávejte ve dvou vyhotoveních.
- Pokud není k dispozici mapa vypracovaná podle tohoto Metodického pokynu, je nutno ji zaměřit podle bodu 3.1.1.2.

3.1.1.4. Zaměření skutečného provedení kabelu světelného signalizačního zařízení (SSZ)

Kabely je nutno zaměřit zásadně před záhozem.
Měří se a uvádí se:

- řadiče SSZ, koordinační skříně CŘD, elektroměrové skříně a ostatní nadzemní znaky kabelů
- průběh kabelu na vrchu kabelového pláště, průběh indukčních smyček, počet kabelů v kynetě, materiál kabelů, kabelové spojky
- chráničky, jejich průběh, šířka chráničky, materiál, průměr potrubí a počet prostupů a jejich obsazení, příčný řez chráničkami - u nových chrániček (u 1 prostupu ne)
- u stávajících chrániček uvést materiál a průměr

Kabel se měří v přímém úseku max. po 15 m. Trasu je nutno zaměřit tak, aby odchylka osy kabelu mezi dvěma zaměřovanými body nepřesáhla 14 cm. Lomové body kabelů a koncové body chrániček je nutno ve výkresu zakótovat nejméně od dvou pevných předmětů měření.
Pokud není k dispozici mapa vypracovaná podle tohoto Metodického pokynu, je nutno ji zaměřit podle bodu 3.1.1.2.
Účelová mapa kabelu (SSZ) bude zaměřena, i s objekty do vzdálenosti min. 10 m na každou stranu od osy kabelu.

3.1.1.5. Zaměření skutečného provedení koordinačního kabelu

Koordinační kabel se zaměří podle bodu 3.1.1.4 stejně jako kabel SSZ.
Rozsah zaměření **nově položeného** koordinačního kabelu bude upřesněn konzultací se správcem sítí, min. do vzdálenosti 10m. Pokud bude k dispozici DSPS, poskytne se zhotoviteli. V případě, že není DSPS, zaměří se situace v rozsahu takovém, jak určí správce sítí. Zhotovitel musí doložit rozsah zaměření schválený správcem sítí.
Rekonstruovaný (opravovaný) koordinační kabel se zaměří podle bodu 3.1.1.4, ale účelová mapa pouze do šířky 7,5 m na každou stranu od osy kabelu.

3.1.1.6. Zaměření skutečného provedení optického kabelu

Optický kabel se zaměří podle bodu 3.1.1.5 stejně jako kabel KK.

3.1.1.7. Zaměření skutečného provedení stavby mostu

Nově postavený nebo rekonstruovaný most se zaměří podle bodu 3.1.1.2.
Navíc se u všech mostů zaměří:

- příčné profily u mostních závěrů a v průsečíku osy mostu s osou přemosťované překážky
- mostní závěry, římsy, křídla
- odvodňovací prvky

- svahové kužely
- revizní schodiště
- protidotykové zábrany, protihlukové stěny s popisem
- výška trolejového vedení na mostě v nejnižším místě - zaměří se jen na základě požadavku správce mostů
- pozorované body nosné konstrukce dle ČSN 73 6201 odst. 13.14 - zaměří se jen na základě požadavku správce mostů

U mostu přes vodoteč se zaměří pod mostem v podélném řezu:

- spodní část nosné konstrukce v ose mostu s výškami dna vodoteče a hladiny v době měření
- nejnižší místo spodní části nosné konstrukce

U mostu přes komunikaci se zaměří podjezd ve třech profilech, na krajích mostu a v ose mostu. V případě, že nosná konstrukce mostu má proměnnou výšku, bude počet měřených profilů stanoven pracovníky oddělení správy mostů a speciálních objektů.

V profilu se zaměří:

- kolmá a šikmá světlost mostního otvoru, volná šířka podjezdu a šířka mezi obrubníky komunikace
- volné podjezdné výšky v ose komunikace, u obrubníku, na obrubnících a 0,5 m za obrubníky
- zaměření troleje a dalších překážek pod mostem

3.1.1.8. Zaměření skutečného provedení stavby tunelu

Zaměření bude provedeno dle metodického pokynu **Mp-SÚ3200-02**.

3.1.1.9. Zaměření změny povrchu vjezdu

Změna povrchu vjezdu v šířce úpravy do 20 m se neměří geodeticky. Do výkresu se uvede název ulice a čísla popisného resp. evidenčního, případně parcelního, použité materiály (včetně materiálů v nejbližším okolí změny) a okótování od stávajících objektů (např. rozhraní budov, plotů apod.), podle rozhodnutí samostatného technika střediska správy komunikací. Viz příloha č. 1. Pokud vjezd nelze okótovat od stávajících objektů, provede se geodetické zaměření dle bodu 3.1.1.2. V případě vybudování nového vjezdu nebo dojde-li ke změně prostorového uspořádání vjezdu (např. změna polohy obrubníků), nejedná se o změnu povrchu a postupuje se dle bodu 3.1.1.2.

3.1.1.10. EZA - Evidence zásahu

Zásahy do vozovek, chodníků a zelení - opravy, překopy, protlaky, izolace objektů a podobně budou zaměřeny a zpracovány v programu EBU.

3.1.2. Předmět dodávky

Geodetická část dokumentace skutečného provedení stavby musí mít toto složení:

1. Technická zpráva
2. Geodetické údaje o pevných bodech.

- seznam souřadnic bodů daných a nově určených - doložit body použité pro připojení do závazných geodetických systémů (S-JTSK, Bpv) dle nařízení vlády č. 430/2006 Sb. § 2 písm. c) a f)

3. Přehledný náčrt PBPP, včetně připojení na stávající bodové pole
4. Seznam souřadnic podrobných bodů (na CD) ve formátu *.csv nebo *.txt
5. Situace s posunutými redukovanými výškami bodů vytisknutá na papíře v měřítku 1:250.
6. Zakreslení geodetického zaměření skutečného provedení stavby do souborů ve formátu DGN systému MicroStation s náležitostmi uvedenými v částech 3.2. a 3.3. tohoto Metodického pokynu .

7. Zhotovitel geodetické dokumentace vyhotoví na náklady zhotovitele stavby tabulku obsahující součty ploch jednotlivých povrchů (tzv. Výkaz výměr). Jednotlivé plochy budou rozčleněny podle požadavků investora.

Písemná část elaborátu geodetické dokumentace skutečného provedení stavby bude ověřena ve smyslu Vyhlášky č. 31/1995 Sb. § 18.

3.2. Předpis pro digitální kresbu geodetického zaměření skutečného provedení stavby

3.2.1. Všeobecné pokyny

Digitální kresba musí být dodána na záznamovém médiu, které bude označeno názvem akce a jménem zhotovitele. Při použití komprimace souboru musí být dodán komprimační program. V případě, že je předmětem měření skutečné provedení stavby mostu, je nutno uvést také evidenční a archivní číslo mostu. Digitální kresba musí být v souborech ***.dgn systému MicroStation** (vzhledem k použití uživatelských čar).

3.2.2. Konkrétní požadavky

1. Souřadnicový systém **S-JTSK**
2. Výškový systém **Bpv**
3. Měřítko situace **1:250**
4. Zdrojový výkres musí mít následující parametry:
   GO=214783.648,214783.648; MU=m; SU=mm;
   Počet základních jednotek na mm:1;
   Souřadnicový systém S-JTSK je umístěn do III. kvadrantu kartézského souřadnicového systému. Souřadnice Y systému S-JTSK odpovídá záporné souřadnici X ve výkresu *.dgn a souřadnice X systému S-JTSK odpovídá záporné souřadnici Y ve výkresu *.dgn.
   BKOM nabízí vlastní zakládací výkresy **bkom2d.dgn a bkom3d.dgn**.
5. Kresba musí být rozdělena na čtyři výkresy s názvy:
   Na prvních pozicích je název akce.
   xxxxxx_b.dgn - pro pevné a podrobné body bez posunu textových prvků (čísel a výšek)
   xxxxxx_p.dgn - pro polohopis (pouze nově zaměřené prvky polohopisu)
   xxxxxx_v.dgn - pro vodorovné dopravní značení
   xxxxxx_t.dgn - pro tisk situace s posunutými redukovanými výškami bodů
   V případě, že se měří kanalizace, kabely SSZ a koordinační kabely, mosty nebo tunel pro BKOM, je nutno dodat navíc speciální výkresy:
   xxxxxx_k.dgn - pro kanalizaci ve správě BKOM
   xxxxxx_s.dgn - pro kabely SSZ, koordinační kabely a optické kabely , pokud jsou zaměřeny současně kabely SSZ a KK v jedné kynetě, musí být vyhotoveny tiskové soubory pro každý kabel samostatně
   xxxxxx_m.dgn – pro mosty (viz odstavec 3.1.1.7), příčný, podélný profil mostu
6. Prvky a jejich atributy jsou uvedeny v části 3.3 tohoto Mp a musí být:
   závislé na pohledu — nezamknuté
   nájezduschopné — kreslené v primární třídě.
7. Výkres **xxxxxx_b.dgn** musí obsahovat vrstvy symbolů (resp. označení) pro pevné a podrobné body. Vztažný bod symbolu (resp. označení) by měl být umístěn v desetinné tečce výšky a nad horním levým rohem čísla bodu, aby výšky i čísla bodů byly při zapnutí jejich vrstev čitelné. **Úchopový bod musí být v jednom totožném místě.**
8. Mapové značky se kreslí podle normy ČSN 01 3411. Ke kreslení speciálních značek BKOM je k dispozici knihovna **bkom_3.cel** a **bkom_3.rsc**. K tvorbě mapových značek (bodových i liniových) je nutno použít knihovny firmy HSI: **norma.cel**, **sit.cel**, **ugeo_e.rsc**, **ugeo_tp.rsc** a **ugeo_vp.rsc**, které obsahují všechny mapové značky z normy ČSN 01 3411 a mají stejný

název jako kód z normy. Tyto knihovny jsou bezplatně k dispozici u společnosti BKOM, ale jejich použití je vázáno výhradně na práce pro BKOM.
Poznámka:
Všechny knihovny jsou vytvořeny v měřítku 1:1000. Pro měřítko 1:250 se kreslí ve velikosti 0.250, výjimkou je vodorovné značení, které se kreslí ve velikosti 1.000.

