

SŽ čj. 509/2025-SŽ-SŽT-NKB

Provozní politika prvků v působnosti systému řízení bezpečnosti informací

účinnost zveřejněním v eDAP

Schváleno pod čj. 509/2025-SŽ-SŽT-NKB
dne

Bc. Jiří Svoboda, MBA
generální ředitel

SŽ čj. 509/2025-SŽ-SŽT-NKB**Provozní politika prvků v působnosti systému řízení bezpečnosti informací**

Gestorský útvar: Správa železnic, státní organizace
Správa železniční telematiky
V Celnici 1028/10,110 00 Praha 1
spravazeleznic.cz
Rok vydání: 2025
Náklad: vydáno pouze v elektronické podobě

© Správa železnic, státní organizace, 2025

Tento dokument je duševním vlastnictvím státní organizace Správa železnic, na které se vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů. Státní organizace Správa železnic je v uvedené souvislosti rovněž vykonavatelem majetkových práv. Tento dokument smí fyzická osoba použít pouze pro svou osobní potřebu, právnická osoba pro svou vlastní vnitřní potřebu. Poskytování tohoto dokumentu nebo jeho části v jakékoli formě nebo jakýmkoli způsobem třetí osobě je bez svolení státní organizace Správa železnic zakázáno.

ZÁZNAMY O OPRAVÁCH A ZMĚNÁCH

Držitel listinné podoby tohoto dokumentu je odpovědný za včasné a správné zapracování účinných oprav a změn a za provedení příslušného záznamu.

oprava/změna a její pořadové číslo	číslo jednací	účinnost od	opravu/změnu zapracoval

OBSAH

	strana
ROZSAH ZNALOSTÍ.....	5
ZKRATKY A ZNAČKY.....	6
1 ÚČEL A ROZSAH POLITIKY	8
2 PŮSOBNOST POLITIKY	8
3 VYMEZENÍ ZÁKLADNÍCH POJMŮ	8
4 ODPOVĚDNOSTI A ROLE.....	8
5 POŽADAVKY NA DOKUMENTACI.....	10
6 ŘÍZENÍ PROVOZU	12
7 BEZPEČNOST KOMUNIKACÍ.....	16
8 ŘÍZENÍ PŘÍSTUPU	20
9 ŘÍZENÍ TECHNICKÝCH ZRANITELNOSTÍ.....	26
10 ZÁLOHOVÁNÍ A OBNOVA	28
11 OCHRANA PŘED ŠKODLIVÝM KÓDEM	31
12 LOGOVÁNÍ A MONITORING	32
13 ŘÍZENÍ ZMĚN	37
14 AKVIZICE, VÝVOJ A ÚDRŽBA.....	39
15 SOFTWAREVÉ LICENCE	43
16 SERVICEDESK	44
17 BEZPEČNÉ PŘEDÁVÁNÍ A VÝMĚNA INFORMACÍ	45
18 OCHRANA OSOBNÍCH ÚDAJŮ	47
19 ZÁVEREČNÁ USTANOVENÍ	47
SOUVISEJÍCÍ DOKUMENTY.....	49
Příloha A (normativní) Krycí list aktiva	50
Příloha B (normativní) Vzor Zprávy z přezkoumání přístupových oprávnění	51

ROZSAH ZNALOSTÍ

Níže uvedená tabulka stanovuje rozsah znalostí tohoto dokumentu pro pracovní zařazení (funkci) nebo činnost, přičemž:

- informativní znalostí se rozumí taková znalost, při které příslušný zaměstnanec má povědomí o tomto dokumentu, zná předmět jeho úpravy a při náhledu do příslušného ustanovení je schopen se podle takového ustanovení samostatně řídit nebo podle něj samostatně konat;
- úplnou znalostí se rozumí taková znalost, při které příslušný zaměstnanec má povědomí o tomto dokumentu, zná předmět jeho úpravy a bez náhledu do příslušného ustanovení je schopen se podle takového ustanovení samostatně řídit nebo podle něj samostatně konat;
- doslovnou znalostí se rozumí taková znalost, při které příslušný zaměstnanec zná text, který je v příslušném ustanovení napsán v uvozovkách kurzivou, přesně a je schopen jej bez náhledu do příslušného ustanovení samostatně reprodukovat.

Není-li rozsah znalostí pro pracovní zařazení (funkci) nebo činnost stanoven, stanoví rozsah znalostí, pokud je tak třeba učinit, příslušný vedoucí zaměstnanec.

pracovní činnost nebo zařazení (funkce)	znalost ustanovení
ředitelé odborů O14, O24, O30 GR	úplná: celý předpis
ředitel CTD	úplná: celý předpis
ředitel SŽT	úplná: celý předpis
zaměstnanci O14, O17, O24, O30 GR	informativní: celý předpis
zaměstnanci CTD	informativní: celý předpis
zaměstnanci PŘP	informativní: celý předpis
zaměstnanci SŽT	úplná: celý předpis
gestoři/vlastníci aplikací (informačních systémů)	úplná: celý předpis
garanti primárních/podpůrných aktiv	úplná: celý předpis

ZKRATKY A ZNAČKY

Níže uvedený seznam obsahuje zkratky a značky použité v tomto předpisu. V seznamu se neuvádějí legislativní zkratky, zkratky a značky obecně známé, zavedené právními předpisy, uvedené v obrázcích, příkladech nebo tabulkách.

AD	adresářová služba (z angl. <i>Active Directory</i>)
BS	bezpečnostní správce
CD	optický datový nosič (z angl. <i>Compact Disc</i>)
CTD	Centrum techniky a diagnostiky
CMDB.....	konfigurační databáze (z angl. <i>Configuration Management Database</i>)
DB.....	databáze
DVD.....	digitální optický datový nosič (z angl. <i>Digital Versatile Disc</i>)
EAP.....	typ počítačového komunikačního protokolu (z angl. <i>Extensible Authentication Protocol</i>)
eDAP.....	elektronická knihovna dokumentů a předpisů
FW.....	bezpečnostní bariéra (z angl. <i>Firewall</i>)
GŘ.....	generální ředitelství
HW	hardware
ICT	informační a komunikační technologie
IdM.....	správa identit (z angl. <i>Identity Management</i>)
IDS/IPS.....	technický systém detekce průniku do IS (z angl. <i>Intrusion Detection System / Intrusion Prevention System</i>)
IS.....	Informační systém
LDAP.....	protokol pro přístup/ukládání dat na adresářovém serveru (z angl. <i>Lightweight Directory Access Protocol</i>)
MS.....	Microsoft
Midd	software pro funkce nad rámec služeb operačního systému (z angl. <i>Middleware</i>)
NB	notebook
O10	odbor personální (SŽ)
O14	odbor zabezpečovací a telekomunikační techniky (SŽ)
O17	odbor interního auditu (SŽ)
O24	odbor elektrotechniky a energetiky (SŽ)
O30	odbor bezpečnosti a krizového řízení (SŽ)
OS.....	operační systém
OJ	organizační jednotka
PRP.....	(oddělení) Podpory řízení provozu
PC	osobní počítač
RADIUS.....	protokol pro přístup k síti/IP mobilitu (z angl. <i>Remote Authentication Dial In User Service</i>)
SLA.....	úroveň poskytované služby (z angl. <i>Service Level Management</i>)
SSH	program/zabezpečený komunikační protokol v počítačových sítích (z angl. <i>Secure Shell</i>)
SSO	jednotná identita (z angl. <i>Single Sign On</i>)
SW	software

SŽSpráva železnic, státní organizace

SŽTSpráva železniční telematiky

TACACS+vzdálený autentizační protokol (z angl. *Terminal Access Controller Access-Control System*)

TLSbezpečnost transportní vrstvy (z angl. *Transport Layer Security*)

UXUnix (Linux)

USBuniverzální sériové rozhraní (z angl. *Universal Serial Bus*)

VLAN.....virtuální lokální síť (z angl. *Virtual Local Area Network*)

VPNvirtuální privátní síť (z angl. *Virtual Private Network*)

VRF VPNvirtuální směrování a přeposílání (z angl. *Virtual Routing and Forwarding*)

Generální ředitel schválil podle čl. 14 odst. 1 a čl. 15 Statutu státní organizace Správa železnic (dále jednotlivě jen „Statut“ a „SŽ“) tento předpis SŽ čj. 509/2025-SŽ-SŽT-NKB Provozní politika prvků v působnosti systému řízení bezpečnosti informací.

1 ÚČEL A ROZSAH POLITIKY

Cílem předpisu SŽ čj. 509/2025-SŽ-SŽT-NKB Provozní politika prvků v působnosti systému řízení bezpečnosti informací (dále jen „předpis“) je stanovit požadavky na bezpečnostní opatření při provozování a rozvoji aktiv (prvků) v působnosti systému řízení bezpečnosti informací, definovat pravomoci a odpovědnosti bezpečnostních a provozních rolí a dále upřesnit požadavky předpisu SŽ čj. 2462/2024-SŽ-SŽT-NKB Politika systému řízení bezpečnosti informací (dále jen „Politika systému řízení bezpečnosti informací“) v této oblasti. Zároveň předpis v jednotlivých kapitolách určuje, jaké mají být použity postupy a procesy. Vymezení základních pojmů pro celou bezpečnostní dokumentaci kybernetické bezpečnosti je uvedeno v Politice systému řízení bezpečnosti informací.

2 PŮSOBNOST POLITIKY

Tento předpis a požadavky z něj vyplývající jsou závazné pro všechna aktiva (prvky) v působnosti systému řízení bezpečnosti informací. Veškeré výjimky z požadavků stanovených tímto předpisem zpracují Garanti primárních aktiv do Krycího listu aktiva (viz článek 5.2 tohoto předpisu) a následně jsou řízeny a schvalovány podle platného postupu pro řízení výjimek uvedeného v Politice systému řízení bezpečnosti informací.

3 VYMEZENÍ ZÁKLADNÍCH POJMŮ

3.1 **Mitigace rizika** – realizace opatření za účelem minimalizace daného rizika, která mohou, ale obvykle nevedou k jeho úplné eliminaci.

Proxy/Proxy server – server, který zabezpečuje, zajišťuje, odbavuje požadavky od svých klientů jejich přeposláním na jiné servery.

Servicedesk – hardware (dále jen „HW“), software (dále jen „SW“), procesy a pracovníci poskytující pomoc Uživatelům při řešení požadavků a incidentů týkajících se zpravidla výpočetní techniky.

3.2 Vymezení dalších základních pojmů pro celou bezpečnostní dokumentaci kybernetické bezpečnosti je uvedeno v Politice systému řízení bezpečnosti informací.

4 ODPOVĚDNOSTI A ROLE

4.1 Bezpečnostní správce

4.1.1 Pravomoci a odpovědnosti Bezpečnostního správce definuje předpis Politika organizační bezpečnosti čj. 2811/2023-SŽ-SŽT-NKB (dále jen „Politika organizační bezpečnosti“).

4.1.2 Bezpečnostní správce může zároveň vykonávat roli Administrátora.

4.2 Administrátor

4.2.1 Provoz aktiv v působnosti systému řízení bezpečnosti informací zajišťuje Administrátor.

- 4.2.2 Administrátor má, z pohledu kybernetické bezpečnosti, následující odpovědnosti:
- zajišťuje nasazení, provoz a údržbu aktiva podle pokynů Garanta aktiva v souladu s bezpečnostními a provozními předpisy;
 - provádí konfiguraci aktiva v souladu s bezpečnostními a provozními předpisy;
 - nastavuje aktivum a jeho funkce tak, aby umožnil jeho zálohování, provozní a bezpečnostní dohled, pořizování logů a provádění pravidelných kontrol;
 - sleduje důležitá bezpečnostní upozornění a doporučení výrobce anebo Garanta aktiva;
 - zaznamenává všechny důležité události a změny do Provozního deníku;
 - udržuje provozní dokumentaci aktuální a případné změny do provozní dokumentace zapracovává neprodleně;
 - poskytuje potřebnou součinnost Bezpečnostnímu správci, Garantu aktiva, Manažerovi kybernetické bezpečnosti, Architektovi kybernetické bezpečnosti a Auditorovi kybernetické bezpečnosti.
- 4.2.3 Přehled aktiv či skupin aktiv, jejichž správa může být kumulována v osobě jednoho Administrátora či skupiny Administrátorů:

tabulka 1 – Přehled oddělení pravomocí a odpovědností Administrátorů¹

	OS	DB	aplikace (IS)	sítě	Midd	FW	AD	Proxy	BS	pracovní stanice (local admin)	pracovní stanice (domain admin)
OS	-				ANO				ANO	ANO	ANO
DB		-	ANO						ANO	ANO	
aplikace (IS)		ANO	-		ANO					ANO	
sítě				-							
Midd	ANO		ANO		-				ANO	ANO	
FW						-		ANO			
AD							-				
Proxy						ANO		-			
BS	ANO	ANO	ANO		ANO				-		
pracovní stanice (local admin)	ANO	ANO	ANO		ANO					-	
pracovní stanice (domainadmin)	ANO										-

¹ Pokud je v dané kombinaci řádku a sloupce uvedeno „ANO“ je možné v osobě jednoho Administrátora či skupiny Administrátorů kumulovat pravomoci a odpovědnosti ve věci správy uvedených systémů.

4.3 **Manažer kybernetické bezpečnosti**

Pravomoci a odpovědnosti Manažera kybernetické bezpečnosti jsou definovány v Politice organizační bezpečnosti a směrnici SŽ SM094 Směrnice ve věci systému řízení kontinuity procesů ve státní organizaci Správa železnic (čj. 38892/2024-SŽ-GR-O30).

4.4 **Architekt kybernetické bezpečnosti**

Pravomoci a odpovědnosti Architekta kybernetické bezpečnosti jsou definovány v Politice organizační bezpečnosti a směrnici SŽ SM094 Směrnice ve věci systému řízení kontinuity procesů ve státní organizaci Správa železnic (čj. 38892/2024-SŽ-GR-O30).

4.5 **Garant primárního aktiva**

Pravomoci a odpovědnosti Garanta primárního aktiva jsou definovány v předpisu Politika klasifikace aktiv (čj. 56784/2018-SŽDC-GR-O30) a směrnici SŽ SM094 Směrnice ve věci systému řízení kontinuity procesů ve státní organizaci Správa železnic (čj. 38892/2024-SŽ-GR-O30).

4.6 **Garant podpůrného aktiva**

Pravomoci a odpovědnosti Garanta podpůrného aktiva jsou definovány v Politice klasifikace aktiv (čj. 56784/2018-SŽDC-GR-O30) a směrnici SŽ SM094 Směrnice ve věci systému řízení kontinuity procesů ve státní organizaci Správa železnic (čj. 38892/2024-SŽ-GR-O30).

4.7 **Výbor pro řízení kybernetické bezpečnosti**

Pravomoci a odpovědnosti člena Výboru pro řízení kybernetické bezpečnosti jsou definovány v Politice organizační bezpečnosti a směrnici SŽ SM094 Směrnice ve věci systému řízení kontinuity procesů ve státní organizaci Správa železnic (čj. 38892/2024-SŽ-GR-O30).

5 **POŽADAVKY NA DOKUMENTACI**

5.1 Pro každé aktivum (primární a podpůrné) v působnosti systému řízení bezpečnosti informací zpracuje Garant aktiva dokumentaci alespoň v následujícím rozsahu:

5.2 **Krycí list aktiva**

5.2.1 Za zpracování Krycího listu aktiva je odpovědný Garant primárního aktiva.

5.2.2 Krycí list popisuje klasifikaci primárního aktiva, způsob implementace jednotlivých bezpečnostních požadavků (nebo důvod jejich nezavedení) a obsahuje odkazy na dokumentaci opatření. Součástí Krycího listu aktiva je seznam schválených výjimek z opatření stanovených tímto předpisem. Garant aktiva tyto výjimky shromažďuje, vyhodnocuje a pravidelně je předává Manažerovi kybernetické bezpečnosti dle procesu řízení výjimek definovaného v Politice systému řízení bezpečnosti informací.

5.2.3 Manažer kybernetické bezpečnosti je odpovědný za přezkoumání všech výjimek v rámci Analýzy (přezkoumání) rizik a aktualizace Plánu zvládnutí rizik.

5.3 **Administrátorská příručka**

5.3.1 Administrátorská příručka je dokument obsahující popis pracovních postupů pro správu a administraci aktiva, včetně zapnutí a vypnutí aktiva, definici a postup provádění standardních změn a řešení běžných chybových stavů.

