MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

NAKIT
Národní agentura pro komunikační a informační technologie, s. p.

Bezpečnostní postupy

Radiokomunikační systém PEGAS

verze 06.2020 (č. j. MV-81020-2/SIK5-2020)

účinnost od 1. září 2020

Obsah

1 Úvod

1.1 Účel dokumentu

Účelem dokumentu je stanovit v radiokomunikačním systému PEGAS (dále také jen „systém“) základní bezpečnostní procesy k zajištění bezpečnosti přenášených informací a přístupu k nim. Dokument stanoví závazná pravidla pro koncové uživatele a operátory systému, který byl určen prvkem kritické informační infrastruktury na základě zákona č. 181/2014 Sb., o kybernetické bezpečnosti, v platném znění, a postupem podle nařízení vlády ČR č. 315/2014 Sb., o kritériích pro určení prvku kritické infrastruktury.

Dokument je členěn do následujících částí:

Úvod: obsahuje všeobecné informace včetně významu zkratek a základních pojmů používaných v dokumentu.

Bezpečnostní zásady: stanoví závazná pravidla pro manipulaci s koncovým zařízením (dále jen „terminál“ nebo „TR“) a pro řízení přístupů do systému.

Provoz: uvádí příklady provozní a referenční dokumentace.

Ostatní: popisuje pravidla k programování TR, pravidla pro zálohování dat generovaných systémem atd.

Formuláře: obsahuje obrazové přílohy dokumentu.

1.2 Určení dokumentu

Tento dokument je určen všem osobám, které pracují se systémem, především:

- uživatelům,
- operátorům dohledu,
- školitelům,
- pracovníkům odpovědným za provoz a servis,
- vedoucím pracovníkům.

1.3 Zkratky a pojmy

Administrátor KMC	pracovník NAKIT ORS, určený ke správě klíčového hospodářství systému PEGAS
AIF	**Anomaly Improvement Form** (formulář hlášení závady nebo změny)
ANOCOD	**ANOmaly CODe** (chybový kód, kód anomálie)
AVL	**Automated Vehicle Localisation** (automatická lokalizace vozidel)
BS	**Base Station** (základnová radiostanice)
CAM Card	přístupové karty k zařízení KMC
CA SD	**CA Service Desk** (helpdesk systému)
CC-API, CC-IS	rozhraní pro linkově a rádiově připojené terminály dispečerů, rozhraní pro databázový server
CETIN	CETIN a.s., Česká telekomunikační infrastruktura
ČTÚ	Český telekomunikační úřad
DIR	**DIRect mode** (režim přímého provozu terminálů mimo síť)
DMK	**Direct Mode Key** (klíč pro režim přímého provozu terminálů)
EPC	nástroj pro získávání údajů ze systému
GŘC	Generální ředitelství cel
HZS ČR	Hasičský záchranný sbor České republiky
HZSp	Hasičský záchranný sbor podniku
CHIF	**Ciphering board** (šifrová deska v hlavní rádiové ústředně)
IAŘ MV ČR	interní akt řízení Ministerstva vnitra ČR
IDR	**Independent Digital Repeater** (nezávislý digitální opakovač)
JSDHo	jednotka sboru dobrovolných hasičů obce
JSDHp	jednotka sboru dobrovolných hasičů podniku
Klíčové proměnné	šifrovací algoritmus k zabezpečení přenosu informací

KLU	**Key Loader Unit** (zařízení pro zavádění klíčových proměnných)
KMC	**Key Management Center** (středisko klíčového hospodářství)
Kryptoperioda	časové období platnosti klíčových proměnných
LAG	**Line Access Gateway** (brána linkového přístupu)
LCT	**Line Connected Terminal** (linkově připojený terminál)
MD	**Mediation Device** (provozní a databázový server)
Medium	**Flash Disk, HDD, CD RW** (datové nosiče – přenosný flash disk, hard disk, přepisovatelné CD)
MěP	městská policie
MSW	**Main Switch** (hlavní rádiová ústředna)
MV	Ministerstvo vnitra České republiky (vlastník systému)
NAKIT	Národní agentura pro komunikační a informační technologie, s. p. (provozovatel systému)
NAKIT ORS	Národní agentura pro komunikační a informační technologie, oddělení Radiokomunikační sítě
Národní síť	celostátní struktura systému tvořená jednotlivými regionálními sítěmi
NDP	Národní dohled PEGAS
OIKT KŘ PČR	odbor informačních a komunikačních technologií Krajského ředitelství Policie České republiky
OMC	**Operation and Maintenance Computer** (řídící a dohledový počítač)
Oprávněná osoba	odborný pracovník uživatele určený ke komunikaci s NDP, pracovištěm TWP, pracovištěm TPS, vlastníkem systému a provozovatelem systému (oprávněnými osobami uživatelů z HZSp, JSDHo a JSDHp jsou oprávněné osoby HZS kraje)
OS	operační středisko nebo obdobné pracoviště uživatele, např. dispečink (operačními středisky uživatelů z HZSp, JSDHo a JSDHp jsou krajská operační a informační střediska HZS krajů)
PČR	Policie České republiky
PK	**Personalization Key** (základní klíč systému)

PMC	Pramacom Prague, spol. s r. o. (servisní organizace)
PP ČR	Policejní prezidium České republiky
RCT	**Radio Connected Terminal** (rádiově připojený terminál)
RCD	RCD Radiokomunikace, a.s.
RFSI	**Regional Fleet Subfleet Identity** (číselná adresa koncového zařízení)
RSW	**Radio Switch** (rádiová ústředna)
SIR	**Site Intervention Report** (hlášení zásahu na stanovišti)
Servisní organizace	subjekt provádějící servis systému PEGAS
Systém	radiokomunikační systém PEGAS
TMK	**Terminal Master Key** (hlavní terminálový klíč)
TMP	**Tactical Management Position** (zařízení pro taktické řízení infrastruktury)
TPS	**Terminal Programming Station** (zařízení pro konfiguraci koncových zařízení)
TR	terminál (koncové zařízení systému PEGAS)
TS	třídy služeb (definice oprávnění terminálu)
TWP	**Tactical Working Position** (zařízení pro taktické řízení uživatelů, komunikací atd.)
VPW	brána vozidlového opakovače
XIP	konvertor X25/IP
ZS MV	Zařízení služeb pro Ministerstvo vnitra
ZZS	Zdravotnická záchranná služba

1.4 Základní úkony

1.4.1 Programování koncových zařízení

Koncová zařízení (terminály), zařízení VPW (brána vozidlového opakovače) a IDR (nezávislé opakovače) jsou programovány prostřednictvím zařízení TPS.