9. Pokud budou do kresby zahrnuty prvky neuvedené v části 3.3 tohoto Metodického pokynu, musí být přiložen jejich seznam včetně atributů. U liniových prvků je nutno dodržovat zásadu, že různé liniové prvky musí být odlišeny alespoň jedním základním atributem (vrstva, typ čáry, tloušťka, barva), aby se prvky daly vybírat. Mezi základní atributy se přitom nepočítá uživatelský typ čáry systému MicroStation.
10. Liniové prvky se kreslí základním nebo uživatelským typem čáry. Pokud je k nakreslení prvku předepsána uživatelská čára, prvek musí být nakreslen příslušnou uživatelskou čarou.
11. Při **kreslení čar** je možno používat lomené čáry - line string (typ 4), elipsy, kružnice (typ 15), oblouky - arc (typ 16). Pro konstrukční úlohy je možno používat také úsečky - line (typ 3). **Není možné používat** složený útvar - complex shape (typ14) a multičáry. Při kreslení hraničních čar (mezi vozovkou, chodníkem, zelení, atd.) **je nutno vyvarovat se přetahů a nedotahů. Odevzdávat pouze začištěnou kresbu.**
12. Při kreslení čar se dodržuje používání následujících typů čar:
    - Typ 0 (plná čára) - pro nadzemní objekty, které mají průnik s terénem
    - Typ 2 (krátce čárkovaná čára) – pro objekt, který nemá styk s terénem
    - Typ 3 (dlouze čárkovaná čára) – pro podzemní drobné objekty (propustek,…)
    - Prvky polohopisu shora neviditelné se zakreslí barvou č. 2, ostatní atributy kresby zůstanou zachovány.
13. **Budovy** musí být zaměřeny průčelím domů, rozhraní se vyznačí kolmicí mezi jednotlivými budovami. Měří se také vrata do budov, garáží a vjezdy na pozemky. U každé budovy musí být umístěno příslušné orientační, resp. popisné číslo. Typ budovy se označí mapovou značkou, resp. se navíc popíše textem.
14. Každou ulici je třeba popsat názvem (vrstva 42).
15. Stavba musí být zaměřena do vzdálenosti 10m na obě strany od kraje silničního tělesa a 10m od obou konců úpravy.
16. Je-li komunikace ohraničena plotem, zídkou, ohradní zdí apod., je nutno zaměřit toto rozhraní a zakreslit typ rozhraní příslušnou uživatelskou čarou. Situace za touto hranicí (evidentně soukromý majetek) se neměří.
17. Kresba musí obsahovat rozhraní různých typů ploch (vozovka, chodník, krajnice-nezpevněná, příkop, silniční zeleň, dopravní ostrůvek, tramvajové těleso, parkoviště, vjezd na pole, zpomalovací práh atd.) a materiálů ploch (asfalt, dlažba betonová zámková, atd.). Každá plocha (i neuzavřená) musí být opatřena popisem nebo mapovou značkou v předepsaných vrstvách. Význam každé čáry i plochy musí být dostatečně jasný, aby nebylo nutno vracet se do terénu a zjišťovat význam.
    Pro popisy povrchů se používá seznam zkratek na str. 22. V případě jiných povrchů je nutno povrch vypsat slovy, příp. napsat legendu.
18. Prvky bez rozlišení druhu se kreslí jen v případě, že druh není možno zjistit. Vlastnosti prvků se označují popisem (průřez potrubního vedení v mm, výška obrubníku, výška zdi, atd.)
19. **Značky** se kreslí orientované k severu, případně s natočením podle příslušné čáry (např. vpustě). Vyskytuje-li se v jednom bodě více objektů (lampa, svislá dopravní značka, ...), do bodu se musí nakreslit všechny mapové značky. Přitom se použijí značky z knihovny

bkom_3.cel, pro více objektů v jednom bodě. Pokud knihovna **bkom_3.cel** příslušné značky neobsahuje, použije se natočení značek.

20. **Svislé dopravní značky** se kreslí do vrstvy 19, resp. do vrstvy 44. Z kresby musí být jasné, na jakém objektu (lampa, trakční sloup, ...) je značka umístěna.
21. **Vodorovné dopravní značky** se kreslí s atributy předepsanými v části 3.3 tohoto Metodického pokynu. Otočení značek musí odpovídat skutečnosti. Ke kreslení bodových vodorovných značek je k dispozici knihovna **bkom_3.cel**. Značky v knihovně jsou vytvořeny ve **skutečné velikosti**, kreslí se ve velikosti 1.0. Vodorovné značky je nutné kreslit podle skutečného tvaru v terénu. Je-li situace atypická, je třeba použít jiné prostředky systému MicroStation a uživatelské čáry z knihovny **bkom_3.rsc**.
22. **K popisům se používá font č. 0** - cs standard nebo anglický standard, tloušťka čáry 0. Aby bylo možno texty v MicroStationu vybírat (za účelem změny atributů), používají se pro texty různé typy čar (viz část 3.3 tohoto Metodického pokynu). V MicroStationu však typ čar nemá vliv na způsob zobrazení textu a text bude vždy zobrazen plnou čarou. Velikost písma v části 3.3 tohoto Metodického pokynu platí pro měřítko 1:250.
23. U **stoky** se uvádí výšky dna v závorce, nad čarou materiál a průměr potrubí, pod čarou délka mezi šachtami a spád v promilích.
24. Součástí dodávky skutečného provedení zaměření kanalizace je **tabulka uličních vpustí**.
25. Na zobrazenou **trasu kabelu SSZ, KK a optického kabelu** se uvede materiál a počet kabelů.
26. U **chráničeк** SSZ a KK se nad chráničkou uvede materiál, průměr potrubí a počet prostupů, pod chráničkou se uvede počet obsazených prostupů. U nově budovaných chrániček se v řezu zakreslí uložení kabelů v chráničkách.
27. **U tunelů** musí být všechny výkresy zpracovány v 3D provedení (v trojrozměrném prostoru).
28. V případě, že je předmětem měření skutečné provedení stavby mostu, je nutno uvést také evidenční a archivní číslo mostu.
29. Při zaměřování **zeleně** se jednotlivý strom nebo keř zaměří bodem v ose a vyznačí se buňkou pro jednotlivý strom, resp. křovinatý porost. Zalesněný nebo křovinatý **prostor se zaměří obvodem**, a ve výkrese se znázorní jako rozhraní ploch (vrstva 7) a doplní příslušnou buňkou (geodet. značkou) pro zalesněný nebo křovinatý porost **bez měřeného bodu**. Živý plot se zaměří obvodem nebo v ose a doplní se informací o jeho šířce.
30. Výkres xxxxxx_p .dgn xxxx_t . dgn bude doplněn o lomenou čáru ve vrstvě 63 barvou 9 stylem 4, tloušť. 4, která bude přesně znázorňovat skutečný rozsah novostavby.

3.3. Prvky s atributy

Výkres xxxxxx_b.dgn

Vrstva	popis	buňka uživ.čára	prvek	typ	tloušťka výška	barva
	Body na kabelech :					
28	výška bodu		17	0	0.4x0.3	7
29	číslo bodu		17	0	0.4x0.3	3
30	symbol bodu		2,3	0	0	0
	Body na kanalizaci:					
48	výška bodu		17	0	0.4x0.3	0
49	číslo bodu		17	0	0.4x0.3	1
50	symbol bodu		2,3	0	0	0

Vrstva	popis	buňka uživ.čára	prvek	typ	tloušťka výška	barva
	Pevné body:					
54	výška pevného bodu		17	0	0.6	3
55	číslo pevného bodu		17	0	0.6	4
56	symbol pevného bodu		2, 3	0	0	0
	Podrobné body:					
58	výška podrobného bodu		17	0	0.4x0.3	5
59	číslo podrobného bodu		17	0	0.4x0.3	2
60	symbol podrobného bodu		2, 3	0	0	0
	Výkres xxxxxx_p.dgn					
	Mapa:					
1	mapový rám					
	legenda					
	podklad ÚMPS-nezaměřený					96
	Body:					
2	bod čs. trigonometrické sítě, PBPP	1.010	2	0	0	0
	bod čs. nivelační sítě	1.030	2	0	0	0
	bod stabilizovaný techn. nivelace	1.040	2	0	0	0
	mezník vlastnické hranice	1.050	2	0	0	0
	popis bodů a výšek PBPP		17	0	0.6	0
	Budovy:					
4	budova		3,4,6,15,16	0,2,3	2	1
	schodiště budovy		3,4,6,15,16	0,2,3	0	1
	Vjezdy:					
5	vjezd do budovy		3,4,16	0	4	3
	vjezd na pozemek		3,4,16	0	4	3
	sklepní okno		3,4,16	3	1	3
	Hraniční čáry:					
7	hraniční čára		3,4,15,16	0,2,3	0	0
	propustek		3,4,16	3	0	0
	Ploty a zídky:					
8	plot bez rozlišení	2.093	3,4,16	U	0	0
	plot bez rozlišení s podezdívkou	2.093	3,4,16	U	2	0
9	plot dřevěný	2.103	3,4,16	U	0	0
	plot dřevěný s podezdívkou	2.103	3,4,16	U	2	0
10	plot drátěný, kovový	2.123	3,4,16	U	0	0
	plot drátěný, kovový s podezdívkou	2.123	3,4,16	U	2	0
11	plot živý	2.143	3,4,16	U	0	0
12	ohradní zeď, zídka,	2.163	3,4,16	U	2	0
	protihluková zeď, stěna	2.163	3,4,16	U	2	0