- 5.3.2 Administrátorská příručka minimálně obsahuje:
- a) popis předmětného aktiva, včetně architektury a rozhraní na aktiva jiná (případně uvedení odkazu);
 - b) způsoby spouštění a vypnutí aktiva, včetně seznamu služeb, které musí být pro provoz aktiva spuštěny;
 - c) popis činností vykonávaných během provozu aktiva, včetně uvedení uživatelských rolí, které tyto činnosti mohou provádět;
 - d) přehled požadavků na úroveň požadovaných služeb (dále jen „SLA“);
 - e) definování Uživatelů a uživatelských rolí, včetně přehledu jejich oprávnění;
 - f) popis autentizace a autorizace při přístupu k aktivu;
 - g) proces řešení incidentů včetně kybernetických bezpečnostních;
 - h) proces řešení změn;
 - i) proces řešení požadavků (přidělování oprávnění, změny oprávnění, rušení oprávnění apod.);
 - j) proces řešení požadavků na úpravu funkcionality;
 - k) způsob řešení známých provozních problémů.
- 5.4 **Uživatelská dokumentace**
- Uživatelská dokumentace je dokument popisující pracovní postupy pro práci s aktivem, včetně školicích materiálů a kontaktů na pracoviště ServiceDesk a způsoby předávání hlášení.
- 5.5 **Provozní deník**
- Do Provozního deníku se zaznamenávají veškeré informace o změnách, událostech v provozu a informace, které s provozem daného aktiva souvisí.
- 5.6 **Konfigurační a architektonická dokumentace**
- 5.6.1 Návrhová část dokumentace obsahuje informace o architekturních rozhodnutích primárního aktiva:
- a) seznam funkčních a nefunkčních požadavků včetně jejich vypořádání;
 - b) popis logické dekompozice informačního systému / aplikace na funkční komponenty, včetně popisu;
 - c) popis fyzické dekompozice informačního systému / aplikace na technologické komponenty, včetně popisu.
- 5.6.2 Dokumentace skutečného provedení informačního systému / aplikace obsahuje všechny důležité informace o funkcích, komponentách, včetně detailního popisu jejich vlastností:
- a) detailní popis technického provedení informačního systému / aplikace;
 - b) komunikační mapu informačního systému / aplikace s detailním popisem vazeb na další informační systémy;
 - c) detailní popis konfiguračních parametrů s uvedením defaultních a použitých hodnot;
 - d) zdrojové kódy (v případě zakázkového vývoje) včetně dokumentace, komentářů, popis nasazení/instalace/konfigurace;

- e) kontaktní údaje na technickou podporu;
- f) servisní smlouvu (pokud je provoz nebo servis zajišťován dodavatelsky).

5.7 **Plán zálohování / Plán kontinuity činností / Plán obnovy**

Obsahuje postupy pro vytváření a ukládání záloh a cíle a postupy pro obnovení chodu informačních systémů / aplikací v případě jejich výpadku.

6 ŘÍZENÍ PROVOZU

6.1 **Principy provozu ICT a řídicích systémů**

6.1.1 Provoz informační a komunikační technologie (dále jen „ICT“) Infrastruktury a řídicích systémů:

Provoz ICT Infrastruktury a řídicích systémů je prováděn podle doporučení relevantních oborových standardů jako jsou například ITIL a ISO. Opatření bezpečnosti informací musí být implementována v souladu s principy procesního řízení.

6.1.2 Opatření bezpečnosti informací jako součást procesů provozu ICT Infrastruktury a řídicích systémů:

Procesy řízení provozu ICT Infrastruktury a řídicích systémů jsou klíčovým vodítkem pro zajištění účelnosti a účinnosti, a proto musí být opatření bezpečnosti informací integrována do souvisejících procesů, aby byla zajištěna jejich účinnost a minimalizace provozních rizik.

6.1.3 Vedoucí zaměstnanci ICT Infrastruktury a řídicích systémů sehrávají roli Garantů aktiv:

Ředitel Správy železniční telematiky (dále jen „SŽT“), ředitel odboru zabezpečovací a telekomunikační techniky (dále jen „O14“), ředitel odboru elektrotechniky a energetiky (dále jen „O24“) a ředitel Centra techniky a diagnostiky (dále jen „CTD“) jsou odpovědní za zajištění provozu, rozvoje a bezpečnosti aktiv jimi spravovaných.

6.1.4 ServiceDesk:

Provozní záznamy jsou ukládány v nástroji ServiceDesk a tvoří klíčové informační zdroje, které Administrátoři udržují kvůli efektivní výměně informací a znalostí o provozu ICT Infrastruktury a řídicích systémů.

6.2 **Pravomoci a odpovědnosti spojené s bezpečným provozem**

6.2.1 Práva a povinnosti Bezpečnostních správců a dalších bezpečnostních rolí jsou definovány v Politice organizační bezpečnosti; práva a povinnosti Administrátorů jsou uvedeny v tomto předpise a v předpise SŽ R10 Řád Informatiky (čj. 15860/2022-SŽ-GR-O22).

6.2.2 Pravomoci a odpovědnosti musí být v rámci řízení provozu a bezpečnosti odděleny tak, aby se snížila možnost neautorizované modifikace nebo zneužití informací zpracovávaných informačními systémy / aplikacemi / zařízeními. Při obsazování rolí je nepřípustná jejich kumulace u jednoho Administrátora nebo skupiny Administrátorů. Musí být např. zabezpečeno, že zaměstnanci podílející se na kontrole a hodnocení kybernetických bezpečnostních incidentů se nepodílejí na provozu nebo návrhu ICT Infrastruktury a řídicích systémů.

6.2.3 Ve výjimečných případech (testovací provoz, havarijní stav, personální nouze apod.) se mohou tyto role po nezbytně nutnou dobu překrývat. Taková výjimka musí být zhodnocena Manažerem kybernetické bezpečnosti dle procesu řízení výjimek definovaného v Politice systému řízení bezpečnosti informací a aktivity daného Administrátora musí být dostatečně monitorovány a dokumentovány, tak aby je bylo možné přezkoumat.

6.2.4 Garant aktiva je odpovědný za určení, jak jsou vykonávány činnosti, které jsou spojeny se zajištěním provozuschopnosti a bezpečnosti ICT Infrastruktury, řídicích

systémů a systémů zajišťujících provozní podmínky. Garanti aktiva zároveň na pravidelné bázi dohlíží na provádění činností a to způsobem, který sami určí.

Pozn.: Tímto ovšem nepřecházejí odpovědnosti Garantů aktiv na jiné organizační jednotky (dále jen „OJ“), které aktivity, spojené se zajištěním provozuschopnosti a bezpečnosti, provádějí.

6.3 Postupy bezpečného provozu

6.3.1 Poučení zaměstnanců

Přístup k aktivům v působnosti systému řízení bezpečnosti informací a jejich používání je povoleno pouze těm zaměstnancům SŽ nebo cizích právních subjektů, kteří jsou prokazatelně poučeni o správných pracovních postupech a zacházení s těmito aktivy.

6.3.2 Údržba zařízení

Aktiva v působnosti systému řízení bezpečnosti informací musí být systematicky udržována na základě plánu údržby a investic vypracovávaného Garantem aktiva. Aktivity spojené s údržbou řídí a odpovídá za ně Garant aktiva.

Ve specifických případech, zvláště v prostředí řídicích systémů, je provozuschopnost a bezpečnost aktiv v působnosti systému řízení bezpečnosti informací systematicky udržována na základě Plánu údržby a investic. Tento Plán vypracovává OJ, která aktivity spojené se zajištěním provozuschopnosti a bezpečnosti provádí, a schvaluje jej Garant aktiva. Ten také řídí a odpovídá za aktivity spojené s údržbou.

6.3.3 Správa uživatelských zařízení

Zařízení (PC, notebook) musí být vždy, před předáním novému Uživateli, reinstalováno (v případě sdílených zařízení, např. technologických PC se neprovádí; případně se přihlídně k technickým možnostem).

Zařízení (tablet, chytrý telefon) musí být vždy, před předáním novému Uživateli, uvedeno do továrního nastavení.

6.3.4 Správa provozního programového vybavení

V rámci správy provozního programového vybavení musí být dodržovány následující zásady:

- a) změny a aktualizace programového vybavení mohou být prováděny pouze oprávněnými osobami a po provedení testů²;
- b) veškeré provozní programové vybavení musí být řádně a bezpečně archivováno a připraveno pro případné použití;
- c) přístup ke zdrojovým kódům musí být v rámci provozního prostředí omezen pouze na nezbytně nutné minimum a pouze pro oprávněné osoby.

6.3.5 Sledování provozu

V rámci systému řízení bezpečnosti informací jsou implementovány nástroje pro detekci, sběr a vyhodnocování kybernetických událostí. Je-li událost vygenerovaná v rámci informačních systémů / aplikací / zařízení v působnosti systému řízení bezpečnosti informací vyhodnocena jako kybernetický bezpečnostní incident, musí být aplikován postup stanovený ve SŽ SM074 Směrnice zvládání kybernetických bezpečnostních incidentů v informačním systému státní organizace Správa železnic, ve znění jejích revizí či dokumentů tuto politiku nahrazujících a dalších vnitřních předpisů SŽ.

6.3.6 Zajištění kontinuity provozu

² Ve specifických odůvodněných případech musí být proveden protokolární test oprávněnou zkušebnou či hodnotitelem bezpečnosti.

Garant primárního aktiva je odpovědný za zpracování Plánu kontinuity činností dle směrnice SŽ SM094 Směrnice ve věci systému řízení kontinuity procesů ve státní organizaci Správa železnic (čj. 38892/2024-SŽ-GŘ-O30), který popisuje postupy zajištění kontinuity služeb poskytovaných aktivem.

Garant podpůrného aktiva je odpovědný za zpracování Plánu obnovy dle směrnice SŽ SM094 Směrnice ve věci systému řízení kontinuity procesů ve státní organizaci Správa železnic (čj. 38892/2024-SŽ-GŘ-O30), který popisuje postupy zajištění kontinuity služeb poskytovaných aktivem a pravidelné provádění zálohování a testování Plánu obnovy včetně použitelnosti provedených záloh.

6.3.7 Provozní pravidla, postupy a dokumentace

6.3.7.1 Pro podpůrná aktiva musí být zpracovány postupy, dokumentace a konkrétní provozní pravidla, zajišťující jejich bezpečný provoz. Provozní pravidla a postupy musí respektovat zásady definované tímto předpisem. Za jejich zpracování, vydání a udržování je odpovědný Garant aktiva.

Součástí provozních pravidel a postupů musí být:

- a) postupy pro spuštění a ukončení chodu informačního systému / aplikace / zařízení, pro restart nebo obnovení informačního systému / aplikace po selhání a pro ošetření chybových stavů nebo mimořádných jevů;
- b) postupy pro sledování kybernetických událostí a pro ochranu záznamů o kybernetických událostech;
- c) postupy řízení a schvalování změn;
- d) postupy pro sledování, plánování a řízení kapacity lidských, technických a informačních zdrojů.

6.3.7.2 Provoz je řízen žádostmi zadávanými do nástroje ServiceDesk. Administrátoři musí zaznamenávat všechny podstatné činnosti související s provozem do nástroje ServiceDesk. Při tom Administrátoři postupují v souladu s postupy stanovenými v provozní a bezpečnostní dokumentaci.

6.3.7.3 Provozní deník musí obsahovat veškeré informace o změnách, událostech v provozu a informace, které s provozem souvisí.

6.3.7.4 Provozní deník nebo jeho část může být, je-li to vhodné, vedena pro více informačních systémů / aplikací / zařízení. Provozní deník může být veden v listinné i elektronické podobě.

6.3.7.5 Záznam v Provozním deníku musí obsahovat alespoň následující údaje:

- a) datum a čas záznamu,
- b) název události nebo aktivity,
- c) informační systém / aplikace / zařízení, kterého se úkon týkal,
- d) popis události nebo aktivity,
- e) autor záznamu – jednoznačná identifikace autora (např. jméno a příjmení, osobní číslo).

6.4 Řízení kapacit

6.4.1 Řízení kapacit musí předcházet poruchám či výpadkům způsobených nedostatkem lidských, technických a informačních zdrojů.

6.4.2 Garanti aktiv jsou odpovědní za řízení kapacit jimi spravovaných aktiv.

- 6.5 Technické přezkoumání informačních systémů / aplikací po změnách provozní platformy**
- 6.5.1 V případě změny provozní platformy musí být přezkoumány a otestovány dotčené informační systémy / aplikace, aby bylo zajištěno, že provedené změny nemají nepříznivý dopad na provoz nebo bezpečnost.
- 6.5.2 Technické přezkoumání informačních systémů / aplikací po změnách provozní platformy zahrnuje:
- a) přezkoumání správnosti funkčních vlastností, bezpečnostních parametrů a Integrity informačních systémů / aplikací, a zda nebyly nevhodně ovlivněny změnami provozní platformy;
 - b) zajištění, že oznámení o změnách provozní platformy jsou poskytovány včas, aby byl před nasazením zajištěn dostatek času na provedení vhodných testů a přezkoumání;
 - c) zajištění, že do Plánů kontinuity činností / Plánů obnovy byly zapracované příslušné změny.
- 6.5.3 Provozní platformy zahrnují operační systémy, databáze (dále jen „DB“) a případně jiné integrační platformy, např. software pro funkce nad rámec služeb operačního systému – Middleware (dále jen „Midd“).
- 6.5.4 Administrátor úzce spolupracuje s projektovými a vývojovými týmy při řešení všech skutečností zjištěných během technického přezkoumání.
- 6.5.5 Všechny skutečnosti zjištěné během technického přezkoumání musí být zaznamenány, a to včetně postupů vedoucích k jejich vyřešení.
- 6.6 Audit**
- 6.6.1 Během auditů a testů, které probíhají v provozním prostředí, musí být dodržována následující pravidla:
- a) rozsah auditů nebo testů musí být předem odsouhlasen Manažerem kybernetické bezpečnosti a příslušným Garantem aktiva (případně ředitelem SŽT, ředitelem O14, ředitelem O24 či ředitelem CTD) a musí být dohlížen osobou, která byla určena jako průvodce auditorů nebo testerů;
 - b) pokud není rozsah požadovaných přístupových oprávnění přímo určen v rozsahu auditu nebo testu, musí být požadavky na přístupová oprávnění používána během auditu nebo testu schválena Manažerem kybernetické bezpečnosti a příslušným Garantem aktiva (případně ředitelem SŽT, ředitelem O14, ředitelem O24 či ředitelem CTD);
 - c) činnosti během auditů a testů musí být omezeny na právo čtení (bez oprávnění změny dat); jsou-li požadována oprávnění vyšší, musí být audit nebo test prováděn v testovacím prostředí;
 - d) použití speciálních nástrojů pro audit a testování, např. nástroje k prolomování hesel apod., musí být vysloveně uvedeno ve schváleném rozsahu auditů nebo testů;
 - e) audity a testy, které by mohly ovlivnit dostupnost služeb, musí být schváleny příslušnými Garanty aktiv a, je-li to možné, musí být prováděny mimo běžnou pracovní dobu; uživatelé musí být předem informováni;
 - f) užití přístupových oprávnění během auditů a testů musí být monitorováno a logováno obvyklými způsoby (viz kapitola 12 tohoto předpisu).
- 6.6.2 Všechny účty, použité v průběhu auditů nebo testů, musí být neprodleně, po dokončení auditu nebo testu, deaktivovány a zrušeny. Pokud byly během auditů nebo testů využity uživatelské účty nebo mohly být během auditů a testů kompromitovány,

musí neprodleně dojít ke změně hesel (platí rovněž pro technologické účty a účty s privilegovanými oprávněními).

6.7 **Další pravidla provozu**

6.7.1 Služby operačních systémů a SW vybavení, které nejsou využívány, musí být deaktivovány (přehled služeb musí být uveden v Administrátorské příručce).

6.7.2 V prostředí řídicích systémů se přihlédne k Všeobecným technickým podmínkám a Zvláštním technickým podmínkám, případně dalším dokumentům, které určují provozní parametry, způsoby použití a správy předmětných podpůrných aktiv a metody přístupu k předmětným podpůrným aktivům.

6.7.3 Výjimky z požadavků stanovených tímto předpisem musí být uvedeny v Krycím listu aktiva (viz kapitola 5 tohoto předpisu).

7 **BEZPEČNOST KOMUNIKACÍ**

7.1 **Principy bezpečnosti komunikační sítě**

7.1.1 Bezpečnost komunikační sítě (interní datové sítě) je založena na sedmi principech definovaných v této kapitole.

7.1.2 Hlubková obrana

7.1.2.1 Bezpečnost je řešena komplexně na všech vrstvách datové komunikace. Přístup z vnější sítě do interní datové sítě je povolen pouze při splnění následujících podmínek:

- a) přístup je podmíněn autentizací Uživatele a zařízení;
- b) přístup do perimetru sítě SŽ je dle přístupových oprávnění Uživatele a zařízení;
- c) musí být generovány a ukládány záznamy (logů) o činnostech přistupujícího Uživatele a zařízení.

7.1.2.2 Vzdálený přístup musí být šifrovaný (viz Politika použití kryptografických prostředků, čj. 56789/2018-SŽDC-GR-O30).

7.1.3 Segmentace

V interní datové síti musí být oddělen provoz informačních systémů / aplikací, Uživatelů a externích subjektů.

7.1.4 Řízené propojení

Jednotlivé segmenty jsou propojovány prostřednictvím řízených propojení, jejichž bezpečnostní opatření vycházejí z bezpečnostních požadavků.

7.1.5 Pružnost

Interní datová síť je navrhována redundantně pro eliminaci jednotlivých bodů způsobujících selhání systému a pro maximalizaci dostupnosti síťové Infrastruktury.

7.1.6 Sledování provozu

Administrátoři sledují a vyhodnocují logy, včetně samotného provozu v interní datové síti.