Programování TR je rozděleno do tří kroků:

1) zavedení základního software,
2) nastavení a zavedení konfiguračních parametrů,
3) zavedení definovaných oprávnění.

1.4.2 Zavedení TR do systému

Soubor s údaji o TR, který je vygenerován zařízením TPS, předá obsluha TPS operátorovi TWP. Forma předání datového souboru je řešena v části 4.1.6. Operátor TWP prostřednictvím tohoto souboru zavede/vymaže TR do/ze systému a provede jeho de/aktivaci.

TR při zavedení do systému musí vždy obsahovat:

- základní software,
- klíčové proměnné (slouží k de/šifrování hlasových služeb),
- RFSI (jedinečné číslo TR, které slouží k jeho identifikaci v síti),
- oprávnění "TS" (např. právo vstupu do DIR, IDR, do telefonní sítě atd.).

TR musí být v zařízení TWP definován pomocí adresy RFSI, která je shodná s RFSI zadávaným při konfiguraci v zařízení TPS.

1.4.3 Kryptoperioda klíčových proměnných

Klíčové proměnné slouží k de/šifrování hlasových služeb a k autentizaci TR v systému. Platnost kryptoperiody základních klíčových proměnných, které jsou při programování zavedeny do TR, je:

a) stanovena administrátorem KMC pro:

- klíč TMK (určený pro autentizaci TR),
- klíč DMK (určený pro přímý režim),
- klíč PK (základní klíč – jedinečný),
- klíče NNK, ONNK (komunikační klíčové proměnné národní),
- ostatní klíčové proměnné (INK, MMK, atd.),
- klíče modifikátorů (určené pro přešifrování klíčových proměnných),
- přičemž doba platnosti není pevně stanovena,
- nepovinné klíčové proměnné;

b) stanovena systémově pro:

- klíč TKK, OAKorg (určené pro autentizaci), RNK a ORNK (komunikační klíčové proměnné regionální).

1.4.4 Prvky tvořící systém a jejich členění

a)	infrastruktura	rádiová ústředna (RSW), základnová radiostanice (BS), opakovač signálu, nezávislý digitální opakovač (IDR),
b)	terminály	mobilní (ruční, vozidlové) a pevné (dispečerská zařízení RCT a LCT),
c)	provozní zařízení	pracoviště technického dohledu (TMP), pracoviště taktického řízení (TWP), pracoviště pro programování TR (TPS), středisko klíčového hospodářství (KMC + KLU), provozní server MD, pracoviště NDP (TMP/ TWP),
d)	rozhraní	brána linkového přístupu (LAG), rozhraní linkově připojeného TR – CC-API, Gatepro, Vehicular rePeater gateWay (VPW), rozhraní pro přístup k databázovému serveru – CC-IS, rozhraní XIP (X25/IP), rozhraní TETRA – TETRAPOL, rozhraní PABX,
e)	doplňkové systémy	automatická lokalizace vozidel (AVL), záznamové zařízení, datový portál,
f)	zařízení údržby	stanice pro konfiguraci zařízení (ECS), stanice pro testování TR.

2 Bezpečnostní zásady pro základní úkony

K zajištění bezpečnosti šifrovaného provozu a znemožnění vstupu neoprávněných osob do šifrovaných komunikací **musí obsluhy provozovaných zařízení, dodavatelé a uživatelé** dodržovat stanovené bezpečnostní zásady, jejichž cílem je chránit klíčové proměnné a znemožnit tak neoprávněný odposlech komunikací. Bezpečnostní zásady jsou zahrnuty do bezpečnostních postupů užívaných v základních pracovních úkonech při:

- záznamu dat z TR,
- ztrátě nebo krádeži TR,
- zničení nebo poškození TR,
- předávání TR do opravy servisní organizaci,
- instalaci TR do vozidel civilní firmou,
- periodické výměně TMK klíčů,
- programování TR zavedeného do systému v jiné regionální síti,

- vyřazení TR z majetkové evidence uživatele a jeho likvidace,
- vyřazení TR z majetkové evidence uživatele a jeho převedení na jiného uživatele,
- vývozu a použití TR mimo území ČR,
- přístupu k provozním zařízením, prvkům infrastruktury a rozhraní CC-IS,
- zálohování dat, uložení dat,
- výdeji dat,
- zveřejňování informací o provozních údajích neveřejné radiotelefonní sítě,
- používání komunikačních prostředků,
- procesech umístění technologií jiných subjektů.

2.1 Záznam dat z TR

V případě nutnosti analyzovat nekorektní stav nebo chování TR je možné poskytnout servisní organizaci obsah paměti RAM z TR. Vzhledem k tomu, že v paměti RAM jsou mimo jiné uchovávány klíčové proměnné, je nutné při provádění záznamu těchto dat dodržovat následující pracovní postup:

- o požadavku servisní organizace na záznam dat paměti RAM z TR informuje obsluha TPS administrátora KMC[1a], v případě jeho nedosažitelnosti operátora NDP[1b],
- záznam dat paměti RAM z TR provádí pracovník servisní organizace pomocí vlastního speciálního programu za přítomnosti obsluhy TPS,
- pracovník servisu zkopíruje uvedená data na médium operátora TPS, do adresáře pojmenovaného RFSI_DDMMRR[2],
- obsluha TPS zkopíruje data z média do TPS, do adresáře s názvem „RAM“ vytvořeného v PC (TPS) na pracovní ploše a zároveň je zálohuje na externí úložiště,
- operátor TPS okamžitě po záznamu dat zajistí přeprogramování příslušného TR (obměnu klíčových proměnných) nebo jeho vymazání ze systému,
- o tomto zásahu provede obsluha TPS zápis do formuláře „Záznam dat RAM“[3],
- záznam dat paměti RAM z TR je prováděn na pracovišti TPS příslušné regionální sítě, ve které je TR zaveden do systému.