Vrstva	popis	buňka uživ.čára	prvek	typ	tloušťka výška	barva
	vnější hrana ohradní zdi, zídky		3,4,16	0	0	0
13	neznatelná hranice tram. tělesa		3,4,16	3	0	0
	Pozemky:					
14	chmelnice	3.020	2	0	0	2
	vinice	3.030	2	0	0	2
	zahrada	3.040	2	0	0	2
	ovocný sad	3.050	2	0	0	2
	louka	3.060	2	0	0	2
	pastvina	3.070	2	0	0	2
	lesní půda bez rozlišení	3.080	2	0	0	2
	lesní půda s jehličnatým porostem	3.090	2	0	0	2
	lesní půda s listnatým porostem	3.100	2	0	0	2
	lesní půda s křovinatým porostem	3.110	2	0	0	2
	jednotlivý strom	3.130	2	0	0	2
	park, okrasná zahrada	3.140	2	0	0	2
	hřbitov	3.150	2	0	0	2
	neplodná půda	3.160	2	0	0	2
	rákosí	3.170	2	0	0	2
	Stavební objekty:					
15	budova zděná	4.020	2	0	0	0
	dřevěná	4.030	2	0	0	0
	budova, podchodná část	4.040	2	0	0	0
	výtah v chodníku	4.051	2	0	0	0
	schody v terénu (které nejsou součástí budovy)		3,4,6,16	0	0	0
	kostel	4.091	2	0	0	0
	synagóga	4.100	2	0	0	0
	střed předmětu malého rozsahu upřesnit popisem ve vrstvě 49)	4.110	2	0	0	0
	předměty malého rozsahu (upřesnit popisem ve vrstvě 49)	4.120	2	0	0	0
	zvonice	4.130	2	0	0	0
	pomník	4.140	2	0	0	0
	mostní váha	4.150	2	0	0	0
	stojan pohonných hmot	4.160	2	0	0	0
	komín	4.170	2	0	0	0
	propagační objekt-reklama	4.190	2	0	0	0
	podpěra betonová (pilíř)		3,4,6,15	0	0	0
17	opěrná, zárubní zeď	4.223	3,4,16	U	2	0
	vnější hrana opěrné, zárubní zdi		3,4,16	0	0	0

Vrstva	popis	buňka uživ.čára	prvek	typ	tloušťka výška	barva
	Doprava:					
19	osa kolejí	5.01	3,4,16	U	2	0
	výměník výhybky	5.081	2	0	0	0
	styk výhybek	5.091	2	0	0	0
	křižovatková výhybka	5.101	2	0	0	0
	zarážedlo	5.131	2	0	0	0
	mech. návěstidlo	5.151	2	0	0	0
	světelné návěstidlo	5.161	2	0	0	0
	mech. závory	5.171	2	0	0	0
	výstražný kříž	5.181	2	0	0	0
	staničník	5.200	2	0	0	0
	zastávka veř. dopravy	5.240	2	0	0	0
	zastávka na objektu	5.241	2	0	0	0
	svět. sign. zařízení	5.250	2	0	0	0
	svět.sign. zař. na objektu	5.251	2	0	0	0
	místní tabule	5.261	2	0	0	0
	svislá dopr. značka	5.270	2	0	0	0
	dopr. značka na objektu	5.271	2	0	0	0
	výstražný majáček	5.280	2	0	0	0
	kamenný patník (rozměrem)		6	0	0	0
21	svodidlo jednostranné	5.2930	3,4,16	U	0	0
	svodidlo oboustranné	5.2931	3,4,16	U	1	0
	zábradelní svodidlo	5.2932	3,4,16	U	2	0
	betonové svodidlo (šířkou)		3,4,16	0	0	0
22	zábradlí	5.303	3,4,16	U	0	0
	zábradlí na zídce	5.303	3,4,16	U	2	0
	Nerozlišené objekty					
23	stožár (sloup bet., kov., dřev.)	6.010	2	0	0	0
	příhradový stožár	6.021	2	0	0	0
	nástěnná konzola	6.031	2	0	0	0
	vstupní šachta bez rozlišení	6.081	2	0	0	0
	šachta bez rozlišení (rozměrná)		6	0	0	0
	šoupě bez rozlišení	6.140	2	0	0	0
	priska bez rozlišení	6.661	2	0	0	0
	priska bez rozlišení (rozměrná)		3,4,6,16	0	0	0
	Vodovody:					
24	vodoměrná šachta	6.111	2	0	0	2
	hydrant nadzemní	6.120	2	0	0	2
	hydrant podzemní	6.130	2	0	0	2
	šoupě vodovodní	6.140	2	0	0	2
	vodovodní potrubí bez rozl.	6.152	3,4,16	U	0	2

Vrstva	popis	buňka uživ.čára	prvek	typ	tloušťka výška	barva
	Kanalizace:					
25	kanalizační šachta	6.200	2	0	0	6
	kanalizační stoka bez rozl.	6.232	3,4,16	U	0	6
	dešťová kanalizace	6.262	3,4,16	U	1	6
	zaolejovaná dešťová kan.	6.282	3,4,16	U	1	6
	vpusť	6.301	2	0	0	6
	vpusť v podchodu	6.301	2	3	0	6
	podobrubníková vpusť		3,4	0	4	6
	žlabová vpusť (prahová)		3,4,6,15	0	0	6
	jímka, lapač splavenin, horská vpusť		3,4,6,15,16	0	2	6
	ORL-odlučovač ropných látek		3,4,6,15,16	0	2	6
	dešťový svod, mostní odvodňovač		15	0	0	6
	Plynovody:					
26	šoupě plynovodní	6.140	2	0	0	4
	plynovodní potrubí bez rozl.	6.322	3,4,16	U	0	4
	čichačka	6.380	2	0	0	4
	kontrolní měřící vývod	6.391	2	0	0	4
	HUP	6.661	2	0	0	4
	HUP (rozměrný)		3,4,6,16	0	0	4
	Teplovody:					
27	tepelné potrubí bez rozl.	6.512	3,4,16	U	0	3
	šoupě teplovodní	6.140	2	0	0	3
	šachta teplovodní	6.081	2	0	0	3
	Elektrická zařízení:					
29	svítidlo na stožáru	6.560	2	0	0	10
	svítidlo na objektu	6.561	2	0	0	10
	svítidlo slavnostní	6.570	2	0	0	10
	svítidlo slavnostní na objektu	6.571	2	0	0	10
	svítidlo na zemi + převěs	6.580	2	0	0	10
	elektrárna, transformovna	6.650	2	0	0	10
	priska (rozděl. nebo el. skříň)	6.661	2	0	0	10
	priska (rozměrná)		3,4,6	0	0	10
	venk. silové vedení bez rozl.	6.592	3,4,16	U	0	10
	silový kabel bez rozl.	6.592	3,4,16	U	1	10
30	venkovní NN	6.602	3,4,16	U	0	10
	kabel NN	6.602	3,4,16	U	1	10
31	venkovní VN	6.612	3,4,16	U	0	10
	kabel VN	6.612	3,4,16	U	1	10
32	venkovní VVN	6.622	3,4,16	U	0	10

	kabel VVN	6.622	3,4,16	U	1	10
Vrstva	popis	buňka uživ.čára	prvek	typ	tloušťka výška	barva
	Spoje:					
34	sdělovací vedení spojové	6.702	3,4,16	U	0	5
	kabel sdělovací	6.702	3,4,16	U	1	5
	telefonní budka	6.750	2	0	0	5
	telefon na objektu	6.751	2	0	0	5
	hlásič pož. ochrany	6.760	2	0	0	5
	policejní hlásič	6.770	2	0	0	5
	hodiny na stožáru	6.780	2	0	0	5
	hodiny na objektu	6.781	2	0	0	5
	rozhlas na stožáru	6.790	2	0	0	5
	rozhlas na objektu	6.791	2	0	0	5
	priska	6.661	2	0	0	5
	priska (rozměrná)		3,4,6,16	0	0	5
	Produktovody:					
35	potrubí produktovodu	6.802	3,4,16	U	0	0
36	kabelovod, multikanál		3,4,16	3	0	0
37	kolektor	6.822	3,4,16	U	0	0
38	chránička	CHR	3,4,6,16	0	0	7
39	povrchová těžba	7.010	2	0	0	0
	sonda	7.090	2	0	0	0
	Vodstvo:					
40	vodní tok	8.021	2	0	0	1
	vodní nádrž	8.030	2	0	0	1
	močál	8.040	2	0	0	1
	studna	8.110	2	0	0	1
	fontána	8.170	2	0	0	1
	hladina vodního toku, nádrže		3,4,16	0	0	1
	Výškopis:					
41	hrana terénního svahu		3,4	0	0	6
	výška 1. nadz. podlaží	9.15	2	0	0	6
	výška vodorovné hrany	9.15	2	0	0	6
28	šrafování svahů		3,4	0	0	6
33	vrstevnice			0	0	6
	Názvy ulic,řek, orient. čísla:					
42	názvy ulic, náměstí, řek		17	0	0.8	7
43	orientační, popisná čísla		17	0	1.0	3
	Značky BKOM:					
44	dopr. značka a SSZ	G1	2	0	0	7
	dopr. značka a lampa	G3	2	0	0	7
	dopr. značka, lampa a trakční sloup	G6	2	0	0	7

	dopr. značka a trakční sloup	G7	2	0	0	7
Vrstva	popis	buňka uživ.čára	prvek	typ	tloušťka výška	barva
44	dopr. značka, lampa a SSZ	G17	2	0	0	7
	dopr. značka, slavn. osvětlení	G31	2	0	0	7
	trakční sloup	G16	2	0	0	7
	trakční sloup a lampa	G5	2	0	0	7
	zastávka, lampa	G29	2	0	0	7
	zastávka, slavn. osvětlení	G30	2	0	0	7
	orientační sloupek	G21	2	0	0	7
	zahražovací sloupek	G32	2	0	0	7
	ochranná tyč	G33	2	0	0	7
	ovládací sloupek SSZ	G4	2	0	0	7
	směrový kůl	G10	2	0	0	7
	sklápěcí sloupek parkovací	G22	2	0	0	7
	koordinační skříň	G28	2	0	0	7
	lapač splavenin	G9	2	0	0	7
	lapol olejů	G11	2	0	0	7
	parkovací hodiny	G24	2	0	0	7
	reklama (linie)	G35	4	U	0	7
	zrcadlo	G12	2	0	0	7
	řadič	G13	2	0	0	7
	Portál-linie, portál-stojka	G19	2,4	0	0	7
	propustek	G25	4	U	0	7
	kamera	G35	2	0	0	7
	kamera na objektu	G35.1	2	0	0	7
	vyústění drenáže	G36	2	0	0	7
	zábrana kovová	zabrana	3,4,6	U	0	7
	zábrana betonová, plastová		3,4,6	0	0	7
	Ostatní kresba:					
45	ostatní kresba		3,4,15,16	0	0	0
46	stojany na kola - obrys		3,4,6,16	0	0	0
	stojany na kola - popis		2,17	0	0.4	0
	Popisy:					
49	popisy objektů (restaurace, ...)		2,17	0	0.4	0
	popisy materiálů (asfalt, ...)		2,17	1	0.4	0
	vysvětlivky		2,17	2	0.4	0
	Výšky objektů:					
50	výšková kóta		2,17	0	0.4	0
	popisy výšek obrubníků, zdí a zábradlí		2,17	1	0.4	0
	průřez potrubního vedení (mm)		2,17	2	0.4	0
52	popis křížků čtvercové sítě		17			
	směr k severu		2			