7.1.7 Jednoznačné identity

Každému Administrátorovi je přiřazen samostatný účet (neexistují sdílené účty), prostřednictvím něhož provádí správu jednotlivých síťových prvků. Totéž platí i v případě Uživatelů.

- 7.1.8 Out-of-band správa
Síťové prvky je možné spravovat pouze prostřednictvím logicky oddělené sítě.
- 7.2 **Bezpečnost komunikační sítě**
- 7.2.1 V interní datové síti musí být zavedena pravidla pro dohled a kontrolu událostí souvisejících s bezpečností sítě.
- 7.2.2 Musí být zavedeny postupy pro:
- a) správu hesel a šifrovacích klíčů,
 - b) přidělování IP adres,
 - c) nastavování aktivních prvků,
 - d) správu ICT Infrastruktury,
 - e) zajištění Integrity interní datové sítě.
- 7.2.3 Garant aktiva je odpovědný za zajištění bezpečnosti interní datové sítě a ochranu souvisejících služeb před neoprávněným přístupem.
- 7.2.4 V rámci jednotlivých lokalit jsou řediteli CTD odborně podřízeni Administrátoři zajišťující provoz a bezpečnost interní datové sítě.
- 7.2.5 K zajištění bezpečnosti interní datové sítě a ochrany souvisejících služeb před neoprávněným přístupem je zejména uplatňováno:
- a) stanovení odpovědností a postupů pro správu síťových prvků;
 - b) odpovědnost za provoz interní datové sítě je oddělena od odpovědnosti za provoz informačních systémů / aplikací / zařízení nebo jejich částí;
 - c) segmentace interní datové sítě;
 - d) využití bezdrátových sítí je podmíněno šifrováním (viz Politika použití kryptografických prostředků, čj. 56789/2018-SŽDC-GR-O30);
 - e) zaznamenávání událostí formou logu a kontinuální monitorování umožňující detekci činností, které mohou ovlivnit bezpečnost nebo jsou pro bezpečnost relevantní;
 - f) nastavení formálních komunikačních kanálů;
 - g) autentizace veškerých informačních systémů / aplikací / zařízení v interní datové síti s důrazem na ujednocené řízení autentizace a autorizace;
 - h) synchronizace systémového času veškerých síťových prvků;
 - i) automatizované zálohování konfigurací síťových prvků.
- 7.2.6 Změna architektury interní datové sítě je prováděna pouze prostřednictvím procesu řízení změn (viz kapitola 13 tohoto předpisu).
- 7.3 **Bezpečnost síťových služeb**
- 7.3.1 V rámci návrhu, implementace a provozu musí být identifikována a aplikována bezpečnostní opatření nezbytná pro konkrétní služby, tj. bezpečnostní prvky, úrovně služeb a požadavky na správu a řízení (viz kapitola 6 tohoto předpisu). Ředitel CTD zajistí implementaci těchto opatření s poskytovatelem síťových služeb.
- 7.3.2 Mezi bezpečnostní prvky síťových služeb patří:
- a) technické prostředky zajišťující bezpečnost síťových služeb, tj. autentizace, autorizace, šifrování a kontrola síťových spojení;

- b) nastavení a parametry pro bezpečné připojení k síťovým službám;
- c) postupy pro omezení přístupu k síťovým službám nebo informačním systémům / aplikacím tam, kde je to nezbytné.

7.4 **Užívání síťových služeb**

7.4.1 Uživatelé mají povolen přístup pouze k těm službám informačních systémů / aplikací, k jejichž užití mají přístupová oprávnění.

7.4.2 Komunikační infrastruktura v působnosti systému řízení bezpečnosti informací musí být oddělena od vnější sítě. Výjimky podléhají schválení Manažera kybernetické bezpečnosti dle procesu řízení výjimek definovaného v Politice systému řízení bezpečnosti informací a musí být řádně dokumentovány a kontrolovány. Výjimky musí poskytovat dostatečné záruky a být řešeny tak, aby jejich prostřednictvím nedošlo k narušení informačních systémů / aplikací.

7.5 **Pravidla a postupy pro řízení přístupů v rámci komunikační sítě**

7.5.1 Musí být formulována pravidla týkající se využívání interní datové sítě. Tyto zahrnují:

- a) komunikační sítě a síťové služby, ke kterým je povolen přístup;
- b) autentizační a autorizační postupy pro stanovení, kdo má povolen přístup a ke kterým sítím a síťovým službám;
- c) opatření a postupy pro ochranu přístupu k interní datové síti a síťovým službám;
- d) prostředky používané pro přístup k interním datovým sítím a síťovým službám (například použití virtuální privátní sítě [dále jen „VPN“] nebo bezdrátové sítě);
- e) požadavky na autentizaci a autorizaci Uživatele pro přístup k různým síťovým službám;
- f) monitorování používání síťových služeb.

7.5.2 Správa síťových prvků je prováděna pouze prostřednictvím centrálně spravovaných identit s využitím protokolů TACACS+. V případě nemožnosti použití TACACS+ je povoleno použít protokol pro přístup k síti/IP mobilitu (RADIUS). Administrátoři jsou pro přístup k zařízení autentizováni a autorizováni pomocí svého jedinečného účtu. Ke vzdálené správě síťových prvků musí být využíván protokol SSHv2 nebo vyšší.

7.5.3 Používání bezdrátové sítě s přímým přístupem do interní datové sítě je podmíněné šifrováním a autentizací na straně klienta (např. 802.1x s EAP-TLS).

7.5.4 V případě bezdrátové sítě s šifrovanou komunikací bez dodatečné autentizace musí být přístup do interní datové sítě realizován prostřednictvím brány v demilitarizované zóně.

7.5.5 Instalace bezdrátových sítí je prováděna tak, aby jejich dostupnost byla mimo kontrolovaný perimetr objektů SŽ minimalizována.

7.6 **Komunikace s vnější sítí**

7.6.1 Veškerá externí připojení k aktivům v působnosti systému řízení bezpečnosti informací musí být vedena přes demilitarizovanou zónu a vhodným způsobem zabezpečena, např. technologií typu VPN, případně pomocí bezpečných protokolů zaručujících autentizaci, šifrování a Integritu spojení. Perimetr sítě musí být vybaven stavovým firewallem.

7.6.2 Řízení přístupu z vnější sítě do interní datové sítě je povoleno pouze za následujících podmínek:

- a) přístup je podmíněn autentizací Uživatele a zařízení;
- b) přístup do perimetru sítě SŽ je dle přístupových oprávnění uživatele a zařízení;

- c) musí být generovány a ukládány záznamy (logů) o činnostech přistupujícího Uživatelé a zařízení.
- 7.6.3 Vzdálený přístup musí být šifrovaný (viz Politika použití kryptografických prostředků, čj. 56789/2018-SŽDC-GR-O30).
- 7.6.4 Uživatelská zařízení (PC, notebook) nesmí do vnější sítě přistupovat napřímo, ale veškerá komunikace musí procházet přes technické prostředky zajišťující ochranu proti škodlivému kódu.
- 7.6.5 Na perimetru sítě by měly být implementovány sondy pro sledování odchylek v provozu.
- 7.7 **Segmentace sítí**
- 7.7.1 Aktiva v působnosti systému řízení bezpečnosti informací musí být umísťována do oddělených síťových segmentů v závislosti na jejich funkci a klasifikaci z hlediska Důvěrnosti, Dostupnosti a Integrity. Vývojové, testovací a produkční prostředí všech informačních systémů / aplikací / zařízení se musí nacházet v oddělených sítích. Provozní a administrativní komunikace by měly být odděleny, a pokud je to možné, probíhat v oddělených sítích.
- 7.7.2 Mezi síťovými segmenty musí být striktně definovány pouze nezbytně nutné síťové prostupy a umístěny kontrolní prvky. Nežádoucí prostupy mezi síťovými segmenty musí být omezeny vhodnými technickými prostředky (firewally, Proxy apod.). Přístupy k Technologickým sítím musí být vybaveny firewallem. Pro řízení komunikace mezi síťovými segmenty musí být zaveden nástroj, který zajistí ochranu Integrity interní datové sítě.
- 7.7.3 Za návrh rozdělení interní datové sítě do segmentů odpovídá Architekt kybernetické bezpečnosti.
- 7.8 **Určení práv a povinností za bezpečný provoz komunikační sítě**
- Za bezpečný provoz komunikační sítě nebo jeho zajištění je odpovědný ředitel CTD.
- 7.9 **Komunikace mezi segmenty interní datové sítě**
- 7.9.1 Při komunikaci mezi prvky ležícími v různých segmentech interní datové sítě je nezbytné provést bezpečnou autentizaci komunikujících informačních systémů / aplikací / zařízení. Komunikace uvnitř interní datové sítě by měla být šifrována.
- 7.9.2 Veškerá komunikace mezi segmenty interní datové sítě musí být logovaná, a to nejméně v rozsahu navázaných a odmítnutých spojení.
- 7.10 **Ochrana portů pro vzdálenou diagnostiku a správu**
- 7.10.1 Fyzický přístup k síťovým prvkům musí být zabezpečen tak, aby se zařízeními mohli manipulovat jenom k tomu určení Administrátoři.
- 7.10.2 Logický přístup k portům síťových prvků je povolen pouze prostřednictvím izolované sítě z vyhrazených zařízení. Izolace sítě musí být provedena minimálně prostřednictvím mechanismů úrovně virtuální lokální sítě (VLAN) či virtuální směrování a přeposílání (VRF VPN), přičemž by komunikace měla být šifrována.
- 7.10.3 Garanti podpůrného aktiva určují způsoby bezpečného nastavení a předávají je k realizaci. Následně jsou odpovědní za provádění kontroly.
- 7.11 **Řízení směrování sítě**
- Sítě, ve kterých jsou umístěny informační systémy / aplikace / zařízení, musí být vybaveny řízeným směrováním. Musí být zajištěno, režijní komunikace aktivních síťových prvků nebude narušována nebo nepřiměřeně omezována vzájemnou komunikací mezi uživateli informačních systémů, aplikacemi a koncovými zařízeními. Tato režijní komunikace musí mít v případě potřeby nastavenou dostatečnou prioritu jejího přenosu, aby nedocházelo k chybám nebo výpadkům této komunikace.

7.12 Bezpečnost aplikací

U informačních systémů / aplikací, které jsou v působnosti systému řízení bezpečnosti informací, musí být zajištěna následující trvalá ochrana:

- a) ochrana informačních systémů / aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou;
- b) ochrana transakcí před jejich nedokončením, nesprávným směřováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.

7.13 Pravidla a postupy pro monitorování sítě a vyhodnocování provozních záznamů

- 7.13.1 Veškeré síťové prvky musí být napojeny na provozní dohled, kde je prováděn průběžný sběr záznamů, včetně jejich vyhodnocování.
- 7.13.2 Pro monitorování musí být používány protokoly se šifrováním komunikace (např. SNMPv3).
- 7.13.3 Záznamy o chybách musí být uchovávány pro účely dalšího ověřování, odstraňování příčin, následků poruch a nežádoucích událostí.
- 7.13.4 Veškeré prostupy z interní datové sítě do vnější sítě musí být nepřetržitě monitorovány.
- 7.13.5 Monitorování provozu sítě a bezpečnostní monitorování je prováděno v souladu se směrnicí SŽ SM074 Směrnice zvládání kybernetických bezpečnostních incidentů v informačním systému státní organizace Správa železnic.

7.14 Specifika prostředí řídicích systémů

- 7.14.1 V prostředí řídicích systémů se přihlídně k Všeobecným technickým podmínkám a Zvláštním technickým podmínkám, případně dalším dokumentům, které určují provozní parametry, způsoby použití a správy předmětných podpůrných aktiv a metody přístupu k předmětným podpůrným aktivům.
- 7.14.2 Výjimky z požadavků stanovených tímto předpisem musí být uvedeny v Krycím listu aktiva (viz kapitola 5 tohoto předpisu).

8 ŘÍZENÍ PŘÍSTUPU

8.1 Požadavky na řízení přístupů

- 8.1.1 Řízení přístupu v rámci všech informačních systémů / aplikací / zařízení spadajících do působnosti systému řízení bezpečnosti informací vychází ze zásady, že přístup je zakázán, kromě těch částí informačního systému / aplikací a určeného zařízení, kam byl přístup Uživateli výslovně povolen (pro které získal oprávnění). Tato zásada musí být naplňována zejména následujícími pravidly:
 - a) Uživatelům jsou přidělovány přístupy pouze k těm informačním systémům / aplikacím / zařízením a pouze v tom rozsahu, který nezbytně potřebují pro výkon svojí pracovní činnosti a zároveň po nezbytně nutnou dobu.
 - b) Garanti primárních aktiv jsou odpovědní za schvalování přístupových oprávnění k jim svěřeným aktivům. Garanti primárních aktiv mohou schvalováním přístupových oprávnění pověřit jinou osobu nebo definovat pravidla, na základě, kterých jsou Uživatelům přidělována přístupová oprávnění.
 - c) Garanti podpůrných aktiv jsou odpovědní za přidělování přístupových oprávnění v rámci jimi spravovaných aktiv.

- d) V maximální možné míře používat standardní uživatelské profily (skupiny nebo role) pro obecné role při zpracování úloh (běžný Uživatel, Uživatel s oprávněním zápisu atd.).
 - e) Procesní role, které jsou zapojeny do zadání, schvalování a přidělování přístupových oprávnění (Uživatel, Žadatel, Schvalovatel, Administrátor) musí být oddělené.
 - f) Správa uživatelských přístupů a oprávnění se provádí tak, aby byl udržován auditovatelný přehled o všech Uživatelích s oprávněním používat informační systémy / aplikace / zařízení, přehled jim přidělených přístupů a přístupových oprávnění a záznamy o změnách těchto údajů.
 - g) Odebírání a změny přístupových oprávnění musí probíhat v co nejkratším čase.
 - h) Musí být prováděno pravidelné přezkoumání všech přístupových oprávnění dle jednotlivých oblastí vedených ve vzoru Zprávy z přezkoumání přístupových oprávnění (viz Příloha B tohoto předpisu).
 - i) Neaktivní spojení Uživatele s informačním systémem / aplikací / zařízením musí být po stanovené době nečinnosti automaticky ukončeno a pro další pokračování v práci musí proběhnout ověření jeho identity.
- 8.1.2 Existuje formalizovaný proces správy uživatelských a privilegovaných účtů, prostřednictvím něhož je prováděno zavádění/změny/deaktivace/přidělování/odebírání oprávnění.
- 8.1.3 Pro řízení uživatelských přístupů k informačním systémům / aplikacím se preferuje použití centrálního nástroje pro správu přístupových oprávnění (Active Directory, LDAP, IdM) formou jednotné identity (dále je „SSO“) nebo autentizace proti tomuto nástroji. Administrátor odpovídá za správnou konfiguraci informačního systému/ aplikace tak, aby s tímto nástrojem správně spolupracovaly a dodržel tak všechny zásady pro řízení přístupových oprávnění.
- 8.1.4 Pouze pokud není možné použít centrální nástroj pro řízení přístupů, mohou být přístupová oprávnění k informačnímu systému / aplikaci řízena lokálně (Administrátorem). V takovém případě Administrátor odpovídá za dodržení zásad pro řízení přístupových oprávnění.
- 8.2 Životní cyklus řízení přístupu**
- 8.2.1 Přidělování přístupových oprávnění
- Založení účtu a přidělení přístupových práv (rolí) pro nového Uživatele se řídí procesem pro nástup, za který je odpovědný ředitel odboru personálního (O10) a další vedoucí zaměstnanci, kteří mají oprávnění v oblasti pracovněprávních vztahů.
- 8.2.2 Při zřizování nových uživatelských účtů nebo přidělování přístupových oprávnění (rolí) musí být dodrženy následující zásady:
- a) Přístup může být zřízen pouze na základě evidované a řádně schválené formální žádosti v nástroji ServiceDesk. Takový požadavek musí obsahovat přesnou specifikaci, o co je konkrétně žádáno. Není přípustné, aby byl požadavek koncipován tak, že má být založen jako analogický s jiným Uživatelem.
 - b) Všem Uživatelům musí být v informačním systému / aplikaci přiděleny unikátní identifikátory. Nesmí být používány sdílené účty.
 - c) Všem Uživatelům musí být přidělena adekvátní autentizační metoda (například heslo s definovanou komplexitou, čipová karta s certifikátem apod.). Za definici adekvátních autentizačních metod odpovídá Manažer kybernetické bezpečnosti.
 - d) Výměna identifikátoru a autentizačních informací (zejména hesla) v případě jejich ztráty musí být zajištěna bezpečným způsobem.

- e) Každý požadavek na přístup je zadáván samostatně, a to z toho důvodu, aby bylo jasné rozeznatelné, jestli a jak došlo ke schválení či zamítnutí. Z tohoto důvodu musí být žádosti s vícenásobnými požadavky zamítány.
- f) Všechna přístupová oprávnění k informačnímu systému / aplikaci jsou udržována v seznamu, který poskytuje přehled o všech Uživatelích s oprávněním je používat, přehled jim přidělených přístupů a přístupových oprávnění a záznamy o všech změnách těchto údajů.