1a Administrátor KMC – pracovník NAKIT ORS
1b Národní dohled PEGAS - 974 841 969, fax: 974 841 387, e-mail: ndpegas@pramacom.cz
2 Příklad: 101120125_251216
3 Vzor formuláře je uveden v příloze č. 1

2.2 Ztráta nebo krádež TR

Ztráta nebo krádež TR je incident s vysokým rizikem zneužití TR nepovolanou osobou. **Z tohoto důvodu je nezbytná součinnost oprávněné osoby nebo OS s operátorem TWP příslušné regionální sítě systému nebo v mimopracovní době s NDP** a striktní dodržování následujícího postupu:

- Oprávněná osoba nebo OS bezodkladně písemně (faxem, e-mailem …) nahlásí ztrátu či krádež TR nebo podezření ze ztráty či krádeže operátorovi TWP regionální sítě systému, případně operátorovi NDP. V případě nebezpečí z prodlení lze událost nahlásit telefonicky s podmínkou, že písemné potvrzení bude zasláno následně v nejkratším možném termínu. V takovém případě operátor zpětně telefonicky ověří požadavek. *Operátor nenese odpovědnost za případný chybný zákrok způsobený nepřesnými nebo mylnými vstupními údaji.*

- Operátor TWP příslušné regionální sítě, případně operátor NDP, okamžitě odebere TR jeho provozní práva[4]. Výpis z TWP o zadání příkazu operátor TWP vytiskne a uloží.

- Poté, co operátor TWP obdrží informaci o tom, že TR byla odebrána provozní práva (TWP ANOCOD 10012) a má písemné potvrzení od oprávněné osoby nebo OS potvrzující telefonické nahlášení ztráty či krádeže, operátor TWP bezodkladně zadá příkaz k odebrání přístupových práv TR do systému[5]. Výpis z TWP o zadání příkazu vytiskne a uloží.

- Poté, co operátor TWP obdrží informaci o tom, že TR byla odebrána přístupová práva (TWP ANOCOD 10017), informuje obsluhu TPS, která provede ruční výmaz TR z databáze TPS, vygeneruje soubor pro smazání TR a předá jej operátorovi TWP. Operátor TWP prostřednictvím souboru dodaného obsluhou TPS vymaže TR ze systému[6]. Výpis z TWP o provedení vymazání TR vytiskne a uloží.

- Obsluha TPS o provedeném úkonu učiní záznam do deníku TPS a operátor TWP do formuláře pro evidenci ztracených TR[7]. Operátor TWP regionální sítě je povinen informovat o ztrátě operátora NDP nebo administrátora KMC, kteří provedou záznam do databáze ztracených a odcizených TR vedených v CA SD.
- Operátor TWP regionální sítě zašle podklady o ztrátě na NDP, který je předá administrátorovi KMC k dalšímu zpracování.

Po vymazání TR ze systému podle výše popsaného postupu lze RFSI vymazaného TR použít při programování jiného TR.

4 TWP / list Subscriber / záložka Characteristics / Traffic operated - nezaškrtnuté pole
5 TWP / list Subscriber / záložka Characteristics / Access enabling - nezaškrtnuté pole
6 TWP / list Subscriber / záložka Identification / Deasign
7 Formulář uvedený v příloze č. 8

Od doby odebrání provozních či přístupových práv je operátor povinen kontrolovat minimálně 4x denně (v pravidelných šestihodinových cyklech) informace o doručení provedení příkazu po dobu 3 dnů, poté min. 1x denně. V případě, že se nejedná o 24 hod. dohled systému dané regionální sítě, je obsluha povinna přizpůsobit kontrolu tak, aby bylo zajištěno sledování výše uvedených informací o doručení příkazu minimálně 2x v průběhu pracovní směny po dobu 3 dnů, poté min. 1x denně.

V případě nahlášení ztráty TR mimo pracovní dobu nebo ve dnech pracovního klidu je operátor NDP povinen kontrolovat síť, ze které ztracený TR pochází z hlediska doručení provedení příkazu minimálně 4x denně od zadání příkazu. V následující pracovní den (po dni pracovního klidu) předá informace o ztrátě obsluze TWP příslušné regionální sítě.

Operátor TWP, který zadal příkaz pro zablokování TR, informuje v nejbližším možném termínu obsluhu TPS o ztrátě nebo nálezu TR (a opačně). Není přípustné, aby číslo RFSI konkrétního TR se zakázanými provozními či přístupovými právy bylo použito pro jiný TR.

Upozornění:

Posloupnost jednotlivých kroků je nutno bezpodmínečně dodržovat! ***TR manuálně vymazaný ze systému bez předchozího odebrání provozních a přístupových práv je pro systém nedostupný, ale zůstává funkční v režimu DIR a IDR****. V takovém případě pak operátor není schopen systémovými prostředky zabránit zneužití TR.*

Pokud je TR nalezen, oprávněná osoba nebo OS má povinnost neprodleně o tom písemně informovat operátora TWP příslušné regionální sítě systému, popř. operátora NDP.

Operátor TWP pak provede potřebné kroky k zajištění funkčnosti TR v systému.

O ztracených a odcizených TR vede regionální operátor TWP následující dokumentaci:

- regionální evidenci ztracených a odcizených TR[8]**,**
- písemné nahlášení ztráty TR,
- písemné nahlášení nálezu TR,
- výpisy z TWP o jednotlivých provedených krocích.

O ztracených a odcizených TR vede regionální obsluha TPS následující dokumentaci:

- záznam v provozním deníku o ručním vymazání TR ze systému na základě hlášení operátora TWP,
- evidenci ztracených a odcizených TR[8].

Administrátor KMC vede centrální evidenci ztracených a odcizených TR v písemné a elektronické podobě. Operátor TWP, případně operátor NDP, je povinen mu zasílat všechny podklady k její aktualizaci.

8 Formulář uvedený v příloze č. 2

2.3 Zničení nebo poškození TR

V případech, kdy dojde ke zničení či poškození TR, je možné ho vymazat ze systému za následujících podmínek:

- Zničený TR nebo jeho zbylé části doručí oprávněná osoba spolu s průvodní zprávou, ve které bude uveden stručný popis události, při níž došlo k poškození TR obsluze TPS v regionální síti, ve které je TR zaveden.
- Obsluha TPS k TR nebo jeho zbylým částem připojí zprávu obsahující tyto informace: RFSI, logické a výrobní číslo a datum posledního zavedení TR do systému. Dále zajistí technické posouzení TR na odborném pracovišti servisní organizace nebo příslušném OIKT KŘ PČR.
- Odborné pracoviště provede posouzení technického stavu TR a závěry uvede v servisní zprávě[9]. TR spolu se servisní zprávou zašle zpět oprávněné osobě cestou obsluhy TPS.
- Na základě odborného posouzení obsluha TPS ve spolupráci s operátorem TWP zajistí vymazání TR ze systému (ruční výmaz TR na TPS, vygenerování souboru o výmazu na TPS, vymazání TR ze systému pomocí vygenerovaného souboru z TPS na TWP). **Uvolněné RFSI může být dále použito pro naprogramování jiného TR.**
- Obsluha TPS vede evidenci zničených TR[10]. Součástí této evidence je kopie odborného posouzení a průvodní zpráva.