62	křížky čtvercové sítě		2, 35			
Vrstva	popis	buňka uživ.čára	prvek	typ	tloušťka výška	barva
63	Obrys stavby		3,4,15,16	4	4	9
	Výkres xxxxxx_v.dgn					
	Vodorovné dopravní značky ze zámkové nebo jiné dlažby					
45	vodor. dopr. značky (linie)		3,4,6,16	U	0	3
	vodor. dopr. značky (značky)		2	0	0	3
	Vodorovné dopravní značky červený nátěr:					
46	vodor. dopr. značky (linie)		3,4,6,16	U	0	3
	vodor. dopr. značky (značky)		2	0	0	3
	Vodorovné dopravní značky bílé:					
47	vodor. dopr. značky (linie)		3,4,6,16	U	0	0
	vodor. dopr. značky (značky)		2	0	0	0
	popis číslování park. stání		17	43	1.0x1.0	0
	Vodorovné dopravní značky žluté:					
48	vodor. dopr. značky (linie)		3,4,6,16	U	0	4
	vodor. dopr. značky (značky)		2	0	0	4
49	***Vodor.dopr.značky jiné***					
	Výkres xxxxxx_k.dgn					
5	dešťová kanalizace,		3,4,16	0	4	6
	dešťová zaolejovaná kan.		3,4,16	0	4	6
6	kanalizační přípojka		3,4,16	0	2	6
7	kanalizační šachta	6.200	2	0	0	6
8	oddělovací komora		6	3	0	6
9	oddělovač deště	6.220	2	0	0	6
10	odlehčovací stoka		3,4,16	0	4	6
11	oměrná		17,33	0	0.4	7
13	text, vč. výšky poklopu, mříže, odkazové čáry		3,4,17	0	0.4	6
14	vpusť, dešťový svod	6.301	2,15	0	0	6
15	žlabová vpusť (prahová)		6	0	0	6
16	vpusť v podchodu	6.301	2	3	0	6
17	podobrubníková vpusť		3,4	0	4	6
18	výška dna, odtoku,napojení (v závorce)		17	0	0.4	6
19	jímka, horská vpusť, lapač splavenin,odlučovač rop.látek		3,4,6,15,16	0	2	6
	drenážní šachta (pod terénem)		15	3	0	6
	retenční nádrž		3,4,6,15,16	3	2	6

20	stáv. kanalizace		3,4,16	3	0	1
Vrstva	popis	buňka uživ.čára	prvek	typ	tloušťka výška	barva
21	kanalizace po záhozu		3,4,16	3	4	6
22	kanalizační prvky jiné					
	Výkres xxxxxx_s.dgn					
5	elektroměrová skříň	6.661	2	0	0	10
6	koordinační skříň	G28	2	0	0	10
7	ovládací sloupek SSZ	G4	2	0	0	10
8	priska (rozměrná)		6	0	0	10
9	řadič (ovládá SSZ)	G13	2	0	0	10
10	SSZ na objektu	5.251	2	0	0	10
11	světelné signal. zařízení, závora,kamera	5.250, 5.171,G35	2	0	0	10
32	kabelovod, multikanál		3,4,16	0	4	0
	Kabel SSZ:					
12	kabel SSZ, kabel NN		3,4,16	0	4	10
	kabel SSZ nadzemní		3,4,16	2	4	10
13	kabel po záhozu		3,4,16	3	4	10
14	oměrná		17,33	0	0.4	2
15	text		17	0	0.4	10
16	kabelová spojka	6.641	2	0	0	10
17	chránička pro kabel SSZ	CHR	3,4,16	0	0	10
	Koordinační kabel metalický:					
18	koordinační kabel metalický		3,4,16	0	4	5
19	kabel po záhozu		3,4,16	3	4	5
20	oměrná		17,33	0	0.4	1
21	text		17	0	0.4	5
22	kabelová spojka	6.641	2	0	0	5
23	chránička pro k.k.metal.+detail	CHR	4,16	0	0	5
24	smyčka IDS		3,4,16	0	4	10
25	šachty			0	0	10
	Koordinační kabel optický:					
27	koordinační kabel optický		3,4,16	0	4	7
33	koordinační kabel opt.po záhozu		3,4,16	3	4	7
28	oměrná		17,33	0	0	7
29	text		17	0	0	7
30	kabelová spojka+romold	6.641	2,15	0	0	7
31	chránička pro k.k.opt.+detail	CHR	3,4,16	0	0	7
	Vyhledané kabely:					
51	Kabel vyhledaný		3,4,16	3	4	5
52	oměrné vyhledaných kabelů		17,33	0	0	1
53	texty		17	0	0	5

	Kabely zádržného systému:					
54	kabely zádrž. systému a zařízení		3,4,16	0	4	10
Vrstva	popis	buňka uživ.čára	prvek	typ	tloušťka výška	barva
55	kabely zádrž. systému po záhozu		3,4,16	3	4	10
56	texty a oměrné ZS		17,33	0	0	10
57	chráničky	CHR	3,4,16	0	0	10
58	indukční smyčka		3,4,16	0	0	10
	Kabely naváděcího systému:					
59	naváděcí tabule		6	0	0	10
60	kabely naváď. systému a zařízení		3,4,16	0	4	10
61	kabely NS po záhozu		3,4,16	3	4	10
62	texty a oměrné NS		17,33	0	0	10
63	chráničky	CHR	3,4,16	0	0	10
	Kabely jiné					
36	kabely SSZ z projektů		3,4,16	0	4	0
45	kabely KK z projektů		3,4,16	0	4	0
47	**Kabely neurčené**		3,4,16	0	4	0

Seznam zkratek pro popis povrchů:

l.a.	litý asfalt
asf.	asfalt
kam.	kámen
bet.	beton
z.dl.	zámková dlažba
r.z.dl.	reliéfní zámková dlažba
k.dl.	kamenná dlažba s uvedením rozměru
b.dl.	betonová dlažba s uvedením rozměru
r.b.dl.	reliéfní betonová dlažba s uvedením rozměru
zatr.dl.	dlažba ze zatravňovacích prefabrikátů
ker.dl.	keramické dlaždice
sil.pan.	silniční panely
tram.pan.	tramvajové panely
nezp.	nezpevněná plocha
b.o.	betonový obrubník
k.o.	kamenný obrubník
zk.b.o.	zkosený betonový obrubník
zk.k.o.	zkosený kamenný obrubník
dv.	dvouřádek ze dvou řad kam. kostek 10x10
b.v.p.	betonový vodící proužek
z.o.	záhonový obrubník
dr.k.	kam. kostka 10x10
v.k.	kam. kostka větší než 10x10
dist.dl.	distanční dlažba s uvedením rozměru
obl.	oblázky
moz.	mozaika

štěrk	štěrk
m.z.k.	mechanicky zpevněné kamenivo

Vysvětlivky:

vrstva	vrstva
buňka	prvek typu buňka, značka z normy ČSN 01 3411 nebo název značky z knihoven BKOM
uživ. čára	uživatelský typ čáry
prvek	typ prvku, např. buňka, úsečka, oblouk, text
typ	typ čáry
tloušťka	tloušťka čáry
výška	u textů znamená výšku písma
barva	barva
Gx	značka z knihoven BKOM

Barvy:

0	bílá
1	tmavomodrá
2	zelená
3	červená
4	žlutá
5	fialová
6	hnědá
7	světlomodrá
9	šedá
10	červenofialová

Typ čáry:

0	plná čára
2	krátce čárkovaná čára-nadzemní
3	dlouze čárkovaná čára-podzemní
U	uživatelský typ čáry

Typy prvků:

2	nesdílená značka, buňka (cell)
3	úsečka (line)
4	lomená čára (line string)
6	útvar (shape)
15	kružnice, elipsa
16	oblouk (arc)
17	text
33	kóta (dimension)
35	sdílená značka, buňka (shared cell)

3.4. **Specifické odpovědnosti**

Za kontrolu dodržování tohoto Mp je zodpovědný vydavatel.

4. SOUVISEJÍCÍ DOKUMENTY

4.1. **Dokumenty nadpodnikové úrovně**

ČSN 01 3410	
ČSN 01 3411	
ČSN EN ISO 9001	Systémy managementu kvality – Požadavky
ČSN EN ISO 14001	Systémy environmentálního managementu – Požadavky s návodem pro použití
ČSN ISO 45001	Systémy managementu bezpečnosti a ochrany zdraví při práci – Požadavky s návodem k použití
ČSN ISO/IEC 27001	Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky
ČSN 01 0391	Systém managementu společenské odpovědnosti organizací – Požadavky

4.2. **Podnikové dokumenty**

Mp-SÚ3200-02 Zaměření skutečného provedení stavby tunelu ve 3D
Mp-SÚ3200-04 Postup pro přebírání dokumentace skutečného provedení staveb (DSPS)

4.3. **Vystavené dokumenty**

Mp-SÚ3200-01-1 - vzor zaměření vjezdu
Mp-SÚ3200-01-2 - vzor tabulky uličních vpustí
Mp-SÚ3200-01-3 - vzor tabulky kanalizačních šachet
Mp-SÚ3200-01-4 - vzor vyhotovení podélného profilu kanalizace
Mp-SÚ3200-01-5 - vzor vyhotovení příčného profilu mostu
Mp-SÚ3200-01-6 - vzor vyhotovení podélného profilu mostu

5. ZÁVĚREČNÁ USTANOVENÍ

5.1. **Účinnost**

Tento Mp nabývá účinnosti dnem 01. 12. 2016.
Tímto vydáním Mp se ruší veškerá předchozí vydání a úpravy.