8.2.3 Schvalování přístupových oprávnění

8.2.3.1 Přidělení či změna přístupových oprávnění (rolí) jsou podmíněny schválením přímého nadřízeného v nástroji ServiceDesk, a v případech, kdy to vyžaduje Provozní předpis informačního či komunikačního systému kritické informační infrastruktury, i Garanta aktiva.

8.2.3.2 Zrušení přístupových oprávnění (rolí) je podmíněno schválením přímého nadřízeného v nástroji ServiceDesk.

8.2.3.3 Přístupové oprávnění (rolí) Administrátor přidělí až poté, co je žádost schválena.

8.2.4 Odebírání přístupových oprávnění

Při odebírání nebo rušení přístupových oprávnění a účtů (rolí) musí být dodrženy následující zásady:

- a) přístupy mohou být rušeny pouze na základě žádosti evidované v nástroji ServiceDesk, v rámci pravidelného přezkoumání přístupových oprávnění, nebo případně na základě příkazu oprávněných zaměstnanců odboru bezpečnosti a krizového řízení (dále jen „O30“) a SŽT či Garantů aktiv, který je řádně zdokumentován a následně zanesen do nástroje ServiceDesk;
- b) v informačních systémech / aplikacích je nutné zajistit rušení nevyužívaných přístupových oprávnění Uživatelů po stanovené době;
- c) odebírání a rušení přístupových práv musí být provedeno v co nejkratším čase.

8.2.5 Změna přístupových oprávnění

Při změně přístupových oprávnění musí být dodrženy následující zásady:

- a) Přístupy mohou být změněny pouze na základě žádosti evidované a schválené v nástroji ServiceDesk, v rámci pravidelného přezkoumání přístupových oprávnění, nebo případně na základě příkazu oprávněných zaměstnanců O30, SŽT či Garantů aktiv, který je řádně zdokumentován a následně zanesen do nástroje ServiceDesk.
- b) V případě změny pracovního zařazení a přechodu na jinou pozici se změna přístupových oprávnění zaměstnance provádí tím způsobem, že jsou nejprve odebrána veškerá přístupová oprávnění nebo role (kromě role zaměstnance) a následně jsou nastavena přístupová oprávnění (role), která jsou nezbytná pro výkon jeho nové pozice. Z tohoto důvodu musí být žádost evidovaná v nástroji ServiceDesk rozdělena na žádost na zrušení stávajících přístupových oprávnění a následně na žádost přidání nových.
- c) Není přípustné, aby žádost byla koncipována tak, že mají být přístupová oprávnění nebo role přiřazeny analogicky s jiným zaměstnancem.

8.2.6 Ukončení pracovního poměru

Při ukončení pracovního poměru Uživatele (platí i pro zaměstnance cizích právních subjektů) je Administrátor povinen zrušit jeho uživatelský účet a všechna další přístupová oprávnění (role). Přičemuž platí:

- a) Přístupy mohou být rušeny pouze na základě žádosti evidované v nástroji ServiceDesk nebo případně na základě příkazu oprávněných zaměstnanců O30

a SŽT či Garantů aktiv, který je řádně zdokumentován a následně zanesen do nástroje ServiceDesk.

- b) V případě ukončení pracovněprávního vztahu s Administrátorem / Bezpečnostním správcem, je jejich přímý nadřízený odpovědný za předání všech jejich znalostí, odpovědností a dokumentace týkajících se provozu aktiv v působnosti systému řízení bezpečnosti informací.

8.2.7 Náhlé ukončení pracovního poměru

- 8.2.7.1 V případě náhlého ukončení pracovního poměru musí přímý nadřízený, prostřednictvím Administrátora, zajistit deaktivaci uživatelského účtu zaměstnance (platí i pro zaměstnance cizích právních subjektů) a veškerých dalších přístupových oprávnění (rolí). Dále přímý nadřízený, spolu s ředitelem O30, zajistí odebrání aktiv, která zaměstnanec využíval. O odebrání aktiv musí být pořízen písemný protokol, ve kterém je uveden soupis odebraných aktiv a současně musí být vyjmenována aktiva, která se odebrat nepodařilo.

- 8.2.7.2 Protokol o odebrání aktiv musí být uložen v osobním spisu zaměstnance a záznam o odebrání aktiv musí být součástí výstupního listu. Přímý nadřízený zaměstnance pak zajistí vrácení odebraných aktiv SŽ.

8.3 Řízení privilegovaných oprávnění

8.3.1 Účet s privilegovanými oprávněními

- 8.3.1.1 Je určen pro omezený počet oprávněných Uživatelů/Administrátorů a jejich počet musí být minimalizován, a to včetně lokálních administrátorských účtů.

- 8.3.1.2 V případě vybraných podpůrných aktiv je zaveden tzv. princip „čtyř očí“, kdy jsou veškeré aktivity prováděny nezávisle dvěma Administrátory. Přehled podpůrných aktiv, kde je aplikován tento princip stanovuje Garant aktiva na návrh Bezpečnostního správce.

- 8.3.1.3 Pod účtem privilegovaným oprávněním nesmí být prováděna běžná uživatelská práce.

- 8.3.1.4 Kromě zásad platných pro standartní Uživatele se musí při přidělování účtů s privilegovaným oprávněním postupovat i podle následujících zásad:

- a) Účty s privilegovaným oprávněním mohou být přidělovány pouze na základě opodstatněné potřeby a žádost přímého nadřízeného. Za schválení je odpovědný Garant aktiva.
- b) Pro udělení privilegovaného přístupu do informačního systému aplikace musí být Uživateli zřízen zvláštní účet. Nesmí dojít ke kumulaci běžných a privilegovaných přístupových oprávnění u jednoho účtu.
- c) Účty s privilegovaným oprávněním mohou být přiděleny pouze těm zaměstnancům, kteří jsou zodpovědní za výkon dané činnosti.
- d) Informační systémy / aplikace musí v maximální možné míře využívat systémové procedury tak, aby se snížila potřeba zakládat účty s privilegovaným oprávněním.
- e) Účty s privilegovaným oprávněním musí být zřetelně označené (např. v názvu) a snadno rozeznatelné od běžných účtů.
- f) Používání účtů s privilegovaným oprávněním je přísně monitorováno a kontrolováno a mohou být využívány pouze pro aktivity, které je přímo vyžadují a na nezbytně nutnou dobu.

8.4 **Politika hesel**

8.4.1 Správa hesel

Základní a prioritní povinností Uživatelů i Administrátorů je dodržování a plnění všech stanovených bezpečnostních zásad a pravidel. Uživatelé i Administrátoři jsou odpovědní za bezpečnou práci s hesly k jednotlivým informačním systémům / aplikacím / zařízením.

8.4.1.1 Uživatel i Administrátor nesmí:

- a) Sdílet své osobní autentizační informace s jinou osobou.
- b) Veřejně zmiňovat jakékoli osobní autentizační informace či postup k jejich vytváření.
- c) Zadávat osobní autentizační informace, když je někým pozorován.
- d) Přihlašovat se pomocí osobních autentizačních informací jiného Uživatele.
- e) Provádět neautorizované změny hesla (platí pro Administrátory).
- f) Používat pro informační systémy / aplikace / zařízení, které požadují separátní přihlášení, stejné heslo.
- g) Zaznamenávat přihlašovací údaje např. na papíry, do souborů nebo do zařízení. Manažer kybernetické bezpečnosti může schválit a povolit ukládání hesel do specializovaných aplikací určených využívajících šifrovaná úložiště.

8.4.1.2 Proces přidělování hesel musí splňovat následující zásady:

- a) Uživateli musí být při zřízení účtu k informačnímu systému / aplikaci / zařízení přiděleno dočasné bezpečné heslo (platné max. 60 minut), jehož změna musí být automaticky vynucena ihned po prvním přihlášení.
- b) Uživatel musí být autentizován ještě před tím, než je mu přiděleno nové nebo dočasné heslo.
- c) Veškeré defaultní účty (root, admin, user) musí být z informačních systémů/ aplikací odstraněny. Pokud účty nejdou odstranit, musí být deaktivovány nebo u nich změněna hesla, která pak musí být bezpečně uložena.
- d) V případě, že Uživatel zapomene heslo, musí mu nastavit Administrátor nové dočasné bezpečné heslo (platné max. 60 minut) podle stejných pravidel, jako při vytváření účtu. Jeho změna musí být automaticky vynucena ihned po prvním přihlášení.

8.4.2 Požadavky na sílu hesel

Všechny informační systémy / aplikace / zařízení musí při vytváření Uživatelských hesel vynucovat následující pravidla:

- a) povolená délka hesla je max. 64 znaků;
- b) minimální délka hesla je 12 znaků (v případě účtů s privilegovaným oprávněním a technologických účtů 19 znaků);
- c) heslo obsahuje alespoň tři z následujících skupin znaků (s tím, že neomezuje množinu použitelných znaků):
 - nejméně jedno velké písmeno,
 - nejméně jedno malé písmeno,
 - nejméně jednu číslici,

- nejméně jeden speciální nealfanumerický znak (tj. ~! @ # \$ % ^ & * _ - + = ` \ () { } [] ; : ' " < > , . ? /),
- d) heslo nesmí obsahovat jméno, příjmení, datum narození Uživatele nebo jeho blízké osoby, a nemělo by obsahovat žádný jiný snadno uhodnutelný řetězec ani mnohonásobně se opakující znaky, včetně posloupností používaných na klávesnici, není založeno na čemkoli, co může někdo jednoduše uhodnout nebo získat na základě informací, které se k osobě vztahují (např. přihlašovací jméno, jména, telefonní čísla, data narození, apod.), neobsahuje názvy předmětných informačních systémů / aplikací / zařízení či služeb;
- e) Uživatel je povinen měnit svá hesla minimálně každých 365 dní (toto pravidlo se nevztahuje na účty sloužící k obnově systémů v případě havárie);
- f) stejné heslo se nesmí opakovat v historii dvanácti posledních hesel;
- g) neaktivní spojení Uživatele s informačním systémem / aplikací / zařízením musí být po stanovené době nečinnosti automaticky ukončeno a pro další pokračování Uživatele v práci musí proběhnout ověření jeho identity.
- 8.4.3 Maximální počet neúspěšných zadání je 10. Následně dojde k progresivnímu prodloužení odpovědi předmětného systému (po každých deseti neúspěšných pokusech je prodloužena odpověď o 1,5násobek oproti předchozímu cyklu).
- 8.4.4 Při podezření na kompromitaci hesla je Uživatel povinen neprodleně provést jeho změnu a následně tuto skutečnost ohlásit na pracoviště ServiceDesk (prostřednictvím telefonu, e-mailu, webové aplikace, osobně nebo přímého nadřízeného).
- 8.4.5 Autentizační mechanismy aktiv v působnosti systému řízení bezpečnosti informací musí být implementovány takovým způsobem, aby byly splněny následující požadavky:
- a) pro autentizaci je vyžadováno použití alespoň dvoufaktorové autentizace, s dvěma nezávislými faktory;
 - b) přístup k informačním systémům / aplikacím je umožněn až po autentizaci;
 - c) autentizační mechanismy musí zajistit odolnost uložených nebo přenášených přístupových údajů proti neoprávněnému odcizení či zneužití;
 - d) přístupové údaje jsou uloženy ve formě odolné proti offline útoku (hesla jsou uložena v zašifrované podobě).
- 8.5 **Pravidelné přezkoumání přístupových oprávnění a přístupových skupin**
- 8.5.1 Garanti aktiv jsou odpovědní za provádění pravidelných kontrol poskytnutých přístupových oprávnění Uživatelům i Administrátorům k jimi spravovaným aktivům.
- 8.5.2 Přístupová oprávnění Uživatelů i Administrátorů musí být pravidelně ověřována za dodržení následujících zásad:
- a) Přístupová oprávnění a zařazení do přístupových skupin či rolí pro běžné účty musí být kontrolována alespoň 1x za rok, nebo po jakékoliv větší změně v informačním systému / aplikace.
 - b) Účty s privilegovanými oprávněními musí být přezkoumávány v intervalu maximálně 6 měsíců.
 - c) Je-li informační systém / aplikace provozován dodavatelsky, je tento povinen na vyžádání Manažera kybernetické bezpečnosti poskytnout aktuální přehled uživatelských účtů a k nim přidělených přístupových oprávnění, včetně jmenného seznamu zaměstnanců cizích právních subjektů a jejich zařazení do rolí.
 - d) Vedoucí zaměstnanci musí v rámci přezkoumání potvrdit oprávněnost všech přístupů do informačních systémů / aplikací včetně rozsahu přidělených práv

a rolí. Všechny účty, pro které není tato oprávněnost potvrzena, musí být, na základě žádosti v nástroji ServiceDesk (případně se aplikuje postup dle čl. 8.2.11 tohoto předpisu), neprodleně deaktivovány a následně odstraněny.

- 8.5.3 O výsledcích kontroly je zpracována písemná zpráva, která je po schválení Garanty aktiva předložena Manažerovi kybernetické bezpečnosti.

8.6 Řízení přístupu aplikací

Všem informačním systémům aplikacím či jejich službám, které přistupují k informačním systémům / aplikacím jiným, musí být zřízeny technologické účty. Všechny technologické účty musejí mít přiděleného gestora a jejich správa se řídí pravidly platnými pro účty s privilegovanými oprávněními.

8.7 Řízení přístupu při mimořádných situacích

- 8.7.1 V případě mimořádných situací (např. při výskytu kybernetického bezpečnostního incidentu nebo instalaci kritických patchů), které vyžadují nestandardní a rychlý zásah do informačních systémů / aplikací, může být Manažerem kybernetické bezpečnosti udělena krátkodobá dočasná výjimka z pravidel řízení přístupu podle platného procesu řízení výjimek.

- 8.7.2 Pro každý jednotlivý informační systém / aplikaci či zařízení musí být vytvořen seznam Administrátorů, kteří se mohou, po dobu trvání mimořádné situace, stát držiteli účtu s privilegovanými oprávněními. Seznam spravuje Manažer kybernetické bezpečnosti na základě návrhů Garantů aktiv.

- 8.7.3 Používání všech takových účtů musí být monitorováno a po pominutí důvodu jejich vzniku musí být jejich použití přezkoumáno.

- 8.7.4 V okamžiku ukončení mimořádné situace zajistí Manažer kybernetické bezpečnosti odejmutí oprávnění k použití účtů s privilegovanými oprávněními a následně vyzve Garanty aktiv, aby zajistili vygenerování nových hesel.

- 8.7.5 Hesla k privilegovaným účtům pro mimořádné situace musí být uložena v zapečetěných obálkách umístěných v trezoru nebo ve specializovaných aplikacích určených pro ukládání hesel.

8.8 Specifika prostředí řídicích systémů

- 8.8.1 V prostředí řídicích systémů se přihlédne k Všeobecným technickým podmínkám a Zvláštním technickým podmínkám, případně dalším dokumentům, které určují provozní parametry, způsoby použití a správy předmětných podpůrných aktiv a metody přístupu k předmětným podpůrným aktivům.

- 8.8.2 Výjimky z opatření stanovených touto politikou musí být uvedeny v Krycím listu aktiva (viz kapitola 5 tohoto předpisu).

9 ŘÍZENÍ TECHNICKÝCH ZRANITELNOSTÍ

- 9.1 Řízení technických zranitelností je zaměřeno na monitorování technických zranitelností používaných informačních systémů / aplikací / zařízení, vyhledávání opravných balíčků a testování kvality zabezpečení s cílem odhalit nedostatky, jejichž zneužití by mohlo ohrozit Důvěrnost, Dostupnost či Integritu aktiv. Nalezené zranitelnosti jsou vstupem do Analýzy (přezkoumání) rizik, v jehož rámci je posouzena jejich závažnost a stanovena opatření, která pomohou snížit dopady takové zranitelnosti.

- 9.2 Pokud není uvedeno jinak, jsou za plnění požadavků řízení technických zranitelností podpůrných a primárních aktiv odpovědní jejich Bezpečnostní správci. O zjištěných zranitelnostech vede Bezpečnostní správce evidenci.

9.3 Požadavky na technickou bezpečnost

- 9.3.1 Za definici bezpečnostních opatření v rámci vývoje, změnového řízení, údržby a zániku aktiv v působnosti systému řízení bezpečnosti informací je odpovědný

Architekt kybernetické bezpečnosti. Za realizaci těchto opatření jsou odpovědní Garanti aktiv. Před každým pořízením, vývojem, změnou nebo implementací systému / aplikace / zařízení musí být zdokumentováno jejich naplnění. Požadavky musí být plněny úměrně výsledkům Analýzy (přezkoumání) rizik. Zváženy musí být minimálně následující bezpečnostní požadavky:

- a) validace vstupních dat,
- b) kontrola vnitřního zpracování dat,
- c) Integrita zpráv a ochrana komunikace,
- d) ochrana Důvěrnosti, Dostupnosti, Integrity, autenticity a nepopiratelnosti odpovědnosti za data při zpracování a přenosu,
- e) kontrola výstupních dat,
- f) autentizace a autorizace Uživatelů,
- g) monitorování a audit důležitých aktivit.

9.3.2 Při použití kryptografických opatření musí vždy být stanovena odpovídající úroveň kryptografické ochrany, způsob ochrany kryptografických prostředků (zejména klíčů) a způsob správy kryptografických prostředků dle Politiky použití kryptografických prostředků (čj. 56789/2018-SŽDC-GR-O30).