Pokud odborné pracoviště posoudí TR jako opravitelný, zajistí obsluha TPS jeho depersonalizaci a odborné pracoviště jeho opravu (viz část 2.4).

Případy, kdy není možné zaslat k posouzení ani části TR (požár, utopení TR ve vodě, atd.), je nutné řešit individuálně s pracovníky kryptografie systému z NAKIT ORS, kteří doporučí další postup vedoucí k uvolnění RFSI konkrétního TR ze systému.

2.4 Předávání TR do opravy a do civilního sektoru

Z bezpečnostních důvodů je možné do opravy předávat pouze depersonalizované TR, není-li dále stanoveno jinak.

2.4.1 Depersonalizovatelné TR

- Oprávněná osoba předá TR obsluze TPS.
- Obsluha TPS zajistí jeho depersonalizaci a o zásahu udělá záznam do protokolu o depersonalizaci TR[11].

9 Formulář uvedený v příloze č. 7
10 Formulář uvedený v příloze č. 3
11 Formulář uvedený v příloze č. 6

- Součástí protokolu o depersonalizaci jsou následující informace: RFSI, logické číslo, výrobní číslo TR, datum depersonalizace, jméno obsluhy TPS, která depersonalizaci provedla, popis chyby TR. V případě, že se jedná o více TR předávaných do opravy, je možné provést zjednodušený protokol o depersonalizaci, který bude obsahovat více TR na jednom formuláři, ve kterém budou obsaženy všechny výše uvedené informace.

2.4.2 Nedepersonalizovatelné TR

V případech, kdy nelze provést depersonalizaci TR, postupují obsluha TPS a oprávněná osoba následovně:

- Oprávněná osoba předá TR regionální obsluze TPS.
- V případě, kdy TR nelze depersonalizovat, obsluha TPS vypracuje protokol[12]. Součástí protokolu jsou následující informace: RFSI, logické číslo, výrobní číslo TR, datum, jméno obsluhy TPS, která se pokusila provést depersonalizaci, popis chyby TR, informaci o manuálním resetu TR z TPS a ze systému.

  Obsluha TPS provede manuální reset TR v zařízení TPS a ve spolupráci s operátorem TWP zajistí vymazání TR ze systému – **vymazání terminálu je možné výhradně prostřednictvím souboru vygenerovaného z TPS.**

Poznámka:

Pokud je terminál funkční, tj. registruje se do systému, ale nelze jej na zařízení TPS načíst, odebere operátor TWP na pokyn obsluhy TPS terminálu přístupová práva do systému (příkaz ACCESS). Dále postupuje jako u nedepersonalizovaného TR. Obsluha TPS do provozního deníku zapíše u TR – R (reset), ACCESS. Operátor TWP do provozního deníku zaznamená odebrání přístupových práv s uvedením RFSI a důvodů (nelze načíst na TPS).

2.4.3 Předání TR servisní organizaci

TR uživatelů rezortu MV (včetně PČR a HZS ČR):

Obsluha TPS předá TR spolu s kopií protokolu o ne/depersonalizaci TR oprávněné osobě, která zajišťuje jeho předání včetně protokolu servisní organizaci na opravu.

TR externích uživatelů (HZSp, JSDHo, JSDHp):

Obsluha TPS předá TR spolu s kopií protokolu o ne/depersonalizaci TR oprávněné osobě HZS ČR. Ta následně TR předá uživateli, který zajistí vlastními silami jeho předání včetně protokolu servisní organizaci na opravu.

TR externích uživatelů (ZZS, GŘC, MěP, atd.):

Obsluha TPS předá TR spolu s kopií protokolu o ne/depersonalizaci TR oprávněné osobě, která zajistí vlastními silami jeho předání včetně protokolu servisní organizaci na opravu.

12 Formulář uvedený v příloze č. 5

Servisní organizace převezme do opravy TR již někdy do systému zavedený **pouze** v případě, že je spolu s ním předán protokol o jeho ne/depersonalizaci.

Obsluhy TPS a servisní organizace mají za povinnost archivovat protokoly o ne/depersonalizaci TR minimálně 2 roky od data ne/depersonalizace TR.

Povinnosti servisní organizace:

- Vede evidenci nedepersonalizovaných TR.
- Nepřijme do opravy TR bez protokolu o ne/depersonalizovaném TR.

Po opravě zkontroluje TR, zda nezůstal naprogramovaný na původní číslo RFSI (u nedepersonalizovaných TR). V případech, kdy číslo RFSI v TR zůstalo naprogramované, zajistí jeho vymazání před předáním oprávněné osobě.

- **Zajistí, aby TR byl vrácen uživateli vždy s aktuální SW verzí.**

Poznámka:

Postup podle bodu 2.4.3 se neuplatní při případné opravě TR dosud nikdy nezavedeného do systému.

2.4.4 Předání vozidla s TR systému do civilního sektoru

Z bezpečnostních důvodů je zakázáno předat vozidlo do civilního sektoru (např. do autoservisu, k úpravci vozidla apod.) s funkčním TR. Z tohoto důvodu je nezbytné provést následující opatření:

a) Oprávněná osoba vyjme TR z vozidla a uloží ho do k tomu určených prostor po dobu opravy vozidla. Po převzetí vozidla z opravy vloží TR zpět do vozidla, otestuje jeho základní funkce a předá ho k užívání.

Nelze-li TR z vozidla vyjmout, lze postupovat podle následujících bodů:

b) Oprávněná osoba písemně zašle e-mailem na NDP (nebo regionální pracoviště systému) požadavek na DISABLE TR z důvodu předání vozidla do civilního sektoru. Požadavek musí obsahovat RFSI TR, jež má být zablokován, a kontaktní údaje na pracovníka, který požadavek zadal (z důvodů prodlení lze požadavek sdělit telefonicky s tím, že bude neprodleně písemně potvrzen).

c) Obsluha NDP (nebo regionálního pracoviště systému) zadá TR příkaz DISABLE (pokud je TR v zapnutém stavu nebo při jeho následném zapnutí se na displeji TR zobrazí hlášení „problém 01“).

d) Po vrácení vozidla z civilního sektoru oprávněná osoba písemně zašle e-mailem na NDP (nebo regionální pracoviště systému) požadavek na ENABLE TR. Požadavek musí obsahovat RFSI TR, jež má být odblokován, a kontaktní údaje na pracovníka, který požadavek zadal (z důvodu prodlení lze požadavek sdělit telefonicky s tím, že bude neprodleně písemně potvrzen).

e) Obsluha NDP (nebo regionálního pracoviště systému) zadá TR příkaz ENABLE (pokud je TR v době provedení příkazu v zapnutém stavu, je nutné jej následně vypnout a opětovně zapnout).