5.2. **Seznam příloh**

Příloha č. 1 - vzor zaměření vjezdu
Příloha č. 2 - vzor tabulky uličních vpustí
Příloha č. 3 - vzor tabulky kanalizačních šachet
Příloha č. 4 - vzor vyhotovení podélného profilu kanalizace
Příloha č. 5 - vzor vyhotovení příčného profilu mostu
Příloha č. 6 - vzor vyhotovení podélného profilu mostu

5.3. **Rozdělovník**

Zaměstnanci s uživatelským účtem obdrží ON v systému DMS. Zaměstnanci bez tohoto přístupu jsou seznámeni s dokumentací v její listinné podobě, uložené u správce řízené dokumentace (+ po jednom výtisku obdrží zhotovitel).

PŘÍLOHA Č.1

ZAMĚŘENÍ VJEZDU

KATASTRÁLNÍ ÚZEMÍ: (např. TRNITÁ)

STAVBA: (např.VJEZD DO GARÁŽE ROD. DOMKU + adresa + parc.č.)

ZHOTOVITEL STAVBY: (název firmy + adresa)

ZHOTOVITEL GEODETICKÉ DOKUMENTACE: (název firmy + adresa)

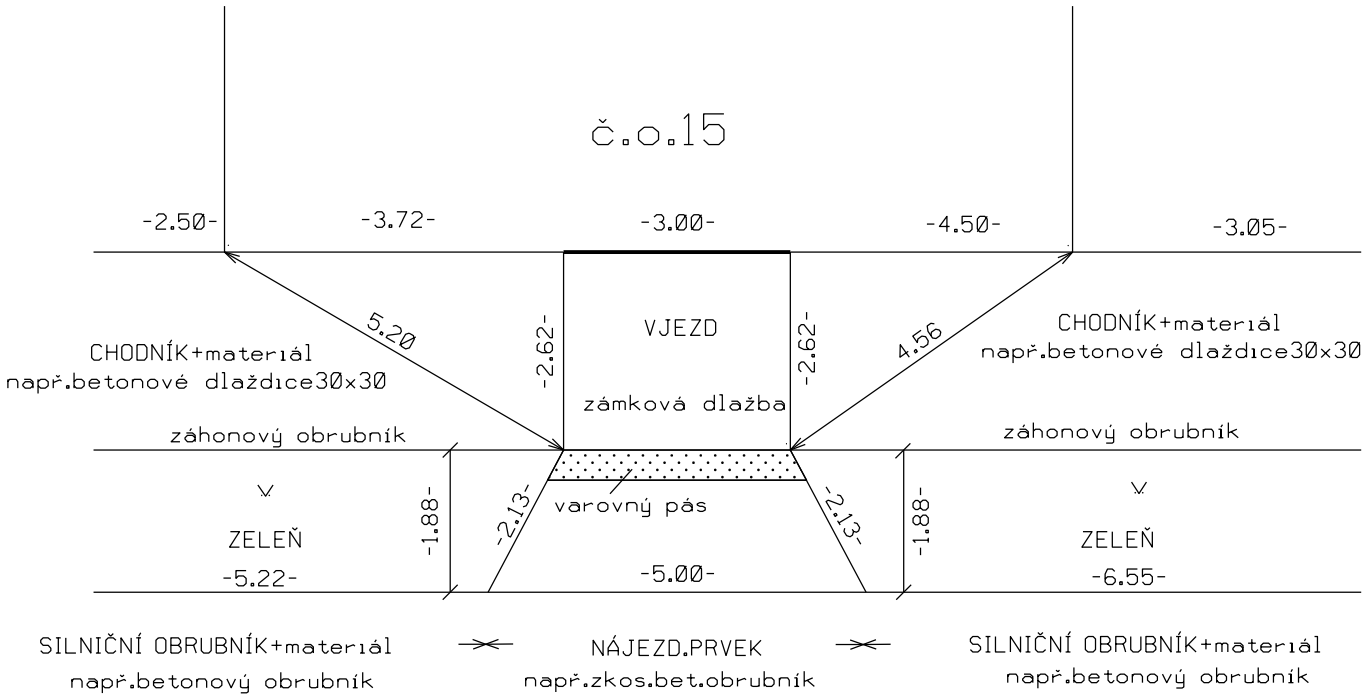
PROJEKTANT: (název firmy + adresa)

INVESTOR: (název firmy + adresa)

SKLADBA KONSTRUKCE VJEZDU: např.- BET.ZÁMK.DLAŽBA TL. 80mm
- DRŤ 4-8 TL. 40mm
- SC C8/10 TL. 150mm
- ŠD TL. 150mm

CELKEM 420mm

MĚŘÍTKO: (např. 1:100)



ŽIVIČNÝ POVRCH

ULICE MASNÁ

SILNIČNÍ OBRUBNÍK+materiál např.betonový obrubník

PŘÍLOHA Č. 2

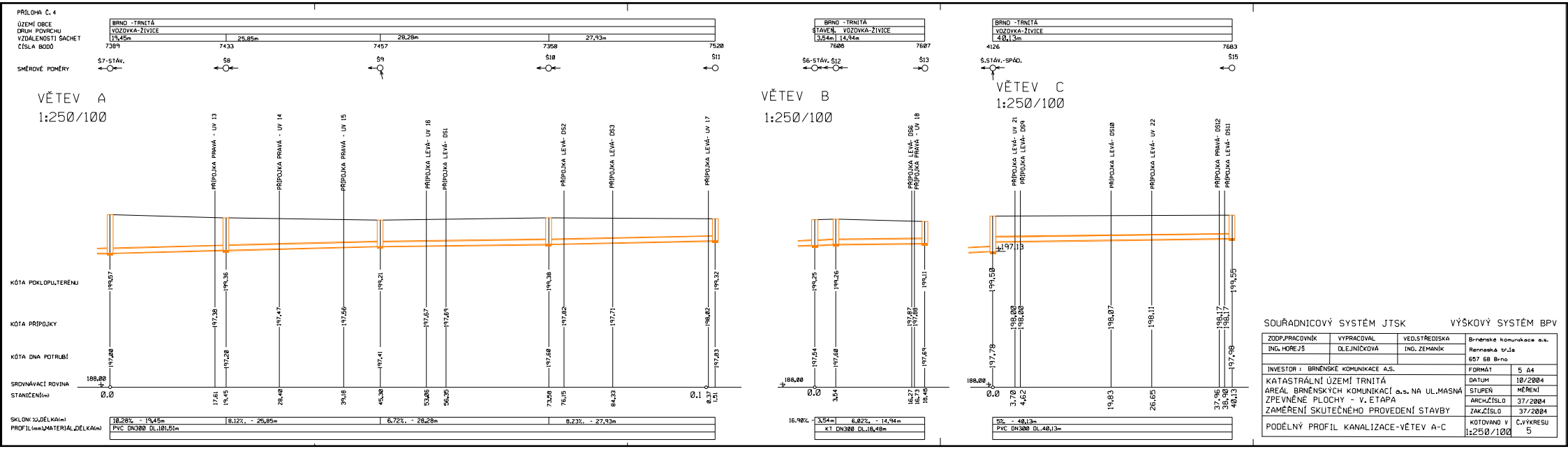
TABULKA ULIČNÍCH VPUSTÍ

číslo vpusti	číslo bodu	výška mříže	výška dna vpusti	výška vyústění	výška zaústění	délka přípojky	materiál průměr	zaústění do	poznámka
UV 1									
UV 2									
UV 3									
UV 4									
UV 5									
UV 6									
UV 7									
UV 8									
UV 9									
UV 10									
UV 11									
UV 13									
UV 14									
UV 15									
UV 16									
UV 17									