9.3.3 Jsou-li účastníky procesu řízení změn nebo provozu Dodavatelé, přechází na ně všechny relevantní povinnosti, a to na základě smluvního vztahu. Za zahrnutí povinností řízení technických zranitelností do smlouvy je odpovědný vlastník smluvního vztahu nebo Garant aktiva.

9.4 **Řízení technických zranitelností použitých technologií**

9.4.1 Pro aktiva v působnosti systému řízení bezpečnosti informací musí být stanoven proces pro kontinuální sledování technických zranitelností systémů a zařízení (resp. použitých technologií). To obnáší sledování hlášení výrobců používaného HW a SW a hlášení Dodavatelů nebo jiných odborných informačních zdrojů.

9.4.2 Zjištěné technické zranitelnosti musí být posouzeny z hlediska možných vlivů na úroveň bezpečnosti aktiv v působnosti systému řízení bezpečnosti informací. Musí být určena priorita jejich řešení, podle které, a v souladu s dalšími pravidly stanovenými tímto předpisem, jsou zranitelnosti vyřešeny. Řešení technických zranitelností a instalace opravných balíčků se řídí procesem pro řízení změn.

9.4.3 Řízení technických zranitelností je podporováno využitím automatizovaných nástrojů, které zjednodušují vyhledávání a nasazení oprav programového vybavení.

9.4.4 Za řízení technických zranitelností odpovídá Bezpečnostní správce, který vyhledává opravné programové balíčky a koordinuje jejich nasazení v provozním prostředí s Garanty aktiv.

9.4.5 Bezpečnostní správce je povinen provést prověření stavu technických zranitelností v rámci provozního prostředí nejméně jednou za tři měsíce. Zranitelnosti podpůrných aktiv, které jsou přímo dostupné z vnější sítě, prověřuje nejméně 1× za měsíc.

9.5 **Vyhledávání opravných programových balíčků**

9.5.1 Za vyhledávání opravných programových balíčků a dalších technických zranitelností je odpovědný Bezpečnostní správce, který musí pravidelně kontrolovat informace o zranitelnostech, které poskytují výrobci používaného HW a SW nebo jiné odborné informační zdroje, a vyhodnotit potřebnost nasazení doporučených záplat do provozního prostředí.

9.5.2 Opravy programového vybavení, které se týkají pracovních stanic (počítač [dále jen „PC“], notebook [dále jen „NB“]), jsou testovány automatickým nasazením na úzkém vzorku. V případě, že se neobjeví žádné vážné problémy, je nasazení opravy

propagováno na zbylé pracovní stanice. V případě vzniku problémů rozhoduje o dalším postupu Bezpečnostní správce.

- 9.5.3 Bezpečnostní správce ve spolupráci s Garantem podpůrných aktiv musí vyhodnotit rizika související s nasazením jednotlivých záplat a rozhodnout o tom, zda bude daná záplata nasazena a jakým způsobem bude provedeno otestování a nasazení.

9.6 **Nasazení oprav programového vybavení**

- 9.6.1 Bezpečnostní správce je ve spolupráci s Garanty podpůrných aktiv povinen provozní prostředí nastavit tak, aby bylo možné provést odinstalování oprav programového vybavení, jejichž nasazení nebylo úspěšné.

- 9.6.2 V případě neúspěšného nasazení opravy programového vybavení musí Bezpečnostní správce provést analýzu příčin neúspěchu. O výsledcích analýzy informuje Garanta podpůrného aktiva a Manažera kybernetické bezpečnosti.

9.7 **Testování technických zranitelností**

- 9.7.1 Pro aktiva přístupná z vnější sítě musí být před jejich uvedením do provozu, a po každé zásadní změně bezpečnostních mechanismů, prováděny testy zranitelností a penetrační testy. Testování technických zranitelností by mělo probíhat pomocí automatizovaných nástrojů. Výsledky testování musí být odborně vyhodnoceny, a to před uvedením aktiva do provozu nebo realizací změny do produkčního prostředí.

- 9.7.2 Za účelem testování musí být pro každý informační systém / aplikaci / zařízení vytvořeno testovací prostředí, které je odděleno od vývojového a produkčního prostředí tak, aby nebylo možno v rámci jednotlivých prostředí přistoupit k ostatním, a tak ovlivnit informační systém / aplikaci / zařízení, který je v daném prostředí provozován. Mezi těmito prostředí nesmí docházet ke sdílení uživatelských účtů.

9.8 **Omezení oprávnění pro instalaci SW**

Uživatelům nesmí být povoleno instalovat neschválený SW, nebo instalovat schválený SW bez povolení Administrátora.

9.9 **Specifika prostředí řídicích systémů**

- 9.9.1 V prostředí řídicích systémů se přihlídně k Všeobecným technickým podmínkám a Zvláštním technickým podmínkám, případně dalším dokumentům, které určují provozní parametry, způsoby použití a správy předmětných podpůrných aktiv a metody přístupu k předmětným podpůrným aktivům.

- 9.9.2 Výjimky z opatření stanovených touto politikou musí být uvedeny v Krycím listu aktiva (viz kapitola 5 tohoto předpisu).

10 **ZÁLOHOVÁNÍ A OBNOVA**

10.1 **Požadavky na zálohování**

- 10.1.1 Účelem zálohování je prevence ztráty dat v případě jejich nedostupnosti z důvodu selhání HW, krádeže apod. Garanti aktiv jsou odpovědní za stanovení přesných požadavků na provádění záloh. Minimální požadavky vyplývající z Dostupnosti aktiv jsou uvedeny v následující tabulce. Požadavky je rovněž nutné vždy upravit na základě výstupů Analýzy (přezkoumání) rizik.

Tabulka 2 – Minimální požadavky na zálohování

požadavek na dostupnost	frekvence záloh	dobu uložení záloh	další požadavky	frekvence testování
1	1× za týden plný	3 měsíce	---	2 roky
2	1× za den inkr. 1× za týden plný	3 týdny 3 měsíce	---	2 roky
3	1× za hodinu inkr. 1× za den plný 1× za měsíc plný	1 týden 3 týdny 3 měsíce	Využití redundance důležitých systémů.	1 rok
4	1× za hodinu inkr. 1× za den plný 1× za měsíc plný	1 týden 3 týdny 3 měsíce	Využití redundance se zrcadlením v návrhu řešení. Zajištění náhradních technických aktiv v určeném čase.	1 rok

- 10.1.2 Požadavek na frekvenci záloh se nevztahuje na dobu, kdy informační systém/ aplikace není používán nebo je mimo provoz (mimo běžnou pracovní dobu nebo během odstávky systému).
- 10.1.3 Pro všechna aktiva uchovávající data platí, že data, obraz aplikace a konfigurace aplikace jsou zálohovány samostatně.
- 10.2 **Pravidla a postupy zálohování**
- 10.2.1 Na základě požadavků na frekvenci zálohování vytvoří Garanti primárních aktiv pro každé aktivum Plán zálohování. Plán zálohování musí z pohledu zálohování obsahovat zejména:
- přehled primárních aktiv, která jsou zálohována,
 - způsob a frekvenci zálohování dat / informačních systémů / aplikací,
 - základní popis zálohovacího procesu,
 - způsob uložení a nakládání s pořízenými zálohami,
 - odpovědnosti a postupy při obnově ze zálohy.
- 10.2.2 Vlastní zálohování musí být zabezpečeno automatizovaně technickými prostředky, které na základě nastavených parametrů zajistí pravidelné provádění záloh dle definovaných pravidel a s definovanou frekvencí. Za toto nastavení v souladu s požadavky Garantů primárních aktiv odpovídá Garant podřídného aktiva.
- 10.2.3 O provádění záloh musí být vedeny provozní záznamy (např. do Provozního deníku, elektronicky v daném zálohovacím prostředku apod.). V rámci procesu zálohování je pak nutné sledovat úspěšnost záloh. V případě, že zálohovací proces často selhává,

nebo selže třikrát po sobě, musí být tato situace neprodleně řešena jako kybernetický bezpečnostní incident.

10.3 **Bezpečné uložení záloh**

10.3.1 Garant aktiva je odpovědný za stanovení požadavků na ochranu záloh, resp. zálohovacích médií, během jejich uložení a manipulace s nimi. Pohyby záložních médií mohou provádět určení zaměstnanci podle stanovených postupů. Zohledněny musí být zejména následující opatření:

- a) Redundance záloh – je-li to technicky a organizačně možné, musí být zálohy uloženy v geograficky vzdálené lokalitě. Tato lokalita musí být přiměřeně vzdálená kvůli ochraně před působením živelních pohrom (např. povodeň), ale současně dostupná, aby obnovení informačního systému / aplikace nepřekročilo stanovanou lhůtu pro obnovení.
- b) Logické zabezpečení záloh – zálohovací media musí být, v návaznosti na klasifikaci informací zpracovávaných daným aktivem, chráněna způsobem stanoveným v Politice klasifikace aktiv (čj. 56784/2018-SŽDC-GR-O30). Zálohy je též vhodné chránit proti smazání nebo nepovolené úpravě.
- c) Fyzické zabezpečení záloh – zálohy musí být uloženy v kontrolovaném prostředí, tak aby byly chráněny proti neoprávněné manipulaci, poškození, krádeži a přírodním vlivům.

10.3.2 Pokud je manipulace se zálohami zajišťována dodavatelsky, je za zahrnutí požadavků na zálohování do smlouvy odpovědný vlastník smluvního vztahu nebo Garant aktiva.

10.3.3 Použití záložních médií mimo stanovená pravidla musí být odsouhlaseno Garantem aktiva, případně ředitelem SŽT.

10.4 **Pravidla a postupy obnovy**

10.4.1 V případě, že dojde ke ztrátě dat v rámci produkčního prostředí, je nutné provést obnovu dat ze zálohy. Garant primárního aktiva je odpovědný za to, že je pro obnovu informačních systémů / aplikací zpracován Plán kontinuity činností. V případě podpůrných aktiv je, Garantem aktiva, zpracován Plán obnovy. Pravidla pro zpracování a obsah Plánu kontinuity činností a Plánu obnovy jsou uvedeny ve směrnici SŽ SM094 Směrnice ve věci systému řízení kontinuity procesů ve státní organizaci Správa železnic (čj. 38892/2024-SŽ-GR-O30).

10.4.2 V případě, že jsou za některé z činností spojených s obnovou odpovědní Dodavatelé, musí být k plnění těchto činností smluvně zavázáni formou SLA. Za zahrnutí těchto požadavků do smlouvy je odpovědný vlastník smluvního vztahu nebo Garant aktiva.

10.5 **Testování zálohování a obnovy**

10.5.1 Za účelem zajištění spolehlivého fungování procesů zálohování a obnovy je nutné pravidelně, alespoň 1× za půl roku, testovat obnovitelnost záloh s tím, že musí být prověřena čitelnost alespoň celé sady záložních médií. Cílem testování je ověřit, zda je ze zálohovacích médií možné obnovit data v plném rozsahu, v požadovaném čase a bez narušení jejich Integrity. Testování musí být provedeno formou reálného obnovení dat podle Plánu kontinuity činností a kontrolou jejich úplnosti a Integrity. O průběhu testu a jeho výsledcích musí být proveden záznam. V případě selhání testu se postupuje jako při řešení kybernetického bezpečnostního incidentu a test je třeba nejpozději do 6 měsíců opakovat.

10.5.2 Za řízení testu, jeho zdokumentování a návrh, a realizaci případných opatření je odpovědný Garant aktiva.

10.6 **Specifika prostředí řídicích systémů**

10.6.1 V prostředí řídicích systémů se přihlédne k Všeobecným technickým podmínkám a Zvláštním technickým podmínkám, případně dalším dokumentům, které určují provozní parametry, způsoby použití a správy předmětných podpůrných aktiv a metody přístupu k předmětným podpůrným aktivům.

- 10.6.2 Výjimky z požadavků stanovených touto politikou musí být uvedeny v Krycím listu aktiva (viz kapitola 5 tohoto předpisu).

11 OCHRANA PŘED ŠKODLIVÝM KÓDEM

- 11.1 Ochrana před škodlivým kódem je založena na:

- a) Úplném pokrytí provozního prostředí vhodnými nástroji pro ochranu před škodlivým kódem.
- b) Ochrana před škodlivým kódem je komplexní problematikou, která je zajištěna uceleným souborem vhodných nástrojů. Primární úsilí je věnováno ochraně komunikace mezi vnější sítí a interní datovou sítí, ochraně serverů a sdílených datových úložišť a ochraně pracovních stanic a mobilních zařízení.

11.2 Pravidelná aktualizace a údržba nástrojů pro ochranu před škodlivým kódem

Používané nástroje pro ochranu před škodlivým kódem musí být pravidelně aktualizovány a udržovány, aby byla zajištěna maximální účinnost těchto nástrojů.

11.3 Opatření proti škodlivému kódu

- 11.3.1 Na řídicích systémech³, je-li to technicky a organizačně možné, musí být nasazeny a udržovány vhodné nástroje pro ochranu před škodlivým kódem, která zajistí ošetření rizik spojených s působením škodlivého kódu.
- 11.3.2 Nástroje pro ochranu před škodlivým kódem musí prověřovat všechny komunikační kanály, jako jsou síťová připojení, brány elektronické pošty a pracovní stanice Uživatelů.
- 11.3.3 Garant aktiva zajistí provádění pravidelné a účinné aktualizace nástrojů pro ochranu před škodlivým kódem včetně jeho definic a signatur.
- 11.3.4 Příslušný Bezpečnostní správce určí nezbytné postupy pro provozování a údržbu nástrojů pro ochranu před škodlivým kódem.

11.4 Ochrana komunikace mezi vnější sítí a interní datovou sítí

- 11.4.1 V rámci ochrany komunikace mezi vnější sítí a interní datovou sítí před škodlivým kódem musí být zavedena taková opatření, která zajistí, že:
 - a) veškerá komunikace mezi vnější sítí a interní datovou sítí je vedena přes demilitarizovanou zónu,
 - b) veškerá komunikace je vedena přes nástroj umožňující filtrování síťového provozu,
 - c) veškerá komunikace je kontrolována na výskyt škodlivého kódu.
- 11.4.2 Komunikace mezi vnější sítí a interní datovou sítí je kromě jiných nástrojů pro kontrolu a filtrování síťové komunikace monitorována nástrojem pro detekci/sběr a vyhodnocení kybernetických bezpečnostních událostí (viz směrnice SŽ SM074 Směrnice zvládání kybernetických bezpečnostních incidentů v informačním systému státní organizace Správa železnic).
- 11.5 **Ochrana serverů a sdílených datových úložišť**
- 11.5.1 Bezpečnostní správce zajistí pravidelnou kontrolu serverů a sdílených datových úložišť na výskyt škodlivého kódu.
- 11.5.2 Za účelem ochrany před škodlivým kódem je v případě serverů a datových úložišť vyžadováno splnění alespoň následujících požadavků:

³ U řídicích systémů je nutné zajistit, že nasazení nástroje pro ochranu před škodlivým kódem nebude mít dopady, které by ohrozily provoz těchto systémů. S nasazením řešení musí souhlasit příslušný Garant aktiva.

- a) oddělení interní datové sítě od vnější sítě s využitím nástrojů pro kontrolu a filtrování síťové komunikace (např. antivirové Proxy, firewally apod.);
- b) využití antivirové ochrany serverů;
- c) udržování aktuálního programového vybavení (sledování a řešení technických zranitelností informačních systémů / aplikací / zařízení instalací aktualizací a bezpečnostních záplat apod.);
- d) použití nástrojů pro detekci a vyhodnocování kybernetických událostí.

11.6 Ochrana pracovních stanic

11.6.1 Pracovní stanice musí být vybaveny nástroji pro ochranu před škodlivým kódem a sledováním změn operačního systému a souborového systému. Za implementaci a údržbu těchto nástrojů odpovídá Bezpečnostní správce.

11.6.2 Za účelem ochrany před škodlivým kódem musí být v případě pracovních stanic zavedeno:

- a) instalace antivirové ochrany, zajištění její aktuálnosti a zamezení její deaktivace Uživatelem;
- b) použití nástrojů pro filtrování síťového provozu (personální firewally), a to zejména u Uživatelů přistupujících do vnější sítě;
- c) udržování aktuálního programového vybavení;
- d) instalace pouze schváleného SW, který byl prověřen na výskyt škodlivého kódu;
- e) zamezení spouštění kódu Uživateli;
- f) monitorování využívání výměnných médií;
- g) řízení automatického spouštění obsahu připojených výměnných médií.

11.6.3 Povinnosti Uživatelů s ohledem na ochranu před škodlivým kódem určuje předpis SŽ R10 Řád Informatiky (čj. 15860/2022-SŽ-GR-O22).

11.7 Specifika prostředí řídicích systémů

11.7.1 V prostředí řídicích systémů se přihlédne k Všeobecným technickým podmínkám a Zvláštním technickým podmínkám, případně dalším dokumentům, které určují provozní parametry, způsoby použití a správy předmětných podpůrných aktiv a metody přístupu k předmětným podpůrným aktivům.

11.7.2 Výjimky z požadavků stanovených tímto předpisem musí být uvedeny v Krycím listu aktiva (viz kapitola 5 tohoto předpisu).