Obsluha NDP (nebo regionálního pracoviště systému) vede elektronickou evidenci TR, kterým byl dán příkaz DISABLE a ENABLE. Tato evidence je součástí provozního deníku pracoviště.

Oprávněná osoba v případě požadavku na opětovné uvedení TR do provozu kontaktuje to pracoviště operátora, které příkaz na zablokování zadalo. Pokud nebude dané pracoviště k dispozici, může kontaktovat obsluhu pracoviště, které příkaz nezadalo s tím, že v požadavku bude uvedeno, které pracoviště TR zablokovalo. Obsluha NDP (nebo regionální pracoviště systému) jsou povinni si tuto informaci mezi sebou předat a zaznamenat v evidenci TR, kým byl zadán příkaz DISABLE nebo ENABLE.

2.4.5 Instalace funkčního TR systému do vozidel civilní firmou

V případě, že instalaci funkčního TR do vozidla zajišťuje civilní firma, postupuje se podle bodů 2.4.4 b) až e).

2.5 Periodická výměna TMK klíčů

Správu střediska klíčového hospodářství (KMC) zajišťuje NAKIT ORS zabezpečující provoz systému. Citlivé informace (klíčové proměnné) jsou uložené v CHIF desce a v HD zařízení MSW v každé regionální síti. Tyto prvky jsou opatřeny bezpečnostní plombou s hologramem proti neoprávněným zásahům. Distribuci a tvorbu klíčových proměnných zajišťuje administrátor zařízení KMC.

V dostatečném časovém předstihu (cca 2 – 4 měsíce podle velikosti regionální sítě) **před uplynutím kryptoperiody TMK klíčů,** která je stanovena na 4 roky, vytvoří administrátor KMC nové klíčové proměnné. Pomocí zařízení KLU zavede klíčové proměnné do systému (MSW) v dané regionální síti a vytvoří sadu klíčových proměnných pro obnovu a programování koncových zařízení, které předá regionální obsluze TPS. Informace o změně klíčových proměnných předá na OPITK MV, který zajistí informovanost uživatelů o termínech změny klíčových proměnných v jednotlivých regionálních sítích.

Obsluha TPS na základě končící kryptoperiody klíčových proměnných (po vygenerování nové sady klíčových proměnných) informuje oprávněné osoby o nutnosti změny klíčových proměnných a zorganizuje jejich výměnu v TR ve spolupráci s oprávněnými osobami a s operátorem TWP. Organizuje a řídí proces výměny klíčových proměnných tak, aby v daném termínu byly TR změněny klíčové proměnné. Oprávněné osoby upozorní, že 14 kalendářních dní před ukončením stanovené kryptoperiody budou všem TR se starými klíčovými proměnnými odebrána provozní práva.

Po uplynutí kryptoperiody TMK klíče je TR systémově nedostupný, ale stále zůstává funkční v režimu DIR a IDR. Proto musí být minimálně 14 dní před stanoveným koncem kryptoperiody přeprogramovány všechny TR zavedené v regionální síti bez ohledu na to, ve kterém časovém úseku uplynulých let byly programovány.

K vyloučení nekontrolovatelného používání TR mimo systém musí obsluha TPS při změně klíčových proměnných TR dodržovat následující pracovní postup:

- Před zahájením změny klíčových proměnných vypracuje seznam TR zavedených v regionální síti a porovná jej s databází zařízení TWP. Oba seznamy musí být shodné. V případě zjištění rozdílů mezi databázemi je nutné zjistit příčinu rozdílů a uvést databáze do souladu.
- 21 kalendářních dní před stanoveným koncem kryptoperiody provede kontrolu počtu přeprogramovaných TR a vypracuje seznam těch TR, kterým nebyly zavedeny nové TMK klíče. Oprávněné osoby pro TR z tohoto seznamu upozorní, že všem TR se starými klíčovými proměnnými budou za 7 dní odebrána provozní práva.
- 14 kalendářních dní před koncem kryptoperiody TMK klíčů předá operátorovi TWP seznam TR se starými klíčovými proměnnými a operátor TWP jim odebere provozní práva[4].
- Po ukončení změny klíčových proměnných ve své regionální síti zašle administrátorovi KMC seznam TR, u nichž žádal odebrání provozních práv.
- Obsluha TPS při změně klíčových proměnných zapisuje změny do provozního deníku TPS[13] nebo do elektronického provozního deníku.
- Média s klíčovými proměnnými, pokud s nimi operátor TPS nepracuje, jsou uchovávána v trezoru nebo umístěna tak, aby k nim neměly přístup neoprávněné osoby.

Přístup k zařízení TPS a klíčovým proměnným je povolen pouze osobám, které mají činnost s nimi uvedenou v náplni práce a byly pro obsluhu zařízení TPS vyškoleny.

Bez souhlasu administrátora KMC je zakázáno kopírovat či jinak upravovat klíčové proměnné.

S počátkem nové kryptoperiody klíčových proměnných administrátor KMC rozhodne o postupu zničení neplatných klíčových proměnných eventuálně o zničení médií. Obsluha TPS postupuje dle pokynů administrátora KMC.

13 Formulář uvedený v příloze č. 4

2.6 Programování TR zavedeného do systému v jiné regionální síti

Každý TR zavedený v systému obsahuje mimo jiné:

- Vlastní jedinečné identifikační číslo (RFSI), které na pozici R nese znak regionální sítě, v níž je TR do systému zaveden.
- Výrobcem přidělené jedinečné číslo logické desky. Tato čísla slouží k identifikaci a autentizaci TR v systému a jejich nesoulad systém vyhodnocuje jako incident (systém generuje alarmová hlášení, neumožní TR provoz v systému nebo jeho části).

Z těchto důvodů jsou pro operátory TPS, TWP a pro uživatele závazná následující bezpečnostní opatření:

- Pokud taktické nebo organizační důvody vyžadují zavedení TR v jiné regionální síti, než ve které byl doposud zaveden, pak uživatel nejdříve zajistí jeho depersonalizaci ve stávající regionální síti.
- Regionální obsluha TPS nesmí vymazat nebo přeprogramovat TR naprogramovaný v jiné regionální síti.

Za mimořádných okolností je možné se souhlasem administrátora KMC zvolit jiný, individuální postup definovaný administrátorem KMC.