PŘÍLOHA Č. 3

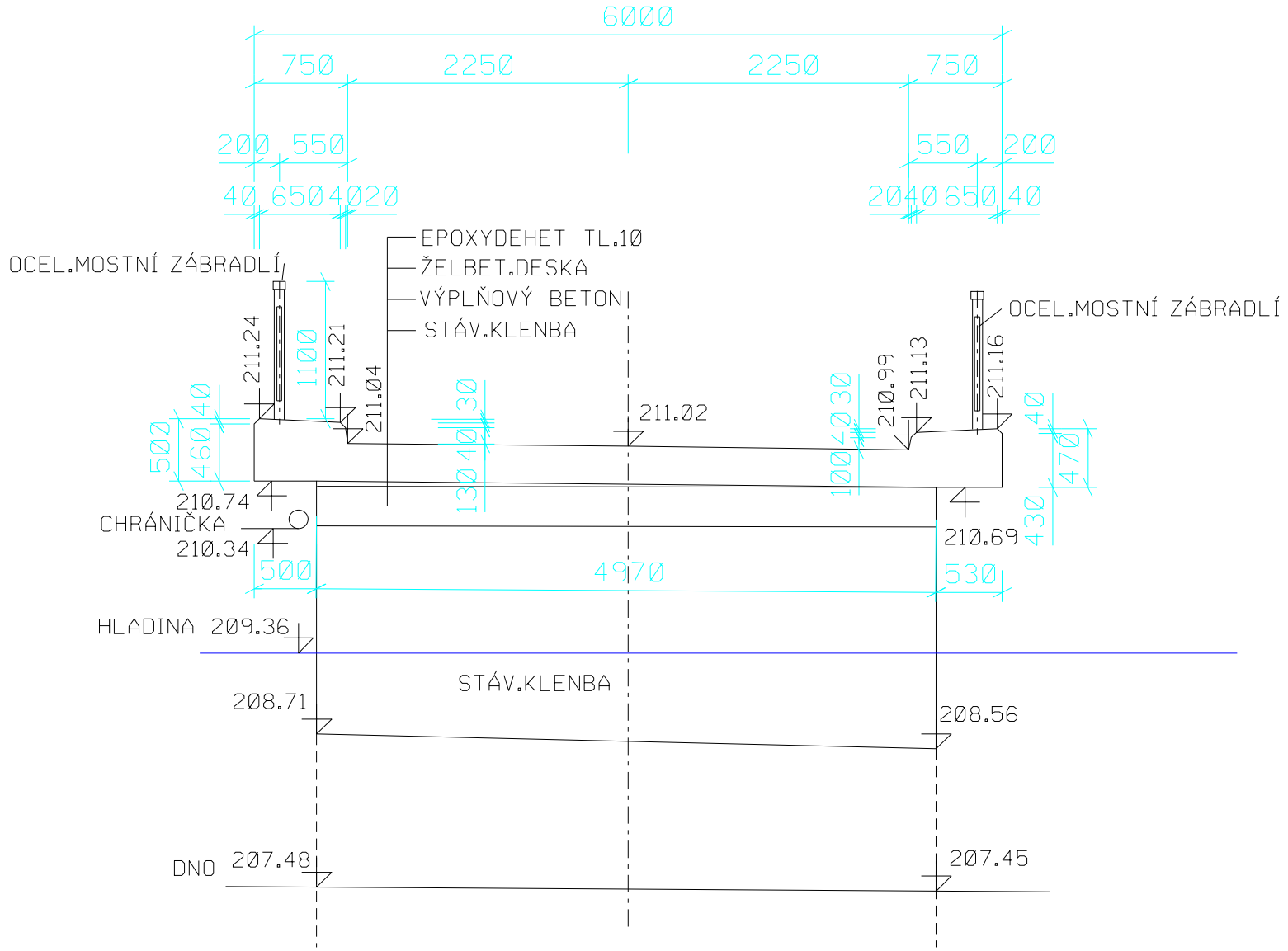
TABULKA KANALIZAČNÍCH ŠACHET

číslo šachty	číslo bodu	výška poklopu	výška dna šachty	výška přítoku	výška odtoku	poznámka MATERIÁL
Š1						
Š2						
Š3						
Š4						
Š5						
Š6						
Š7						
Š8						
Š9						
Š10						
Š11						
Š13						
Š14						
Š15						
Š16						
Š17						

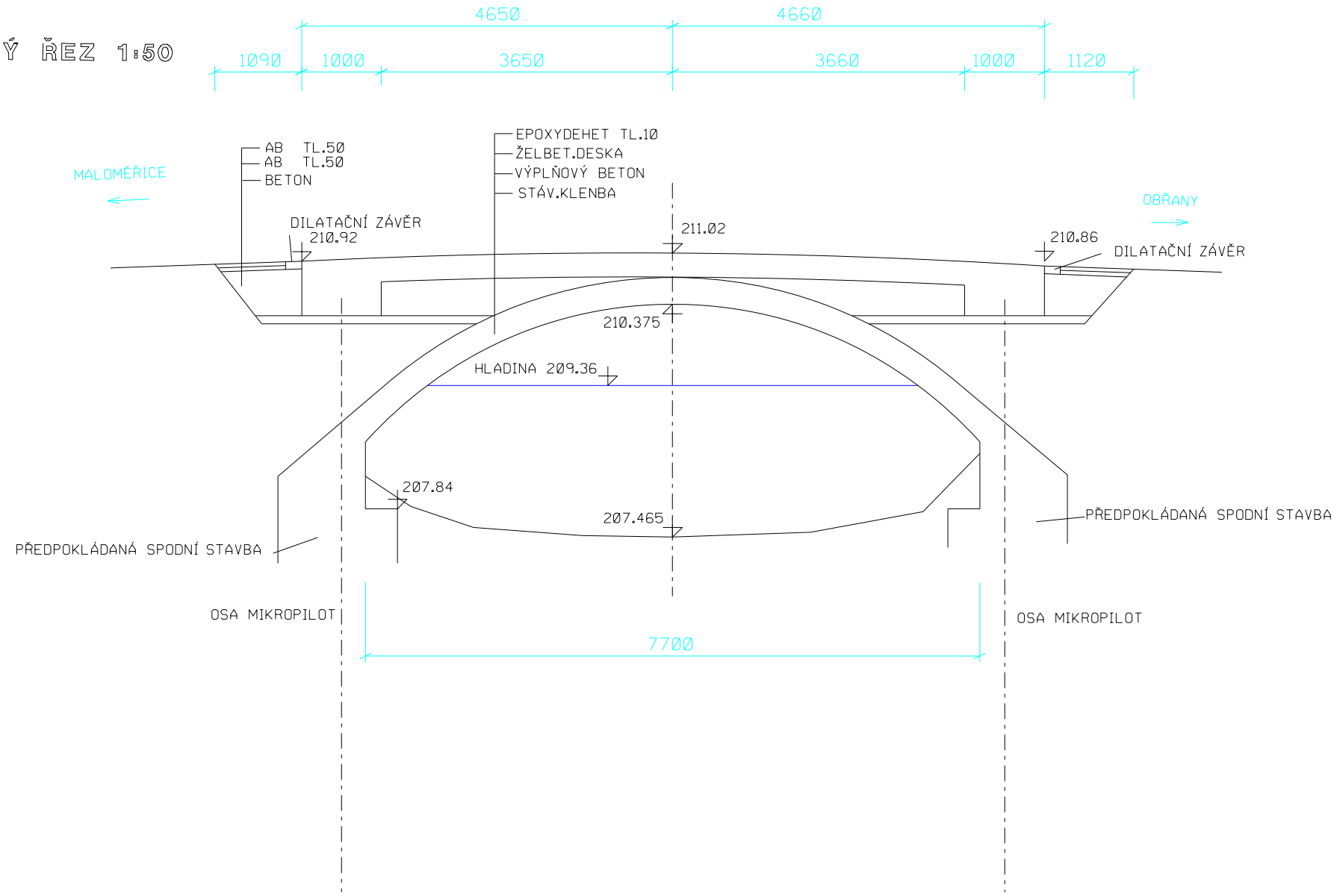


priloha 4_v8.dgn 17.7.2012 14:25:54

PŘÍČNÝ ŘEZ 1:50



PODÉLNÝ ŘEZ 1:50



Protokol o připojení dopravního řadiče k dopravní ústředně SSZ (VZOR)

Datum: 22. 2. 2022	**Číslo křižovatky - název křižovatky**				typ řadiče
Název testu:	**Vyhověl**	**Nevyhověl**	**Podpis**		**Poznámka: zdůvodnění, soupis poruch**
Poruchy světelných zdrojů	ano		Provozní úsek		
Test detektorů - jejich funkce	ano				
Test výpadku napájení řadiče	ano				
Kontrola výstroje řadiče dle PD.	ano				
Test výpadku komunikací CTD - řadič včetně následného přenosu dat	ano		CTD		
Test převzetí řízení křižovatky z CTD po ztrátě komunikace s řadičem	ano				
Test obousměrného přechodu řízení CTD - lokal	ano				
Přepínání SP, správné číslování SP	ano				
Vypnutí a zapnutí dynamického řízení	ano				
Vizualizace SP včetně detektorů	ano				
Preference MHD včetně vizualizace na DÚ	ano				
Provádění úprav konfigurace řadiče z DÚ (JAUT, SP, fázové přechody, parametry řízení atd.)	ano				
Kompletní test VIP tras	ano				
Kompletní test IZS tras	ano				
Kontrola řízení na křižovatce dle DŘ - SP, fázové přechody, logika řízení atd.	ano		ÚDI		
Závěr:	**ano**		CTD		

Obsah DŘ

- Průvodní zpráva (současný stav křižovatky z pohledu řízení, výchozí podklady, popis širších dopravních vztahů, situační řešení, dopravní značení, stavební úpravy, základní charakteristika řízení, popis způsobu řízení, tabulka mezičasů, detekce účastníků silničního provozu, požadavky na zařízení pro preferenci MHD, ruční řízení, závěry projednání a ostatní požadavky)
- Tabulková data, schéma rozmístění návěstidel
- Schéma fází
- Signální skupiny
- Matice konfliktů, tabulka mezičasů
- Fázové přechody
- Postupový diagram – logika řízení (detektory, detekční body MHD, přihlašovací úseky MHD, časové parametry MHD, proměnné, konstanty, parametry, pre-logika, hlavní logika, logika, post-logika, vedlejší logika, použité funkce atd.)
- Signální plány (dynamický, pevný, aktivační, deaktivační plán a pomocné plány)
- Fázové plány
- Speciální signální plán – VIP (schéma fází pro signální plány IZS, fázové přechody pro signální plány IZS, schéma fází pro signální plány VIP, fázové přechody pro signální plány VIP)
- Týdenní automatika,
- Koordinační schémata
- Závěr