12 LOGOVÁNÍ A MONITORING

12.1 V rámci provozu informačních systémů / aplikací / zařízení v působnosti systému řízení bezpečnosti informací musí být použity nástroje pro zaznamenávání událostí, které zajistí:

- a) sběr informací o provozních a bezpečnostních událostech; zejména typ činnosti, datum a čas, identifikace aktiva, které činnost zaznamenalo, identifikace původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti;
- b) ochranu informací před neoprávněným čtením nebo změnou.

12.2 Nástroje musí být schopné zaznamenávat následující činnosti:

- a) změny konfigurace nástroje pro sledování událostí:
 - pokus o změnu konfigurace oprávněným Administrátorem,
 - pokus o změnu konfigurace neoprávněnou osobou,
 - změna souborů nástroje;
- b) přihlášení (a odhlášení) k podpůrným aktivům (Uživatelé/Administrátoři);
- c) činnosti prováděné Administrátory (s využitím privilegovaných oprávnění):
 - k jakému zařízení přistoupili,
 - jaké otevřeli soubory a dokumenty (včetně logů),
 - změny konfigurace,
 - změny souborů,
 - v případě Uživatelů logování pokusů o přístup k těm souborům či dokumentům, ke kterým nemají přístupová oprávnění;
- d) činnosti vedoucí ke změně přístupových oprávnění:
 - změna hesla včetně pokusů o jejich provedení,
 - reset hesla včetně pokusů o jejich provedení,
 - včetně pokusů o jejich provedení;
- e) neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti Uživatelů:
 - zadání nesprávného přihlašovacího jména oprávněným Uživatelem,
 - zadání nesprávného hesla oprávněným Uživatelem,
 - zadání nesprávného přihlašovacího jména neoprávněnou osobou či strojem,
 - zadání nesprávného hesla neoprávněnou osobou či strojem,
 - pokus o přistoupení k souborům/dokumentům, ke kterým nemají oprávnění;
- f) zahájení a ukončení činností podpůrných aktiv;
- g) automatická varovná nebo chybová hlášení podpůrných aktiv:
 - HW (PC, NB, servery, virtuální servery, síťové prvky, sandbox, FW, IDS /IPS, Proxy atd.),
 - SW (aplikace / informační systémy);
- h) deaktivace běhu technických prostředků:
 - antivirový systém,
 - FW,
 - IDS/IPS;

- i) přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech:
 - přístup k logům,
 - pokusy o smazání logů,
 - pokusy o změnu logů;
- j) použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení;
- k) specifiky prostředí Microsoft (MS):
 - změna/přidání/odstranění záznamů v registrech,
 - změna/přidání/odstranění služeb (včetně start, stop a způsobu spouštění),
 - změna/přidání/odstranění/konfigurace ovladačů či aplikací,
 - změna/přidání/odstranění/konfigurace zařízení,
 - změna/přidání/odstranění práv k adresářům a souborům;
- l) specifiky prostředí UX:
 - změna/přidání/odstranění služeb (včetně start, stop a způsobu spouštění),
 - změna/přidání/odstranění/konfigurace ovladačů či aplikací,
 - změna/přidání/odstranění/konfigurace zařízení,
 - změna/přidání/odstranění práv k adresářům a souborům.

12.3 **Zaznamenávání událostí formou logů**

- 12.3.1 Záznamy (logy) musí být v informačních systémech / aplikacích / zařízeních pořizovány a uchovávány takovým způsobem, aby byly využitelné pro monitorování řízení přístupu a případné budoucí vyšetřování kybernetického bezpečnostního incidentu.
- 12.3.2 Garant aktiva ve spolupráci s Architektem kybernetické bezpečnosti musí, v souladu se zájmy SŽ, určit a udržovat požadavky na zaznamenávání událostí formou logů dle čl. 12.2 tohoto předpisu. V případě, že aktivum, v návaznosti na typ a klasifikaci vyžaduje logování odlišné či podrobnější, stanoví Garant aktiva, v součinnosti s Architektem kybernetické bezpečnosti, požadavky další.
- 12.3.3 Za vyhodnocování logů je odpovědná oprávněná osoba.
- 12.3.4 Záznam událostí musí formou logů obsahovat (v případě, že to informační systém / aplikace / zařízení umožňují):
 - a) jednoznačnou identifikaci účtu provádějícího akci;
 - b) činnosti informačního systému / aplikace / zařízení;
 - c) datum, čas a podrobnosti důležitých událostí, například přihlášení a odhlášení;
 - d) identitu nebo umístění zařízení, pokud je to možné, a identifikátor informačního systému / aplikace / zařízení;
 - e) záznamy o úspěšných a odmítnutých pokusech o přístup k informačnímu systému / aplikaci / zařízení;

- f) záznamy o úspěšných a odmítnutých pokusech o přístup k datům a dalším zdrojům;
 - g) změny konfigurace informačního systému / aplikace / zařízení;
 - h) použití systémových nástrojů a aplikací;
 - i) použití účtů s privilegovanými oprávněními;
 - j) soubory, ke kterým bylo přistupováno, a typ přístupu;
 - k) síťové adresy a protokoly;
 - l) poplachy vyvolané systémem řízení přístupu;
 - m) aktivace a deaktivace ochranných systémů, jako jsou antivirové systémy, sandbox, IDS/IPS, FW, Proxy atd.);
 - n) záznamy transakcí provedených Uživateli v informačních systémech/aplikacích.
- 12.3.5 Za funkčnost nástroje pro zaznamenávání událostí v informačních systémech / aplikacích / zařízeních odpovídá Manažer kybernetické bezpečnosti. Za prosazování zásad monitorování a auditu pro jednotlivé informační systémy / aplikace / zařízení, včetně pořizování a archivace auditních záznamů, odpovídá příslušný Garant aktiva.
- 12.3.6 Záznamy (logy) se uchovávají minimálně po dobu 18 měsíců, nicméně Garant aktiva může rozhodnout o prodloužení této doby.
- 12.3.7 Datová kapacita úložiště logů musí být do budoucna rozšiřitelná tak, aby respektovala možné budoucí změny závazné legislativy i dodatečné požadavky Garantů aktiv (viz čl. 12.3.6 tohoto předpisu).
- 12.4 **Ochrana logů**
- 12.4.1 Nástroje pro uchovávání logů, stejně jako logy samotné, musí být chráněny proti neoprávněnému přístupu a změně, aby byla zachována jejich Integrita a autenticita. Administrátoři musí mít přístup k logům generovaným informačními systémy/aplikacemi, síťovými prvky, servery a dalšími prvky ICT Infrastruktury, na jejich správě se podílejí, ale nesmí mít oprávnění záznamy upravovat či mazat nebo deaktivovat vytváření záznamů o své vlastní činnosti. Přístup k záznamům o činnostech musí být povolen pouze určeným osobám. Tyto osoby naopak nesmí disponovat privilegovanými oprávněními určenými ke správě informačních systémů/aplikací, síťových prvků, serverů a dalších prvků ICT Infrastruktury.
- 12.4.2 Kdyby došlo k pozměnění záznamů nebo byly některé záznamy o událostech vymazány, může vzniknout falešný pocit bezpečnosti. Kopírování logů do samostatného informačního systému / aplikace / zařízení, který je mimo správu Administrátorů, je jednou z možných ochran.
- 12.5 **Záznamy o činnosti Administrátorů**
- 12.5.1 Aktivity Administrátorů musí být zaznamenávány formou logů, které by měly být chráněny a jejich obsah a Integrita pravidelně přezkoumávány tak, aby bylo zajištěno odpovědné použití všech privilegovaných oprávnění. Za zajištění logování odpovídá Garant aktiva, za přezkoumání logů je odpovědný Bezpečnostní správce.
- 12.5.2 K monitorování činností prováděných během správy informačních systémů / aplikací / zařízení, musí být použit nástroj spravovaný jinými osobami než Administrátory.

- 12.5.3 Následující činnosti musí být součástí logů o činnosti Administrátorů:
- a) přihlášení a odhlášení k účtům Administrátorů a dalším účtům s privilegovanými oprávněními;
 - b) nakládání s účty, jako je přidání nového účtu, uzamčení či zrušení účtu, změny přístupových hesel apod.;
 - c) nakládání s nástroji a zařízeními pro zpracování informací a síťovými prostředky, jako je přidání nového zařízení či odebrání rušeného zařízení;
 - d) změny bezpečnostních parametrů, jako jsou změna politiky přístupových hesel, změna politiky logování, změny nastavení času, změny konfigurace serverů včetně virtuálních, změny pravidel antivirového systému, sandboxu, FW, IDS/IPS, Proxy, změny pravidel přepínání a směrování apod.;
 - e) přístupy k primárním a podpůrným aktivům, jako jsou úložiště přístupových hesel, úložiště logů, úložiště kryptografických klíčů, evidence kybernetických událostí či kybernetických bezpečnostních incidentů apod.;
 - f) použití systémových nástrojů, které mohou snižovat efektivnost a účinnost opatření systému řízení bezpečnosti informací (použití nástrojů pro rozpoznání topologie sítě, nástroje pro odhalení zranitelností, nástroje pro zachytávání, hesel apod.).
- 12.5.4 Administrátoři dále zaznamenávají důležité úkony provedené v informačních systémech / aplikacích / zařízeních (zapínání nebo vypínání služeb, prováděné opravy, změny nebo pravidelná údržba apod.) do Provozních deníků. Ty musí být z provozních důvodů dostupné všem ostatním Administrátorům.
- 12.5.5 Záznam v Provozním deníku musí obsahovat alespoň následující údaje:
- a) datum a čas záznamu,
 - b) název události nebo aktivity,
 - c) informační systém / aplikace / zařízení, na kterém byl úkon prováděn,
 - d) popis události nebo aktivity,
 - e) autor záznamu – jednoznačná identifikace autora (např. jméno a příjmení, osobní číslo apod.).
- 12.6 **Synchronizace systémového času**
- 12.6.1 Systémový čas informačních systémů / aplikací / zařízení (a všech relevantních podpůrných aktiv) musí být v rámci SŽ synchronizován s jediným referenčním zdrojem.
- 12.6.2 Přesné nastavení systémového času je důležité proto, aby byla zajištěna přesnost logů o činnostech informačních systémů / aplikací / zařízení (a všech dalších relevantních podpůrných aktiv) a aktivitách spojených s jejich správou, které mohou být využívány během vyšetřování nebo jako důkazy v případě právních nebo jiných sporů souvisejících s kybernetickými útoky či s porušením povinností při jejich výskytu. Nepřesné logy mohou vyšetřování ztížit a poškodit věrohodnost takovýchto důkazů.
- 12.6.3 Musí být definován standardní referenční čas, který ovšem nesmí vycházet pouze z jednoho zdroje času.
- 12.6.4 Synchronizace systémového času informačních systémů / aplikací / zařízení (a všech relevantních podpůrných aktiv) probíhá minimálně jednou za 24 hodin a je automatizovaná. Garant aktiva odpovídá za přesné nastavení parametrů pro synchronizaci času a provedení kontroly těchto nastavení:
- a) jednou týdně,

- b) po změně z a na letní čas,
 - c) po změně verze programového vybavení.
- 12.6.5 O synchronizaci systémového času musí být prokazatelný záznam. Případné selhání synchronizace systémového času musí být řešeno jako méně významný kybernetický bezpečnostní incident (kategorie I).
- 12.7 **Specifika prostředí řídicích systémů**
- 12.7.1 V prostředí řídicích systémů se přihlédně k Všeobecným technickým podmínkám a Zvláštním technickým podmínkám, případně dalším dokumentům, které určují provozní parametry, způsoby použití a správy předmětných podpůrných aktiv a metody přístupu k předmětným podpůrným aktivům.
- 12.7.2 Výjimky z požadavků stanovených touto politikou musí být uvedeny v Krycím listu aktiva (viz kapitola 5 tohoto předpisu).

13 ŘÍZENÍ ZMĚN

13.1 Principy řízení změn

- 13.1.1 Jakékoliv změny provedené na aktivech v působnosti systému řízení bezpečnosti informací musí být prováděny takovým způsobem, aby byla trvale zaručena Důvěrnost, Dostupnost a Integrita zpracovávaných informací a prováděných procesů.
- 13.1.2 Ředitel SŽT, ředitel O14, ředitel O24 a ředitel CTD jsou odpovědní za určení procesu řízení změn, zohlednění požadavků na kybernetickou bezpečnost v rámci tohoto procesu a řízení všech žádostí o změnu za svou oblast v souladu s tímto procesem.
- 13.1.3 Všechny žádosti o změnu a záznamy o jejich schválení musí být zaznamenány v nástroji ServiceDesk.
- 13.1.4 Po každé změně bezpečnostních mechanismů informačního systému / aplikace musí být proveden test zranitelnosti a penetrační test.
- 13.1.5 Proces řízení změn musí splňovat alespoň následující požadavky:
- a) Všechny fáze musí být řádně evidovány a dokumentovány předepsaným způsobem.
 - b) Účel změny a všechny další kroky její implementace musí být řádně popsány.
 - c) Požadavek na změnu musí být schválen Garantem aktiva, případně jejich nadřízenými, případně dalšími odpovědnými osobami.
 - d) Pro každou změnu musí být provedena analýza dopadů, která zhodnotí potenciální dopady na Důvěrnost, Dostupnost a Integritu na aktiva v působnosti systému řízení bezpečnosti informací a na soulad s požadavky bezpečnostních politik. Případné nesoulady musí schválit Manažer kybernetické bezpečnosti jako výjimku dle procesu řízení výjimek definovaného v Politice systému řízení bezpečnosti informací.
 - e) U každé změny musí být ověřeno, zda obsahuje informace o souvisejících rizicích a zohledňuje požadavky na kybernetickou bezpečnost a řízení kontinuity.
 - f) Při každé změně, pokud je to relevantní, musí být připravena komunikace směrem ke koncovým Uživatelům a provedeno jejich poučení.
 - g) Musí být identifikovány ty části bezpečnostních politik, které bude nutné po implementaci změny upravit.
 - h) Musí být identifikovány ty části pracovních postupů, které bude nutné po implementaci změny upravit.

- i) Všechny změny musí být před schválením a implementací do provozního prostředí řádně otestovány, včetně regresních testů dopadů na další aktiva. Za vypracování testovacích scénářů je odpovědný Garant aktiva.
- j) Implementaci změny musí předcházet schválení Garanty dotčených aktiv.
- k) Postup implementace v produkčním prostředí musí být řádně zdokumentován.
- l) Pro případ selhání implementace musí být připraven postup pro stažení změny z produkčního prostředí (rollback plán).
- m) Pro každou změnu musí být provedeno vyhodnocení úspěšnosti nasazení a případně stanovení požadavků na zlepšení.
- n) Po implementaci změny musí dojít k aktualizaci údajů v konfigurační databázi (dále jen „CMDB“).
- o) Během procesu řízení změny musí být dodržována povinnost oddělení rolí, a to alespoň v následujícím rozsahu:
 - oddělení rolí mezi žadatelem a schvalovatelem,
 - oddělení rolí mezi vývojem a testováním,
 - oddělení rolí mezi schvalovatelem a osobou provádějící implementaci změny.

13.2 Změnový projekt

13.2.1 Jedná se o změnu:

- a) která má dopad na více informačních systémů / aplikací a širokou skupinu Uživatelů;
- b) ovlivňuje kybernetickou bezpečnost nebo kontinuitu informačních systémů / aplikací;
- c) její provedení může být vysoce rizikové v případě, že by byla podceněna řádná příprava.

13.2.2 Provedení změny musí být projednáno Garanty aktiv a schvalováno Výborem pro řízení kybernetické bezpečnosti.

13.3 Významná změna

13.3.1 Z hlediska kybernetické bezpečnosti se za Významnou změnu považuje taková změna, která má významný vliv na bezpečnost aktiv v působnosti systému řízení bezpečnosti informací nebo na výsledky Analýzy (přezkoumání) rizik.