2.7 Vyřazení TR z majetkové evidence a jeho převedení na jiného uživatele

TR je možné vyřadit z majetkové evidence uživatele a převést na jiného uživatele pouze za předpokladu, že není zaveden v systému. V případě, že uživatel chce funkční TR ze své majetkové evidence vyřadit a převést jinému uživateli, je nutné postupovat následovně:

- depersonalizovat (vymazat) TR na pracovišti TPS postupem dle části 2.4.1 a dále jej vymazat ze systému standardním způsobem,

nebo

- pokud nelze TR depersonalizovat (vymazat) je nutné postupovat dle části 2.4.2 a TR předat do opravy dle části 2.4.3. V případě, že je oprava TR nerentabilní, nebude TR jinému uživateli převeden a bude se postupovat dle části 2.8,

- převést depersonalizovaný TR jinému uživateli.

2.8 Vyřazení TR z majetkové evidence a jeho likvidace

TR je možné dát k likvidaci pouze za předpokladu, že není zaveden v systému. Postup při vyřazení a likvidaci TR je následující:

- **TR typu G1, G1+, G2 a G3** depersonalizovat (vymazat) na pracovišti TPS a dále TR vymazat ze systému standardním způsobem. Pokud nelze TR takto depersonalizovat (vymazat), je nutné zabezpečit TR před zneužitím. Pokud TR lze zapnout, ale nejde načíst na TPS, obsluha TPS ve spolupráci s obsluhou TWP provede na TR příkaz ACCESS, o čemž se přesvědčí na TR, a následně provede vymazání ze systému pomocí ručního výmazu v databázi TPS a přes vygenerovaný soubor na TWP. Obsluha TPS zaznamená informaci o nemožnosti vymazání nebo o použití příkazu ACCESS do protokolu o nedepersonalizovaném TR, který vede na svém pracovišti. Jeho druhý výtisk předá oprávněné osobě.

- **TR, který je vymazán nebo jej nelze vymazat, je nutné <u>před předáním k ekologické likvidaci viditelně fyzicky poškodit</u>** (úderem kladiva do displeje a klávesnice nebo provrtáním těla TR minimálně na dvou místech vrtákem o průměru cca 10 mm) – zajistí oprávněná osoba.

Poznámka:

Likvidace TR ve vlastnictví organizačních složek státu se řídí zákonem č. 219/2000 Sb., o majetku České republiky a jejím vystupování v právních vztazích, v platném znění, a vyhláškou č. 62/2001 Sb., o hospodaření složek státu a státních organizací s majetkem státu, v platném znění.

2.9 Vyvezení funkčního TR systému mimo území ČR

Vyvézt funkční TR systému mimo území ČR je možno za následujících podmínek:

2.9.1 Vyvezení plánované

V případě potřeby vyvézt funkční TR mimo území ČR bez následného vedení rádiového provozu v cizí zemi (odřady, jízda techniky na výstavy, soutěže, apod.), i v případě potřeby vyvézt funkční TR mimo území ČR s následným rádiovým provozem v základním nebo rozšířeném kmitočtovém pásmu v cizí zemi, platí:

- Vyvezení je podmíněno udělením předchozího souhlasu vlastníka systému. Žádost bude obsahovat:
  - datum vyvezení a vrácení TR z/do ČR,
  - tranzitní a cílová země působení TR,
  - RFSI předmětných TR,
  - kdo požaduje, kontaktní osoba.

Žádost zasílá odpovědná osoba nebo OS vlastníkovi systému (e-mailem na sekretariat5@mvcr.cz, rezortní spisovou službou, dopisem na adresu MV ČR, Náměstí Hrdinů 1634/3, 140 21 Praha 4 nebo elektronicky na ID datové schránky: 6bnaawp). MV žádost posoudí bez zbytečného odkladu. Informaci o ne/schválení zašle žadateli zpět (obvykle způsobem podle formy přijetí žádosti).

- V případě, že při plnění úkolů v mimořádných situacích nelze postupovat výše uvedeným způsobem (např. při požadavku na vyslání odřadu o víkendu), oznámí oprávněná osoba nebo OS požadavek na vyvezení TR na NDP. Oznámení bude obsahovat údaje identické se žádostí. Vrácení TR zpět do ČR oznámí oprávněná osoba nebo OS na NDP. NDP bude o vyvezení a vrácení TR dané organizace informovat MV e-mailem na adresu sekretariat5@mvcr.cz.

2.9.2 Vyvezení operativní v rámci přeshraniční spolupráce

Při plnění bezpečnostních a záchranných úkolů v rámci mezinárodní přeshraniční spolupráce (např. řešení mimořádné události na území cizího státu v blízkosti státní hranice) pro vyvezení TR platí:

- Každý vyvážený TR musí mít předem upravenou konfiguraci parametrů, umožňující operátorovi TWP odejmutí přístupových práv ke službám systému v případě jeho ztráty nebo odcizení.

- Uživatel TR má povinnost aktivovat funkci monitoring sítě v režimu DIR. Tato povinnost se neuplatní v případě časové tísně nebo v případě, že by aktivace monitoringu ohrozila plnění bezpečnostních a záchranných úkolů.

Po návratu ze zahraničí je uživatel povinen provést fyzickou kontrolu TR. V případě zjištěné ztráty nebo odcizení postupuje podle části 2.2.

2.10 Provoz TR systému mimo území ČR

Provozovat TR systému mimo území ČR je možno za dále uvedených podmínek.

2.10.1 Provoz plánovaný

- Uživatel, který má od MV schváleno vyvezení TR mimo území ČR dle bodu 2.9.1 a který má záměr vést na území cizího státu rádiový provoz v základním nebo rozšířeném kmitočtovém pásmu systému, je povinen si předem zajistit od věcně příslušného orgánu daného státu (v souladu s legislativou tohoto státu) povolení k používání kmitočtů, které bude na jeho území používat. Bez tohoto povolení je používání TR systému na území cizího státu nelegální.

- SW koncových zařízení typu G3 byl frekvenčně upraven tak, že umožňuje pracovat v pásmu 380 – 430 MHz. Některým uživatelům, kteří dočasně plní úkoly na území cizího státu, je umožněno v DIR komunikovat svými TR na kmitočtech z pásma 406 – 430 MHz, tedy mimo základní kmitočtové pásmo přidělené pro systém.