Příloha 14.10

Vzor pásového diagramu pro on-line vizualizaci

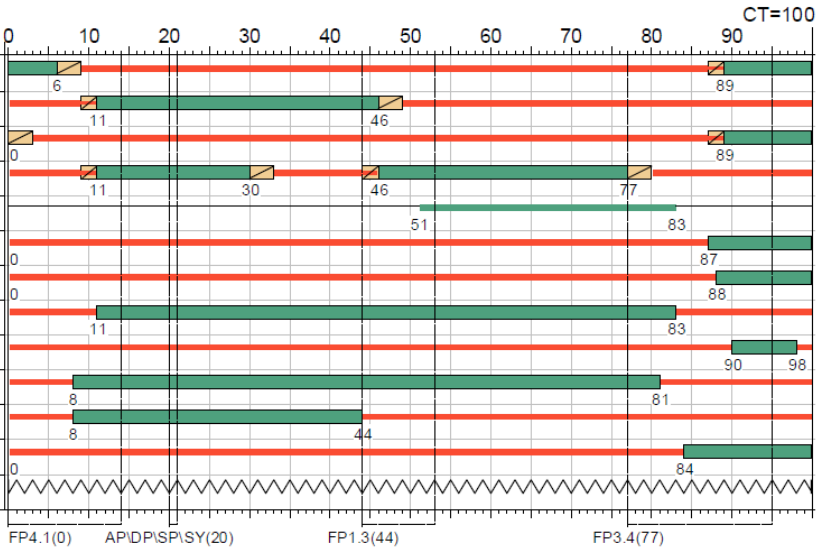
Signální plány s pevnou délkou cyklu (pevné i dynamické) musí být naprogramovány tak, aby se při vizualizaci daného SP na DÚ i v řadiči (na zobrazovacím zařízení řadiče nebo na připojeném PC) zobrazovala taková hodnota Tx a takové časy (vteřiny signálního plánu) změn stavů jednotlivých signálních skupin, jaké jsou uvedeny v DŘ. Tyto hodnoty Tx a časy změn stavů musí být takové, jaké by byly v případě, že by se daný SP opakoval od začátku aktuálního roku, přičemž 1. ledna v čase 00:00:01 by probíhala 1. vteřina SP dle DŘ. Na všech takto správně naprogramovaných řadičích pak ve stejném čase za použití SP se stejnou délkou cyklu probíhá stejná vteřina SP. Toto pravidlo musí být dodrženo i pro SP vytvářené či měněné prostřednictvím DÚ nebo servisní aplikace – zadané hodnoty spínání jednotlivých signálních skupin v SP se musí stejně zobrazovat ve vizualizaci a musí být správně umístěny v čase. Při přepínání mezi různými SP musí řadič nejpozději do 3 cyklů zkoordinovat aktuální SP tak, aby byl správně umístěn v čase. Během tohoto procesu koordinace (nejdéle 3 cykly) nemusí hodnoty Tx a časy změn stavů ve vizualizaci odpovídat DŘ. Koordinace musí probíhat mimo oblasti fázových přechodů (standardně v přepínacím bodě definovaném v DŘ), a nesmí je tedy ovlivnit.

Příklad č. 1 – Pevný SP s délkou cyklu 100 s

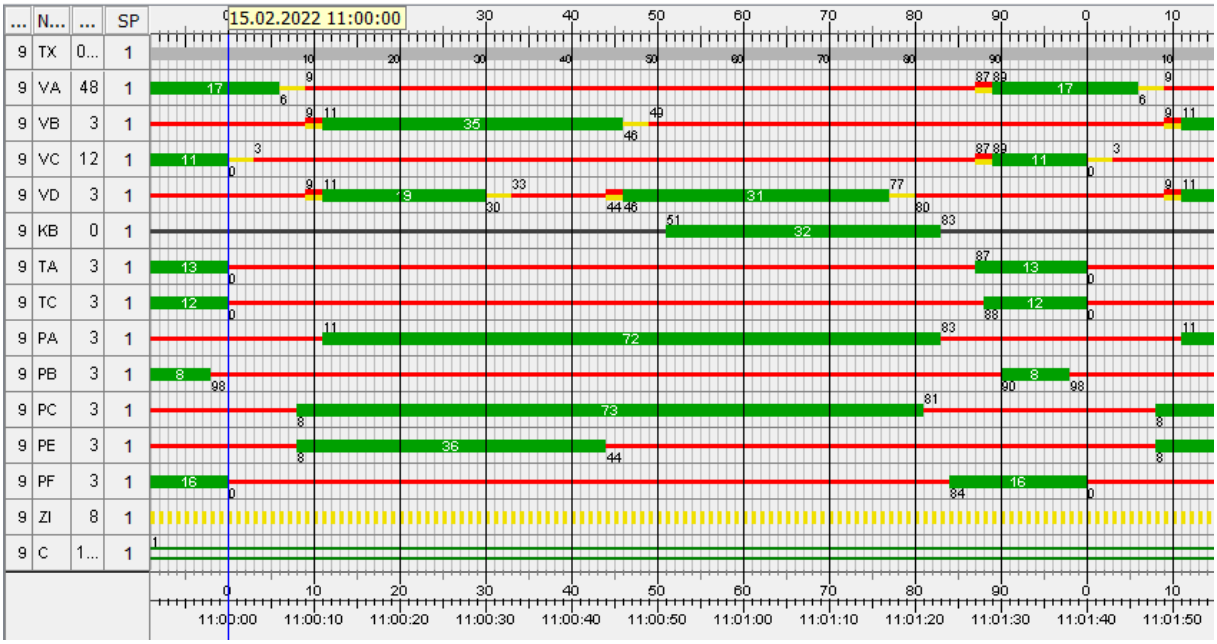
Na Obr. 1 je vzor pevného SP s délkou cyklu 100 s specifikovaného v DŘ. Pokud je tento SP spuštěn, musí fungovat a zasílat hodnoty pro vizualizaci tak, jako kdyby se v této podobě opakoval od začátku aktuálního roku, přičemž by hodnota 0 (zde např. konec zelené pro VC) odpovídala času 00:00:00 1. ledna (u délky cyklu 60, 80, 100 a 120 s se hodnoty opakují stejně v každé hodině každého dne). Na Obr. 2 je vidět správné fungování a vizualizace požadovaného SP – v čase 11:00:00 je hodnota Tx 0 a vteřina změny skupiny VC (konec zelené) je také zobrazena jako 0. Podobně pak v čase 11:00:06 je u změny skupiny VA zobrazena hodnota 6, atd.

Pevny 100s

Signal group	Init	Term	Init2	Term2	GT
VA	87	6			17
VB	9	46			35
VC	87	0			11
VD	9	30	44	77	50
KB	51	83			32
TA	87	0			13
TC	88	0			12
PA	11	83			72
PB	90	98			8
PC	8	81			73
PE	8	44			36
PF	84	0			16
ZI					100



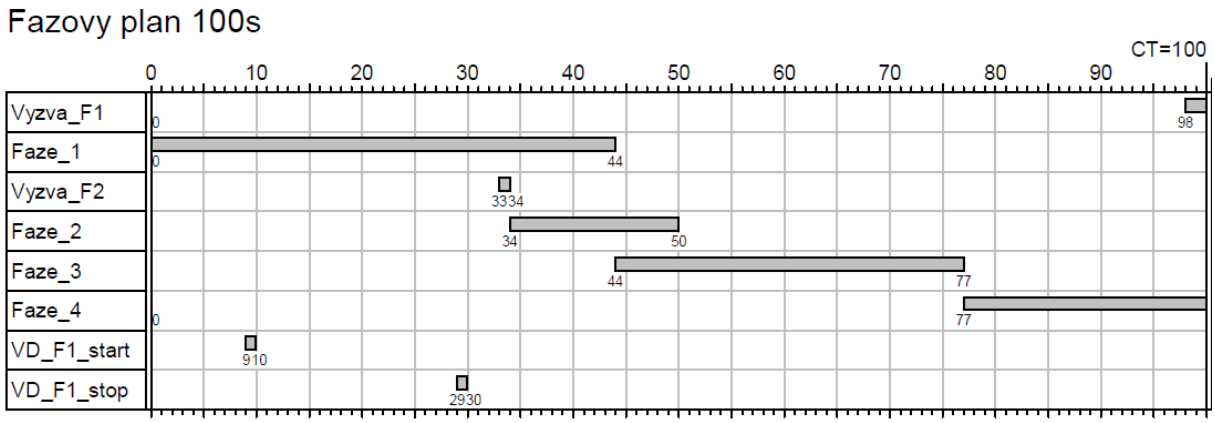
Obrázek 1



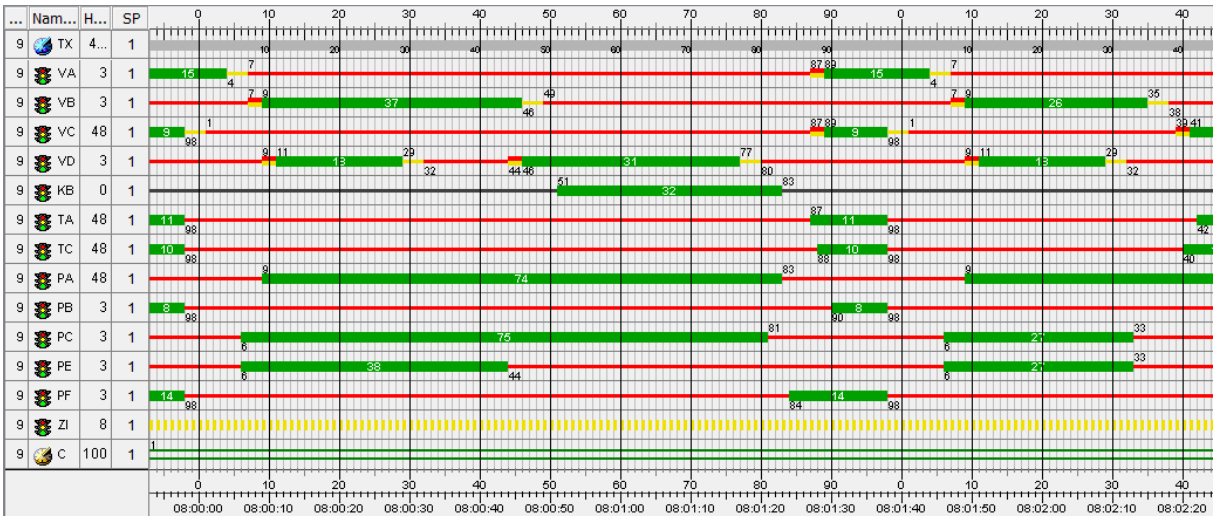
Obrázek 2

Příklad č. 2 – Dynamický (fázový) SP s délkou cyklu 100 s

Na Obr. 3 je vzor dynamického (fázového) SP s délkou cyklu 100 s specifikovaného v ĎR. V tomto dynamickém plánu je fáze 3 vždy ukončována v 77. vteřině cyklu. Fáze 1 pak může končit mezi 33. a 44. vteřinou cyklu. Na Obr. 4 je vidět správné fungování a vizualizace tohoto SP. V čase 08:01:17 je ukončena fáze 3 (konec druhé zelené pro VD) a hodnota Tx je 77. Toto by se opakovalo o 100 s později (1 cyklus) v čase 08:02:57 opět s hodnotou Tx 77. Konec fáze 1 (konec zelené pro PE) se v zobrazených cyklech liší, v čase 08:00:44 ve 44. vteřině cyklu, v čase 08:02:13 pak v 33. vteřině cyklu, což opět odpovídá předloze.