13.3.2 Za Významnou změnu je možné považovat:

- a) změny pravidel ochranných systémů (sandbox, FW, IDS/IPS, Proxy), aplikačních firewallů a pravidel přepínání a směrování v sítích;
- b) změny autentizačních mechanismů (politika hesel, politika logování apod.);
- c) přidání, změna nebo odebrání služeb, informačních systémů / aplikací nebo ochranných systémů;
- d) změny, které umožňují sdílení informací, služeb nebo zdrojů mimo provozní prostředí;
- e) vytvoření Proxy serverů;
- f) změny, opatření pro zajištění bezpečnosti vzdáleného přístupu;
- g) zavedení skriptů pro automatické přihlášení;

- h) migraci dat do jiné databáze;
 - i) změna Dodavatele;
- 13.3.3 Pro Významné změny, kromě požadavků uvedených v čl. 13.1.5 tohoto předpisu, platí:
- a) Požadavek na změnu musí být schválen Manažerem kybernetické bezpečnosti.
 - b) Přezkum dopadů Významné změny je potřeba konzultovat s Manažerem kybernetické bezpečnosti, který vyhodnotí rizika související s implementací změny.
 - c) V rámci testování změny před implementací do produkce musí být provedeny i bezpečnostní testy, včetně penetračních. Scénář a rozsah bezpečnostních testů určí Manažer kybernetické bezpečnosti.
 - d) Provedení změny musí být před uvedením do produkce znovu schváleno Manažerem kybernetické bezpečnosti.
- 13.4 **Standardní změna**
- 13.4.1 Za účelem snížení administrativní zátěže v rámci procesu řízení změn je možné, pro každé aktivum v působnosti systému řízení bezpečnosti informací, definovat standardní změny. Jedná se většinou o opakující se změny, u nichž je již zavedený postup a předem znám či odhadnutelný možný dopad na fungování aktiv v působnosti systému řízení bezpečnosti informací.
- 13.4.2 Pro standardní změny není vyžadována analýza dopadů ani schválení před implementací. Standardní změny musí být definovány a popsány v provozní dokumentaci aktiva, která je schvalována Garantem aktiva a Manažerem kybernetické bezpečnosti.
- 13.5 **Naléhavá změna**
- 13.5.1 Změna, která musí být provedena co nejdříve, aby byly odvráceny negativní dopady spojené s neprovedením změny. Naléhavé změny mohou být prováděny zcela výjimečně.
- 13.5.2 Jakmile je to možné, musí být každá naléhavá změna dodatečně schválena v rámci procesu řízení změn.
- 13.6 **Změny služeb provozovaných Dodavateli**
- 13.6.1 V případě, že je informační systém / aplikace / zařízení provozováno dodavatelsky na vlastní ICT Infrastrukturu, musí Dodavatel s dostatečným předstihem informovat Garanta aktiva o záměru provést změnu a musí mu poskytnout relevantní podklady pro analýzu dopadů a zdokumentování všech požadavků procesu řízení změn.
- 13.6.2 Za zahrnutí všech povinností vyplývajících z procesu řízení změn do Smlouvy je odpovědný vlastník smluvního vztahu či Garant aktiva.
- 13.7 Specifika prostředí řídicích systémů
- Výjimky z požadavků stanovených tímto předpisem musí být uvedeny v Krycím listu aktiva (viz kapitola 5 tohoto předpisu).
- 14 AKVIZICE, VÝVOJ A ÚDRŽBA**
- 14.1 **Bezpečnostní požadavky na vývoj informačních systémů / aplikací**
- 14.1.1 Požadavky na bezpečnostní opatření pro zajištění Důvěrnosti, Dostupnosti a Integrity musí být součástí návrhu nového informačního systému / aplikace či změny stávajícího informačního systému / aplikace. Opatření navrhuje Architekt kybernetické bezpečnosti, přičemž zohlední předpokládanou (v případě nového

informačního systému / aplikace) a stávající klasifikaci informačního systému / aplikace.

14.1.2 Požadavky na nové informační systémy / aplikace nebo na změny stávajících musí zohledňovat zejména následující:

- a) požadavek na řízení přístupu (logického i fyzického),
- b) požadavek na bezpečné autentizační mechanismy,
- c) požadavek na použití šifrování,
- d) požadavek na úroveň logování,
- e) požadavek na integraci s nástroji pro monitorování bezpečnosti,
- f) požadavek na technologickou nezávislost na ICT Infrastruktuře,
- g) požadavek na soulad s uznávanými standardy aplikační bezpečnosti.

14.1.3 Naplnění všech bezpečnostních požadavků na vývoj informačních systémů / aplikací musí být vyžadováno smluvně. Za jejich zahrnutí do smlouvy odpovídá vlastník smluvního vztahu či Garant aktiva.

14.1.4 Naplnění všech požadavků musí být zdokumentováno takovým způsobem, aby bylo možné provést jejich audit v rámci přejímání dodávky.

14.1.5 Při nákupu krabicových produktů, které nesplňují požadavky na kybernetickou bezpečnost, musí být ještě před jejich nákupem zváženo přijetí dodatečných bezpečnostních opatření vedoucích k mitigaci identifikovaných rizik.

14.2 **Pravidla pro vývojové a testovací prostředí**

14.2.1 V rámci ICT Infrastruktury, která je součástí systému řízení bezpečnosti informací, musí být důsledně oddělena prostředí pro vývoj a testování od prostředí provozního. Za vytvoření podmínek pro rozdělení ICT infrastruktury na vývojové, testovací a provozní prostředí a za jejich bezpečný provoz odpovídá Garant podpůrného aktiva. Ve vývojovém a testovacím prostředí musí být dodrženy následující požadavky:

- a) Vývojové prostředí musí být dostatečně chráněno proti neautorizovanému přístupu, který by mohl vést k získání citlivých informací o vyvíjeném programovém vybavení nebo k jeho neautorizované změně.
- b) Pro přenos SW z vývojového do testovacího a následně do provozního prostředí musí být definována pravidla a odpovědnosti. Součástí těchto pravidel musí být kontrola na výskyt škodlivého kódu. Důsledně musí být aplikovány požadavky procesu řízení změn.
- c) Pro účely testování mohou být použita pouze data klasifikovaná jako Veřejná. V případě použití dat klasifikovaných jako Interní nebo vyšší je potřeba požádat Manažera kybernetické bezpečnosti o výjimku dle procesu řízení výjimek definovaného v Politice systému řízení bezpečnosti informací.
- d) Testovací data musí být dostatečně chráněna a kontrolována pro zamezení přístupu neautorizovaných osob. V případě použití neveřejných dat musí být v testovacím prostředí přijata stejná bezpečnostní opatření jako v produkčním prostředí.
- e) Pokud jsou pro testování použita provozní data, musí být použita neplatná data, případně musí být vytvořena syntetická data se stejnou strukturou.
- f) V případě, že jsou k testování používány osobní údaje, musí se provést jejich anonymizace (např. s využitím vhodného automatizovaného algoritmu).

14.2.2 Vývojové a testovací aktivity, které budou prováděny v provozním prostředí, musí být schváleny příslušným Garantem aktiva a Manažerem kybernetické bezpečnosti

a při jejich provádění musí být minimalizována související rizika, např. tím, že vývoj nebo testy budou realizovány mimo pracovní dobu, nebo tak, že rizika dopadu na provoz budou minimalizována.

14.3 **Testování před nasazením**

14.3.1 Před nasazením informačního systému / aplikace do produkčního prostředí se musí provést přezkoumání a testování. Testy musí zahrnovat minimálně následující:

- a) posouzení z pohledu vlivu na funkčnost a bezpečnost;
- b) funkční testy integrace s ostatními informačními systémy / aplikacemi;
- c) přezkoumání kontrolních opatření a postupů zajišťujících Důvěrnost, Dostupnost a Integritu;
- d) testování zranitelností;
- e) penetrační testy.

14.3.2 Za návrh scénářů a rozsahu bezpečnostních testů je odpovědný Manažer kybernetické bezpečnosti. Informační systém / aplikace může být uveden do produkčního provozu až po akceptaci výsledků testů Manažer kybernetické bezpečnosti.

14.4 **Plánování systémů**

14.4.1 Během plánování nových informačních systémů / aplikací musí být zabezpečeno splnění následujících požadavků:

- a) příprava na integraci do stávajícího provozního prostředí;
- b) ověření, že instalace nového informačního systému / aplikace neovlivní nežádoucím způsobem existující informační systémy / aplikace;
- c) zavedení požadavků stanovených v bezpečnostní dokumentaci, v případě potřeby upřesněných Manažerem kybernetické bezpečnosti;
- d) příprava, standardizace a testování provozních procedur;
- e) nastavení procesů a vytvoření procedur pro obnovu po chybách a pro restart,
- f) školení v provozu a používání nových informačních systémů / aplikací;
- g) jednoduchost použití ve vazbě na výkonnost Uživatele a potlačení chyb obsluhy;
- h) zpracování provozní, administrátorské, uživatelské a bezpečnostní dokumentace;

14.4.2 Za zajištění zohlednění uvedených požadavků je odpovědný Vlastník projektu.

14.5 **Přejímání systémů**

14.5.1 V rámci každého projektu musí být vytvořena kritéria pro akceptaci informačních systémů / aplikací, jejich aktualizací a použití nových verzí. Součástí vývoje a dodávky informačních systémů / aplikací musí být i návrh vhodných akceptačních testů.

14.5.2 Kromě týmu, pověřeného řešením projektu, se do závěrečného testování musí zapojit i vybraní koncoví Uživatelé a Administrátoři. Pro tyto účastníky musí být vytvořen dostatečný časový prostor, aby se mohli s informačním systémem / aplikací seznámit a provést relevantní testování.

14.5.3 Všechny činnosti spojené s testováním informačního systému / aplikace, musí být prováděny mimo provozní prostředí. Při implementaci informačního systému / aplikace do provozního prostředí musí být dodrženy následující zásady:

- a) implementace, popř. aktualizace je prováděna pouze oprávněnými Administrátory;
- b) provozní systémy nesmí obsahovat vývojový SW (kód);
- c) informační systém / aplikace musí být, před přechodem do produkčního provozu, důkladně otestován (vč. bezpečnostního testování) a výsledky testů schváleny příslušnými Garanty aktiva a Manažerem kybernetické bezpečnosti;
- d) informační systém / aplikace musí v rámci konfigurace umožňovat aplikovat bezpečnostní požadavky;
- e) informační systémy / aplikace musí být zavedeny do CMDb a musí být dostupná veškerá dokumentace (provozní, administrátorská, uživatelská a bezpečnostní dokumentace);
- f) starší verze informačních systémů / aplikací musí být uchovány po dobu jednoho roku. Před upgradem na nový informační systém / aplikaci se provede kompletní záloha stávajících verzí;
- g) při implementaci informačního systému / aplikace do produkčního prostředí musí být postupováno podle procesu řízení změn. V rámci toho musí být připraven přesný postup, aby se snížila rizika poškození provozního prostředí;
- h) informační systém / aplikace musí umožnit odstranění nebo změnu výchozích přístupových údajů pro Administrátory;
- i) přístup ke zdrojovému kódu musí být omezen pouze na oprávněné osoby;
- j) při implementaci do produkčního prostředí musí být přijata taková opatření, která umožní případné navrácení do stavu před zahájením migrace.

14.5.4 Převzetí informačního systému / aplikace (např. do testovacího provozu) je možné provést i tehdy, nejsou-li splněny všechny funkční / nefunkční požadavky či smluvní ujednání. Např., když byly zjištěny nedostatky, které nejsou závažné. Nicméně akceptace informačního systému / aplikace je možná až po jejich celkovém napravení.

14.5.5 Akceptaci informačního systému / aplikace je možné provést pouze tehdy, jsou-li splněny veškeré funkční / nefunkční požadavky či smluvní ujednání a splněna veškerá definovaná akceptační kritéria.

14.5.6 Uživatelská dokumentace musí být v českém jazyce. Kvalita dokumentace musí být testována na skupině vybraných koncových Uživatelů, kteří s její pomocí, a po zaškolení, musí zvládnout běžnou práci v informačním systému / aplikaci.

14.6 Vyřazování aktiv

14.6.1 Vyřazování informačních systémů / aplikací musí vždy probíhat takovým způsobem, aby byla zaručena kontinuita provozu a bezpečnost všech aktiv a zaručeno splnění legislativních požadavků. Zejména je nutné dodržet:

- a) Všechny služby a informace poskytované vyřazovaným informačním systémem / aplikací musí být migrovány na jiné provozované aktivum.
- b) Veškerá data a konfigurace vyřazovaného informačního systému / aplikace musí být zálohována takovým způsobem a v takovém rozsahu, aby ho bylo možné v budoucnu obnovit. Zálohy musí být uloženy alespoň tak dlouho, kolik pro data zpracovávaná informačním systémem / aplikací vyžaduje Politika archivace informací (čj. 56870/2018-SŽDC-GR-O30) a předpis SŽ R2 Spisový řád státní organizace Správa železnic.
- c) Všichni Uživatelé informačního systému / aplikace musí být informováni o jeho deaktivaci, a musí jim být, pokud budou nadále provádět činnosti původně

podporované rušeným informačním systémem / aplikací, zpřístupněna adekvátní náhrada.

- d) Před samotným vypnutím služeb je informační systém / aplikace převeden do módu údržby. V tomto módu jsou služby poskytované informačním systémem / aplikací nepřístupné běžným Uživatelům. Umožňují-li to technické podmínky, musí být možné Informační systém / aplikaci, v případě nečekané události, převést zpět do produkčního provozu.
- e) Před samotným vyřazením informačního systému / aplikace je nezbytné zrušit veškerá přístupová oprávnění a revokovat veškeré certifikáty.

14.6.2 Za bezpečné vyřazení aktiva je odpovědný příslušný Garant.

14.7 **Specifika prostředí řídicích systémů**

Výjimky z požadavků stanovených touto politikou musí být uvedeny v Krycím listu aktiva (viz kapitola 5).

15 **SOFTWAREVÉ LICENCE**

15.1 **Nasazení programového vybavení a jeho evidence**

- 15.1.1 V rámci správy aktiv musí být vedena evidence a kontrolováno používání SW. Nastavená pravidla a postupy musí zajistit užívání SW výlučně oprávněnými Uživateli na základě licenčních smluv, důsledného souladu užívání SW s platnými právními předpisy ČR a příslušnými licenčními ujednáními a musí respektovat zákonná práva nositelů autorských a průmyslových práv k jednotlivým SW produktům.
- 15.1.2 O pořízení SW produktů a jejich schválení pro provozní prostředí rozhoduje SŽT, a to v souladu se směrnicí SŽDC č. 54 Směrnice k pořízení IS/IT a provozu jednotné evidence HW, SW a SW licencí programem AW Caesar.
- 15.1.3 SŽT odpovídá za evidenci a udržování dokumentace o vlastnictví licencí. Nelze provést instalaci SW, aniž by došlo k ověření dostupnosti licence.
- 15.1.4 Instalace standardního SW na pracovní stanice je v odpovědnosti pověřeného zaměstnance SŽT či jím metodicky řízeného zaměstnance OJ. Na pracovních stanicích musí být použito jednotné bezpečné nastavení operačního systému a základního SW. O instalaci SW je vždy proveden záznam do nástroje ServiceDesk.
- 15.1.5 Instalace individuálního SW na pracovní stanice je v odpovědnosti Administrátora, který případně spolupracuje s Dodavatelem nebo Garantem aktiva. Na uživatelská zařízení (tj. pracovní stanice, mobilní zařízení apod.) je instalován pouze SW vedený na seznamu standardního SW. V případě, že Uživatel pro svojí pracovní činnost vyžaduje SW, který na seznamu standardního SW není, požádá o nainstalování daného SW prostřednictvím nástroje ServiceDesk. Požadavek podléhá schválení přímého nadřízeného a ředitele SŽT.
- 15.1.6 Neoprávněná instalace autorsky chráněného SW, freeware nebo shareware Uživateli je zakázána.
- 15.1.7 Instalace SW na servery a další prvky ICT Infrastruktury je řízeno procesem řízení změn (viz kapitola 13 tohoto předpisu).
- 15.2 **Kontrola dodržování licenčních podmínek**
- 15.2.1 Za dodržování podmínek licenčních smluv odpovídá Uživatel, kterému byl SW poskytnut.
- 15.2.2 SŽT, O14, O24 a CTD vedou evidenci licencí instalovaného SW a jsou odpovědní za pravidelné (min. 1× za dva roky) prověřování shody této evidence se skutečně nainstalovaným SW, resp. s počty nakoupených licencí.
- 15.3 **Specifika prostředí řídicích systémů**

Výjimky z požadavků stanovených touto politikou musí být uvedeny v Krycím listu aktiva (viz kapitola 5 tohoto předpisu).

16 SERVICEDESK

16.1 Pro každé aktivum v působnosti systému řízení bezpečnosti informací musí být určeno pracoviště a nástroj ServiceDesk, na které se mohou obracet jeho Uživatelé v případě zjištění porušení bezpečnosti informací či podezření na něj. Kontaktní informace na pracoviště ServiceDesk musí být popsány v provozní dokumentaci aktiva.

16.2 Nástroj ServiceDesk je používán minimálně pro:

- a) zřizování uživatelských účtů,
- b) přidělování přístupových práv,
- c) vyřizování žádostí Uživatelů,
- d) řízení změn,
- e) řešení provozních incidentů,
- f) příjem hlášení kybernetických událostí.

16.3 Nástroj ServiceDesk musí být pro Uživatele dostupný minimálně v době, kdy je běžně dané aktivum používáno, případně musí být k dispozici náhradní způsob pro nahlášení porušení kybernetické bezpečnosti či podezření na něj. Garant aktiva je odpovědný za to, že jsou pro vyřizování žádostí, incidentů apod. stanovena interní SLA, jejichž plnění musí být alespoň 1 × ročně vyhodnocováno.

16.4 Všechny záznamy v nástroji ServiceDesk vztahující se k aktivům v působnosti systému řízení bezpečnosti informací musí být řádně zabezpečeny tak, aby nedošlo k porušení bezpečnostních politik, a musí být archivovány po dobu alespoň tří let.

16.5 Pokud je aktivum provozováno Dodavatelem, musí být všechny požadavky na úroveň poskytování služeb pracoviště ServiceDesk (včetně nástrojů, souvisejících procesů a komunikačních kanálů) definované Garantem aktiva, vedeny jako smluvní požadavky. Za zahrnutí těchto požadavků do Smlouvy je odpovědný vlastník smluvního vztahu či Garant aktiva.