Jedná se o anomální případy, při kterých je nutno dodržovat i následující podmínky:

- Úprava naprogramování TR se provede na základě písemného požadavku předloženého NAKIT, ve kterém bude uvedeno:
  - datum vyvezení a navrácení TR z/do ČR,
  - tranzitní a cílová země působení TR,
  - RFSI předmětných TR, kterým má být upraven kmitočtový rozsah,
  - kmitočet, který má být do TR nakonfigurován,
  - souhlas MV s vyvezením TR mimo území ČR,
  - kdo požaduje, kontaktní osoba.
- Úprava naprogramování TR bude provedena výhradně na TPS NAKIT.
- TR s upraveným naprogramováním nesmí být na území ČR provozován na kmitočtu mimo základní kmitočtové pásmo.
- Po návratu do ČR bude TR doručen na TPS NAKIT ke zpětnému přeprogramování.
- V případě, že TR nebude ke zpětnému přeprogramování doručen v určené době (dohodnuté při přeprogramování – záznam v žádosti), budou mu odebrána provozní práva.

Uživatel odpovídá za to, že TR nebude provozován na území cizího státu na kmitočtech, pro které v daném státě nemá povolení, a na území ČR na kmitočtech mimo základní kmitočtové pásmo systému.

2.10.2 Provoz operativní v rámci přeshraniční spolupráce

Při plnění operativních úkolů v rámci mezinárodní přeshraniční spolupráce je možno TR provozovat na území cizího státu v rádiové dostupnosti vf signálu infrastruktury systému. Provoz je veden identicky jako na území ČR.

2.11 Provoz TR složek cizích států na území ČR na kmitočtech základního kmitočtového pásma systému

Pokud je pro plnění plánovaných úkolů bezpečnostního a záchranného charakteru na území ČR nutná komunikace subjektů cizích států ve vlastních komunikačních systémech, je nutno provést v souladu s platnými předpisy ČR následující úkony:

- Cizí subjekt požádá ČTÚ o povolení používat své kmitočty na území ČR nebo jeho části (seznam kmitočtů jeho rádiové komunikace). Toto nevylučuje možnost předjednání použití kmitočtů přidělených pro systém s MV před podáním žádosti na ČTÚ.

- ČTÚ posoudí požadované kmitočty z pohledu Národní kmitočtové tabulky ČR. K případné možnosti dočasného použití kmitočtů z kmitočtového pásma přiděleného pro systém si vyžádá posouzení od vlastníka systému.

- MV posoudí možnost dočasného použití požadovaných kmitočtů subjektem cizího státu. Výsledek posouzení předá zpět ČTÚ.

- ČTÚ podle výsledku posouzení žádost zamítne, nebo vydá cizímu subjektu povolení k provozu na dobu určitou.

2.12 Přístupy k provozním zařízením, prvkům infrastruktury a rozhraní CC-IS

2.12.1 Přístupy obsluhy TPS

Obsluha TPS má přidělena plná práva k aplikaci TPS. Je to z toho důvodu, že některé úkony prováděné obsluhou TPS vyžadují administrátorská práva (např. manuální reset TR).

2.12.2 Přístupy operátora TWP

Operátor TWP zabezpečuje taktické řízení sítě PEGAS prostřednictvím zařízení TWP. Přístup k zařízení TWP operátorem je umožněn prostřednictvím zadání přihlašovacího jména a hesla (login / password). Každá regionální síť má definována přístupová práva podle přiděleného oprávnění, vyplývajícího z činnosti operátorů jednotlivých regionálních sítí. Oprávnění nastavuje pro jednotlivé regionální sítě administrátor KMC prostřednictvím přístupové aplikace PACK. Aplikace PACK je instalována společně s aplikaci TWP. Z hlediska nepřetržitého dohledu a nemožnosti odhlašování jsou vytvářeny společné přístupy pro všechny operátory dané regionální sítě.

Operátor TWP má definované dvě úrovně přístupů:

- první jen pro domácí regionální síť (tato úroveň je omezena z hlediska zobrazení a modifikace multiregionálních komunikací),
- druhou pro více regionálních sítí.

V rámci správy národní sítě jsou zřízeny:

- přístupy pro servisní organizaci s možností vstupu do všech regionálních sítí,
- přístup pro NDP a pro operátora regionální sítě Praha s možností vstupu do všech regionálních sítí.

Rozšíření nebo další přístupy je možné zřizovat jen se souhlasem administrátora KMC.

2.12.3 Přístupy obsluhy TMP

Operátor TMP zabezpečuje technické řízení systému prostřednictvím zařízení TMP (MD, TMP local / remote, OMC, XIP). Přístupy k těmto aplikacím jsou nastaveny jednotně v rámci národní sítě a jsou využívány operátory TMP, servisní organizací a vybranými pracovníky NAKIT. Přístupy jsou vytvářeny při instalaci výše uvedených aplikací a jsou pro všechny regionální sítě identické.

2.12.4 Přístupy integrátora pro OS

Integrátor pro OS má prostřednictvím rozhraní CC-IS přístup k MD systému. Přístupová oprávnění jsou definována ve dvou úrovních:

- pomocí aplikace PACK (shodná s aplikací pro TWP) se nastavuje oprávnění pro čtení, zápis a mazání,
- pomocí xml souboru v Bridge, který je podřízen nastavení oprávnění z PACK a umožňuje omezit definované oprávnění z jeho rozsahu.

Oprávnění určuje vlastník systému. Každý integrátor pro OS dané regionální sítě má svůj specifický přístup (login / password). V systému nastavení a přístupy definuje pro integrátora administrátor KMC. Oprávnění se nastavuje pro vlastníky CC-IS, které schvaluje vlastník systému pro každou regionální síť. OS může obsluhovat pomocí CC-IS jen vlastní organizaci ve své regionální sítí.

2.13 Uveřejňování informací o systému

Radiokomunikační systém PEGAS byl určen prvkem kritické informační infrastruktury postupem, uvedeným v části 1.1. Podle nařízení Vlády ČR č. 522/2005 Sb., v platném znění, je v jeho příloze č. 8 stanoven seznam utajovaných informací v oblasti působnosti Ministerstva vnitra, ve kterém se pod položkou č. 19 uvádí **Komplexní provozní údaje o neveřejné radiotelefonní síti** se stupněm utajení „V“**.** Vzhledem k tomu je nezbytné zamezit jakémukoliv neschválenému uveřejňování informací tohoto typu, a to například o provozním řešení systému (i o jeho částech), o nastavení sítí a jejich prvcích, o jejich umístění, uživatelích atp. Uveřejnění informací o provozním nastavení (i o jeho částech), o lokalitách, o uživatelích a dalších citlivých informací o systému (o autentizaci, o principech zavádění terminálů, o kryptografii) podléhá uveřejňování takových údajů schválení vlastníkem systému.

2.14 Používání komunikačních prostředků systému

Používat koncová zařízení systému mohou výhradně osoby, které úspěšně absolvovaly předepsané školení organizované danou organizací, jehož součástí byla obsluha koncových zařízení a seznámení s bezpečnostními postupy. Uživatel je při používání komunikačních prostředků systému povinen dodržovat technická a organizační opatření vydaná vlastníkem nebo provozovatelem systému k zajištění bezpečnosti a provozu.