Obrázek 3



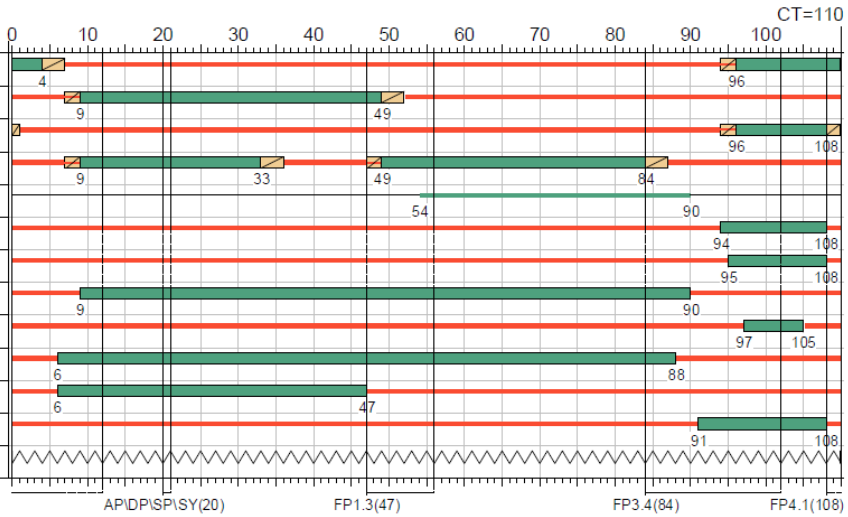
Obrázek 4

Příklad č. 3 –Pevný SP s délkou cyklu 110 s

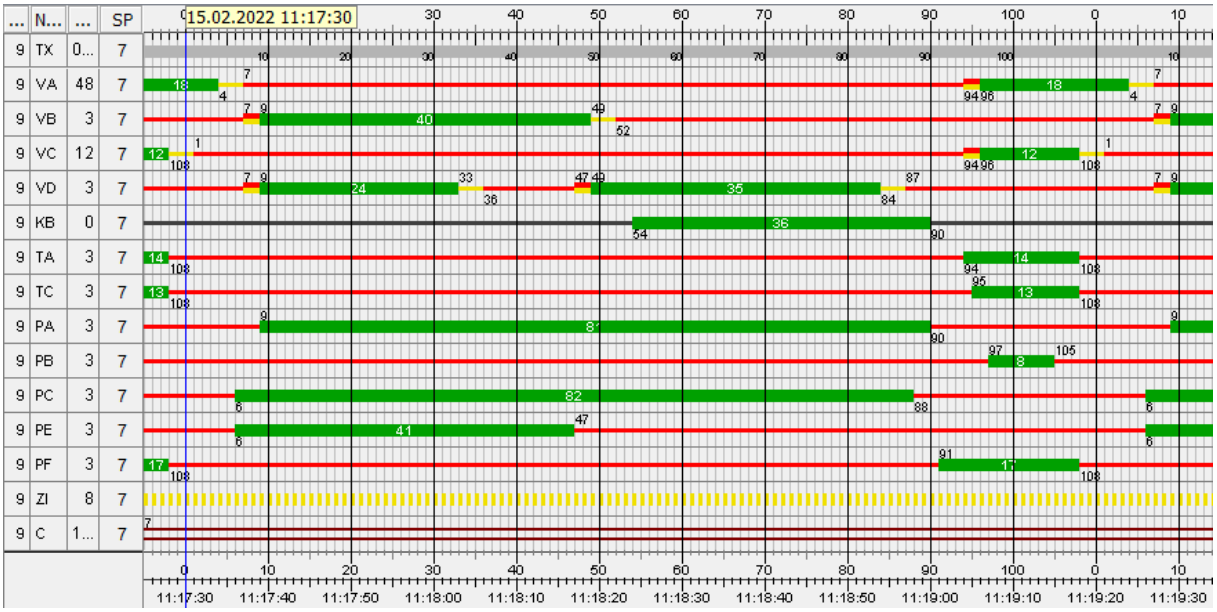
Na Obr. 5 je vzor pevného SP s délkou cyklu 110 s specifikovaného v DŘ. Protože se do jednho dne nevejde celý počet cyklů s délkou 110 s, je důležité brát v potaz konkrétní den spuštění SP. Pro den 15. 2. 2022 vychází začátek cyklu (Tx = 0) např. pro čas 11:17:30. Na Obr. 6 je vidět správné fungování a vizualizace tohoto SP. V čase 11:17:34 je ukončena zelená pro VA a je zobrazena 4. vteřina cyklu. O 110 s později se toto opakuje – v čase 11:19:24 se ve 4. vteřině cyklu ukončuje zelená pro VA.

Pevny 110s

Signal group	Init	Term	Init2	Term2	GT
VA	94	4			18
VB	7	49			40
VC	94	108			12
VD	7	33	47	84	59
KB	54	90			36
TA	94	108			14
TC	95	108			13
PA	9	90			81
PB	97	105			8
PC	6	88			82
PE	6	47			41
PF	91	108			17
ZI					110



Obrázek 5



Obrázek 6

Návrh koncepce rozmístění kamer na křižovatkách

Technická specifikace zadavatele kamer umísťovaných do křižovatek SSZ v Brně.

Každá nová křižovatka (i rekonstrukce) bude v následující konfiguraci připravena na umístění níže uvedených kamer.
Křižovatka tvaru „T“ bude mít 3x fixní + 1 otočnou kameru
Křižovatka tvaru „X“ bude mít 4x fixní + 1 otočnou kameru.
Pro každou kameru je potřeba doplnit příslušný počet licencí do Video Management Software (VMS) Genetec Security Center Omnicast 5.11.1.0

Fixní kamera s parametry:

- umístění – jedna kamera v jednom jízdním směru
- minimálně 4.0Mpx (rozlišení 2560x1440)
- kódování H264 profily main a high
- kódování H265 – main profile
- varifokální objektiv s IR korekcí, světelnost 1.5 a nižší - snímací čip max. 1/1.8“
- snímací rychlost min. 100 snímků za sekundu
- citlivost pro den 0,02 lux při 50 IRE F 0.9 (pro 1080 p při 25 snímcích za sekundu)
- citlivost pro noc 0,004 lux při 50 IRE F 0.9 (pro 1080 p při 25 snímcích za sekundu)
- možnost připojení na otočnou hlavici (PTZ)
- slot pro paměťovou kartu s lokálním záznamem v případě výpadku konektivity
- možnost instalace analytických softwarových aplikací třetích stran přímo v kameře, např. počítání objektů, detekce pohybu, stojící vozidlo, čtení RZ, (typy aut, autobusy, kamiony...)
- ARTPEC 8, DLPU pro strojové učení, kybernetická bezpečnost
- Podpora vícenásobného video streamingu (minimum 2x 1080p,30 fps současný stream)
- vyrobeno v EU

Otočná přehledová kamera s parametry:

- umístění na sloupu min. 6m vysoko (nejlépe VO nebo TS), aby pokryla 100% celou křižovatku
- minimálně full HD (1080 p)
- kódování H264 profily main a high
- kódování H265 - minimálně 31x ZOOM
- snímací čip max. 1/2“
- citlivost pro den 0,06 lux při 30 IRE F 1.6
- citlivost pro noc 0,001 lux při 30 IRE F 1.6
- slot pro paměťovou kartu s lokálním záznamem v případě výpadku konektivity
- Možnost instalace analytických softwarových aplikací třetích stran přímo v kameře, např. počítání objektů, detekce pohybu, stojící vozidlo stojící vozidlo, čtení RZ, (typy aut, autobusy, kamiony...)
- kybernetická bezpečnost
- podpora vícenásobného video streamingu (minimum 2x 1080p,30 fps současný stream)
- vyrobeno v EU

Datová infrastruktura:

Kamery budou propojeny do MKDS z rozvaděče na křižovatce, kde bude zakončena optická trasa propojující rozvaděč se serverovnou Brněnských komunikací a.s.
Kabeláž ze sloupů do rozvaděče bude použita kategorie 6A a napájení přes PoE+ (30W) v případě fixních kamer a PoE++ (60W) v případě kamery otočné.
Jako injektor slouží průmyslový switch, který má 8 portů v konfiguraci min. 6x PoE+, 2x PoE++ a 2x SFP pro připojení optické trasy.
Napájení zajišťuje průmyslový záložní zdroj min. 300W na DIN lištu s baterií min 72Ah.

Záznam:

Pro ukládání záznamů je nutno doplnit diskové pole MKDS o příslušný počet disků dle této specifikace z provozního řádu MKDS:

Diskové pole

Jako úložiště slouží robustní diskové pole výrobce NEXSAN osazeno disky o kapacitě 6TB s rozhraním NL-SAS. Pro připojení jedné kamery je třeba kapacity 3TB, na každé dvě kamery je třeba počítat s jedním 6TB diskem.

K rozšíření kapacity bude použito výhradně disků certifikovaných a dodaných výrobcem diskového pole a zamezí se tak případné nekompatibilitě a tím pádem problémům, které by měly dopad na fungování úložiště.

Pokud jsou v diskovém poli ještě volné sloty lze doplnit pouze disky, pak se dokupují pouze disky v následujících bundlech:

E48V(T) / E48XV 8x6TB 7.2K Drives	P/N: DP48V-48N/6
E48V(T) / E48XV 16x6TB 7.2K Drives	P/N: DP48V-96N/6

Pokud je nabízená konfigurace plná, musí se doplnit disky + expanzní police. K dispozici jsou následující bundle:

E48XV 16x6TB 7.2K	P/N: E48XVR96N/6
E48XV 32x6TB 7.2K	P/N: E48XVR192N/6

Klientská stanice:

Optimální konfigurace klientské stanice firmou Genetec pro Security Center 5.11 je:

- 4tá Generace Intel Core™ I7-4770 nebo vyšší
- 32 GB RAM
- 64bit operační systém Windows
- 256 GB Solid State Drive karta na PCI express
- Gigabit Ethernet síťová karta
- NVIDIA* GeForce GTX 1060 6 GB video karta na každé 2 monitory
- 32“ 4K IPS monitor