16.6 Náležitosti žádosti

Pro každou žádost v nástroji ServiceDesk musí být evidovány minimálně následující náležitosti:

- a) jméno a příjmení zadavatele,
- b) popis žádosti (jakého informačního systému / aplikace / zařízení se týká),
- c) kategorizace a naléhavost žádosti,
- d) identifikace schvalovatele žádosti,
- e) lhůta pro řešení žádosti,
- f) řešitel žádosti,
- g) popis řešení žádosti.

16.7 Specifika prostředí řídicích systémů

Výjimky z požadavků stanovených touto politikou musí být uvedeny v Krycím listu aktiva (viz kapitola 5 tohoto předpisu).

17 BEZPEČNÉ PŘEDÁVÁNÍ A VÝMĚNA INFORMACÍ

17.1 Pravidla předávání a přístupu k informacím

17.1.1 V případě, že dochází k výměně informací mezi informačními systémy / aplikacemi mimo systém řízení bezpečnosti informací, musí být jejich výměna upravena Dohodou o výměně informací, s výjimkou výměny informací, která je upravena zákonem (např. zák. 365/2000 Sb., o informačních systémech veřejné správy; zák. 111/2009 Sb., o základních registrech).

17.1.2 Pokud je třeba, aby zaměstnanci cizích právních subjektů měli přístup k informacím klasifikovaným jako Interní a vyšší, jsou tyto informace poskytovány výhradně na základě uzavření Rámcové dohody o přístupu k důvěrným informacím dle pokynu SŽDC PO-22/2018-GŘ Pokyn GŘ Rámcová dohoda o ochraně důvěrných informací (případně obdobné dohodě), mezi SŽ a daným cizím právním subjektem.

17.1.3 Dohoda musí upravovat minimálně následující oblasti:

- a) vzájemné povinnosti obou stran;
- b) definici důvěrných a veřejných informací;
- c) postupy pro zajištění sledovatelnosti a nepopiratelnosti;
- d) požadavky na ochranu důvěrných informací;
- e) bezpečnostní pravidla pro předávání informací / přístup k informacím;
- f) odpovědnosti a povinnosti v případě kybernetických bezpečnostních incidentů;
- g) postup změnového řízení dohody;
- h) sankce za nedodržení dohody.

17.1.4 Předávání informací uvnitř systému řízení bezpečnosti informací se řídí interními postupy pro práci s informacemi klasifikovanými dle stupnice uvedené v Politice klasifikace aktiv (čj. 56784/2018-SŽDC-GŘ-O30).

17.1.5 Informace, které jsou veřejně přístupné (např. webové stránky), musí být chráněny proti neoprávněné modifikaci. Pro publikování veřejně přístupných informací je povoleno užívat pouze oficiální systémy ve správě SŽ, které splňují bezpečnostní požadavky, byla prověřena jejich bezpečnost (např. pomocí penetračních testů) a byly, k danému účelu, schváleny Manažerem kybernetické bezpečnosti.

17.1.6 Vedoucí zaměstnanci na úrovni odborů generálního ředitelství a výše, ředitelé oblastních ředitelství, ředitel Centra sdílených služeb, ředitelé stavebních správ, ředitelé centrálních dispečerských pracovišť, ředitelé Správ železniční geodézie, ředitel Správy železniční energetiky, ředitel CTD a ředitel HZS SŽ jsou oprávněni upřesnit pravidla pro specifické případy předávání a výměny informací v rámci své působnosti (např. odlišná pravidla použití sociálních sítí v případě tiskového mluvčího SŽ, apod.).

17.1.7 Za uzavření Rámcové dohody o ochraně důvěrných informací dle Pokynu GŘ Rámcová dohoda o ochraně důvěrných informací dle pokynu SŽDC PO-22/2018-GŘ Pokyn GŘ Rámcová dohoda o ochraně důvěrných informací s konkrétním Dodavatelem odpovídá vlastník smluvního vztahu.

17.2 Dohody o mlčenlivosti

Obsah a způsoby užití Rámcové dohody o ochraně důvěrných informací určuje pokyn SŽDC PO-22/2018-GŘ Pokyn GŘ Rámcová dohoda o ochraně důvěrných informací. Rámcová dohoda o ochraně důvěrných informací musí být uzavřena se všemi subjekty, se kterými jsou sdíleny informace kategorie Interní, Diskrétní či Vysoké diskrétní, a to i v případech, kdy se nejedná o Dodavatele/Provozovatele.

17.3 **Způsoby ochrany předávaných informací**

- 17.3.1 Výměnná média, která obsahují informace klasifikované jako Interní a vyšší, musí být, při přepravě mimo systém řízení bezpečnosti informací, zajištěny heslem nebo šifrováním dle Politiky klasifikace aktiv (čj. 56784/2018-SŽDC-GR-O30. Pokud nejsou informace na výměnném médiu zajištěny pomocí hesla nebo šifrování, musí být výměnné médium zajištěno pomocí fyzických opatření. Za ochranu informací na přepravovaných výměnných médiích odpovídá Uživatel, který informace na výměnné médium uložil, případně pověřená osoba zajišťující přepravu a manipulaci s výměnným médiem.
- 17.3.2 Informace přenášené v elektronické podobě musí být vždy zajištěny způsobem, který odpovídá jejich bezpečnostní klasifikaci a pravidlům pro nakládání s informacemi stanovených Politikou klasifikace aktiv (čj. 56784/2018-SŽDC-GR-O30. Veškeré informace klasifikované jako Interní a vyšší musí být při přenosu prostřednictvím e-mailu zajištěny heslem nebo šifrováním dle Politiky klasifikace aktiv (čj. 56784/2018-SŽDC-GR-O30). Za šifrování informací je odpovědný jejich odesílatel. Uživatelé nejsou oprávněni sdílet informace klasifikované jako Diskrétní a Vysoce diskrétní s cizím právním subjektem bez souhlasu jejich vlastníka.
- 17.3.3 Obdobně musí být zajištěny informace při automatizovaném přenosu mimo systém řízení bezpečnosti informací nebo musí být přenos informací realizován zabezpečeným spojem (např. VPN tunel apod.).
- 17.3.4 Podrobnosti o ochraně elektronického předávání informací jsou určeny Politikou klasifikace aktiv (čj. 56784/2018-SŽDC-GR-O30) a předpisem SŽ R10 Řád informatiky.

17.4 **Pravidla ochrany médií**

- 17.4.1 Výměnná média (USB flashdisky, externí disky, CD/DVD, pásky, diskety a další média pro ukládání dat) musí být fyzicky chráněna a zabezpečena před nepovoleným přístupem k jejich obsahu, a to zejména ta, která obsahují informace klasifikované jako Diskrétní a Vysoce diskrétní. Pravidla stanovuje Politika klasifikace aktiv (čj. 56784/2018-SŽDC-GR-O30).
- 17.4.2 Všechna výměnná média musí být ukládána na bezpečném místě, aby byla zajištěna čitelnost a předešlo se možnému fyzickému poškození, neoprávněné modifikaci informací, odcizení či ztrátě.
- 17.4.3 Běžně používaná média, např. CD/DVD média používaná k dočasnému uložení dat v rámci provozu, jsou evidována pouze v rámci zásob „prázdných“ médií.
- 17.4.4 Systematicky používaná média, např. zálohovací pásky používané k centrálnímu zálohování dat v rámci systému řízení bezpečnosti informací, musí být evidována po celou dobu svého používání, včetně vyřazení a skartace.

17.5 **Likvidace médií**

- 17.5.1 Veškerá výměnná média používaná k uložení informací musí být po skončení svého používání (např. když uložená data již nejsou potřebná) odpovídajícím způsobem skartována. Za odpovídající způsob fyzické likvidace se považuje skartace v mechanickém skartovacím zařízení.
- 17.5.2 U běžně používaných výměnných médií (CD/DVD, USB flashdisky) za spolehlivou likvidaci nebo spolehlivé smazání dat odpovídá Uživatel, který výměnné médium používal. Uživatel může likvidaci pověřit oprávněného zaměstnance, kterému výměnná média k likvidaci fyzicky předá, o čemž musí existovat písemný záznam. Způsob mazání dat stanoví Politika klasifikace aktiv (čj. 56784/2018-SŽDC-GR-O30).
- 17.5.3 U systematicky používaných médií (disky, pásky apod.) musí být o provedené likvidaci učiněn záznam v Provozním deníku.

17.6 Pravidla pro využívání kryptografické ochrany

Volbu vhodného šifrovacího mechanismu a způsoby jeho použití upřesňuje Politika použití kryptografických prostředků (čj. 56789/2018-SŽDC-GŘ-O30), ve znění jejích revizí či dokumentů tuto politiku nahrazujících.

18 OCHRANA OSOBNÍCH ÚDAJŮ**18.1 Principy ochrany osobních údajů**

Ochrana osobních údajů je založena na principech definovaných v této kapitole.

18.2 Znalost charakteristiky a účelu zpracování osobních údajů

Pro efektivní zajištění ochrany osobních údajů je důležitá znalost charakteristiky a účelu osobních údajů, které jsou v rámci SŽ zpracovávány.

18.3 Realizace opatření v souladu s Politikou klasifikace aktiv

Organizační a technická opatření pro ochranu osobních údajů jsou volena v souladu s Politikou klasifikace aktiv (čj. 56784/2018-SŽDC-GŘ-O30).

18.4 Charakteristika zpracovávaných osobních údajů

18.4.1 Charakteristika a účel zpracování osobních údajů, u kterých je SŽ správcem osobních údajů, je uvedena v seznamu udržovaném správcem osobních údajů SŽ a obsahuje alespoň charakteristiku zpracovávaných osobních údajů a účel zpracování. Kopie aktuálního seznamu je též k dispozici u Pověřence pro ochranu osobních údajů ustanoveného směrnicí SŽ SM097 Ochrana osobních údajů.

18.4.2 Osobní údaje zpracovávané v rámci SŽ musí být klasifikované jako Diskrétní (viz Politika klasifikace aktiv [čj. 56784/2018-SŽDC-GŘ-O30]).

18.4.3 Citlivé údaje zpracovávané v rámci SŽ musí být klasifikované jako Vysoce diskrétní (viz Politika klasifikace aktiv [čj. 56784/2018-SŽDC-GŘ-O30]).

18.4.4 Vlastník, pod kterého zpracování osobních údajů spadá, je oprávněn zvýšit míru ochrany zpracování osobních údajů tím, že jemu svěřené osobní údaje bude klasifikovat jako Vysoce diskrétní, případně, v součinnosti s Pověřencem pro ochranu osobních údajů, určí jiný způsob jejich ochrany.

18.5 Popis přijatých a provedených organizačních opatření pro ochranu osobních údajů

Organizační opatření určená pro ochranu osobních údajů jsou určena směrnicí SŽ SM097 Ochrana osobních údajů a Politikou klasifikace aktiv (čj. 56784/2018-SŽDC-GŘ-O30)

18.6 Popis přijatých a provedených technických opatření pro ochranu osobních údajů

Technická opatření určená pro ochranu osobních údajů jsou určena směrnicí SŽ SM097 Ochrana osobních údajů a Politikou klasifikace aktiv (čj. 56784/2018-SŽDC-GŘ-O30).

19 ZÁVEREČNÁ USTANOVENÍ

19.1 SŽ čj. 509/2025-SŽ-SŽT-NKB Provozní politika prvků v působnosti systému řízení bezpečnosti informací nahrazuje vnitřní předpis Provozní politika prvků v působnosti systému řízení bezpečnosti informací čj. 56805/2018-SŽDC-GŘ-O30.

19.2 Manažer kybernetické bezpečnosti je oprávněn měnit přílohy předpisu ve věci formy a obsahu. Toto provádí ve spolupráci s gestorem daného předpisu a ve spolupráci s O25. Veškeré změny příloh musí reflektovat pravidla vnitřního předpisu SŽ N1. Tvorba a vydávání vnitřních předpisů a služebních rukověť státní organizace Správa železnic.

- 19.3 Tento předpis nabývá účinnosti zveřejněním v elektronické knihovně dokumentů a předpisů SŽ (eDAP).
- 19.4 Účinnost předpisu Provozní politika prvků v působnosti systému řízení bezpečnosti informací (čj. 509/2025-SŽ-SŽT-NKB) je stanovena ode dne zveřejnění v eDAP do 31. prosince 2025.

SOUVISEJÍCÍ DOKUMENTY

Mezinárodní a národní právní předpisy, technické normy, ve znění pozdějších předpisů

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů

Zákon č. 111/2009 Sb., o základních registrech

Vnitřní předpisy, v aktuálním znění

SŽ čj. 2462/2024-SŽ-SŽT-NKB Politika systému řízení bezpečnosti informací

SŽDC PO-22/2018-GŘ Pokyn GŘ Rámcová dohoda o ochraně důvěrných informací

Politika organizační bezpečnosti, čj. 2811/2023-SŽ-SŽT-NKB

Politika klasifikace aktiv, čj. 56784/2018-SŽDC-GŘ-030

Politika použití kryptografických prostředků, čj. 56789/2018-SŽDC-GŘ-O30

Směrnice SŽDC č. 54 k pořízení IS/IT a provozu jednotné evidence HW, SW a SW licencí programem AW Caesar

SŽ SM074 Směrnice zvládání kybernetických bezpečnostních incidentů v informačním systému státní organizace Správa železnic

SŽ SM094 Směrnice ve věci systému řízení kontinuity procesů ve státní organizaci Správa železnic

SŽ SM097 Ochrana osobních údajů

SŽ R10 Řád Informatiky

SŽ R2 Spisový řád státní organizace Správa železnic

SŽ N1 Tvorba a vydávání vnitřních předpisů a služebních rukověť státní organizace Správa železnic

Příloha A (normativní)**Krycí list aktiva**

Primární aktivum					
Klasifikace primárního aktiva		Důvěrnost: Dostupnost: Integrita:			
Způsob řešení požadavků Provozní politiky prvků v působnosti systému řízení bezpečnosti informací					
	Požadavek aplikovatelný (ANO / NE / ČÁSTEČNĚ) ⁴	Splněno (ANO / NE / ČÁSTEČNĚ) ⁵	Důvod nezavedení ⁶	Výjimka ⁷ (č., stav, datum evidence a schválení Manažerem kybernetické bezpečnosti)	Odkazy na dokumentaci
Řízení provozu					
Bezpečnost komunikací					
Řízení přístupu					
Řízení technických zranitelností					
Zálohování a obnova					
Ochrana před škodlivým kódem					
Logování a monitoring					
Řízení změn					
Akvizice, vývoj a údržba					
SW Licence					
ServiceDesk					
Bezpečné předávání a výměna informací					
Ochrana osobních údajů					

4 V případě, že je uvedeno ČÁSTEČNĚ, popište, pro které konkrétní oblasti jsou požadavky v kontextu daného primárního aktiva plněny, a pro které nikoliv.

5 V případě, že je uvedeno ČÁSTEČNĚ, popište, jak je řešeno.

6 Uvedte zdůvodnění, proč daný požadavek není u primárního aktiva plněn.

7 V případě, že je ve sloupci „Splněno“ uvedeno ČÁSTEČNĚ, nebo není některý z požadavků u primárního aktiva plněn, doplňte informace o výjimce, která se k danému případu vztahuje.

Příloha B (normativní)**Vzor Zprávy z přezkoumání přístupových oprávnění**

čj.
klasifikace
důvěrnosti Interní
informací

..(Název IS).. –

provedeno podle stavu ke dni

Předmětem prověření bylo:	Nález/zjištění
a) přehled Uživatelů s přístupem do IS	
b) přehled přidělených úrovní přístupových oprávnění Uživatelů s přístupem do IS	
c) zda existující testovací účty nejsou zakládány jako sdílené a zda jsou přiřazovány výhradně konkrétním Uživatelům IS	
d) zda jsou aktivní testovací účty nadále potřebné (viz c)	
e) zda je zakázáno přihlášení prostřednictvím jména a hesla pro ty Uživatele IS, kteří mají účet v Active Directory (je-li používáno pro autentizaci do daného IS)	
f) zda Uživatelé byli poučeni o povinnosti použití silných hesel (obdobné platí i v případě testovacích a technologických účtů)	
g) zda jsou role zavedené v IS nadále potřeba k jeho provozu a užívání	
h) zda není možné danou roli sloučit s jinou a snížit tak počet rolí s cílem efektivnějšího řízení přístupových oprávnění	

Zpracoval

YYY

Gestor informačního systému

V Praze dne

Garant informačního systému

V Praze dne

Schválil

YYY

B.2 Přehled Uživatelů, úrovně oprávnění a přidělených rolí

status	číslo Uživatele	uživatelské jméno	jméno	příjmení	testovací účet	dodavatel	útvár SŽ	název modulu	licence plnohodnotná / omezená	název pozice 1	název pozice 2	název pozice 3	název role 1	název role 2	název role 3

LEGENDA



**testovací
účet**

zrušení Uživatelé – bez přístupu do IS.

V případě, že se jedná o testovací účet, označte (x).

Dodavatel

V případě, že se jedná o účet Dodavatele, označte (x).