2.15 Proces umístění technologie jiných subjektů na vysílací stanoviště

Pro správnou funkci systému jakožto prvku kritické informační infrastruktury byl stanoven procesní postup pro společné umisťování jiných technologií na vysílacích stanovištích ve správě MV, ZS MV a PČR., kde je instalována technologie infrastruktury systému. Obdobný postup je uplatňován rovněž cizími subjekty na vysílacích stanovištích, kde je umístěna technologie systému na základě nájemního smluvního vztahu. Pro nové umístění jiné technologie na vysílací stanoviště ve správě MV, ZS MV nebo PČR je požadavek žádajícího subjektu předán na ZS MV, které ve spolupráci s NAKIT a případně dalšími subjekty (PČR, PMC, RCD, CETIN,…) provede technické a administrativní procesní kroky podle níže uvedeného schématu:

- předání požadavku se záměrem na instalaci nové telekomunikační technologie, jehož součástí bude podkladová dokumentace v nezbytném rozsahu,
- provedení místního šetření (je-li nezbytné k posouzení záměru),
- posouzení záměru a závěrů z místního šetření s návrhem na umístění technologie ano/ne nebo vznik požadavku na doplnění dokumentace,
- v případě kladného výsledku pak povolení zkušebního provozu (pro PČR 1 měsíc, pro ostatní subjekty 2 měsíce),
- vyhodnocení zkušebního provozu především z hlediska rušení,
- v případě kladného výsledku pak vydání povolení k trvalému provozu.

3 Provozní data - zálohování, ukládání a výdej

3.1 Zálohování dat z TPS, TWP, TMP, KMC, EPC a Repeater

Zálohování provozních dat provádí obsluha nebo operátor. Záloha dat je určena pro obnovu systému nebo pro jejich analýzu. Data se uchovávají v systému 30 dní, případně méně při překročení jejich určitého objemu. Vždy je nutné provést zálohování dat tak, aby byla zálohovaná data za uplynulý měsíc kompletní.

Příklad 1:

Registrace u organizace 2 jsou za uplynulý den v počtu 22000. Zařízení TWP je schopné zobrazit pouze 15000 záznamů. Je nutné stáhnout data ve dvou souborech, které budou uloženy s jiným id (c:\\TWP/záloha R_2016/ reg_org2_15_08_a; c:\\TWP/záloha R_2016/ reg_org2_15_08_b).

Operátor může řadit zálohy dat podle měsíců, týdnů nebo dnů vložením podadresáře (do základní struktury adresářů) s názvem či označením měsíce, týdne nebo dne.

Příklad 2:

Registrace z 15. března - org. 2

c:\\TWP/záloha R_2016/03/15/reg_org2_15_08_a;
reg_org2_15_08_b;

Data se ukládají v daném zařízení a zároveň se ukládají na externí úložiště (HDD, není-li stanoveno jinak). Data se archivují po dobu 5 let. Pracoviště NDP předává data o registracích TR organizace 1 a 2 na server PČR.

3.2 Tabulka záloh dat a jejich uložení

Zodpovídá	Název	Interval	Úložiště PC	Externí úložiště
Obsluha TPS	Databáze organizací	1x týdně nebo po každé změně denně	Adresář TPS/záloha dbf_YYYY/*	Adresář TPS/ záloha dbf_YYYY/*
Obsluha TPS	Třídy služeb	1x ročně nebo po každé změně	Adresář TPS/záloha TS_YYYY/*	Adresář TPS/záloha TS_YYYY/*
Operátor TWP	Alarmy	podle potřeby, minimálně 1 x měsíčně	Adresář TWP/záloha A_YYYY/*	Adresář TWP/záloha A_YYYY/*
Operátor TWP	Voice	podle potřeby, minimálně 1 x za 14 dní	Adresář TWP/záloha V_YYYY/*	Adresář TWP/záloha V_YYYY/*
Operátor TWP	Registrace (po organizacích)	podle potřeby, minimálně 1 x denně	Adresář TWP/záloha R_YYYY/*	Adresář TWP/záloha R_YYYY/*
Operátor TWP	Operating	podle potřeby, minimálně 1 x měsíčně	Adresář TWP/záloha O_YYYY/*	Adresář TWP/záloha O_YYYY/*
Operátor TWP	Command	podle potřeby, minimálně 1 x měsíčně	Adresář TWP/záloha C_YYYY/*	Adresář TWP/záloha C_YYYY/*
Operátor TMP	Alarmy	podle potřeby, minimálně 1 x za 30 dní	Adresář TMP/záloha A_YYYY/*	Adresář TMP/záloha A_YYYY/*
Operátor KMC	Databáze	podle potřeby, minimálně 1 x denně	-	Na USB/CD RW – týdenní cyklus **
Administrátor KMC	Záloha TMK,DMK,PK	Po vygenerování a změně	KLU	Záložní a provozní flash disk v každé RN
Administrátor KMC	Záloha přístupových práv CCIS, TWP	Po vygenerování a změně	KLU	Záložní flash disk u KMC
Operátor NDP	Databáze repeatru	1 x týdně	Automaticky	Adresář Repater/záloha R_YYYY/*

Operátor NDP	Registrace (org.1 a 2)	1 x denně	-	Server PČR
Operátor TWP	Výstupní soubor zavádění TR	dle zavádění	Klíčové proměnné_201x /měsíc/den	RNxx /Klíč. prom._201x/ /měsíc/den
Operátor TMP (systémově)	Záloha ODB	1 x denně	-	server
Operátor NDP	data EPC	denně 1 x měsíčně	denně	1x měsíčně dle stanovené struktury

==========

Poznámka: YYYY – rok, * - název souboru_den_měsíc_id dle potřeby,
** - týdenní cyklus (záloha na medium označené 1 – 7, 1 = pondělí, 2 = úterý, …).
Záloha dat se provádí z následujících zařízení:
operátor TWP – z aplikace TWP, obsluha TPS – z aplikace TPS, operátor TMP – z aplikace TMP, operátor KMC – z aplikace KMC, operátor NDP – z aplikace Repeater

3.3 Výdej dat

Archivovaná data jsou určena pro obnovu systému nebo pro analýzu, případně pro statistické údaje o provozu nebo dohledání konkrétních provozních údajů (o TR, komunikacích apod.). Analýza může být provedena pro detekci chyb způsobených systémem či uživatelem a nalezení vhodného opatření k jejich eliminaci.

Data ze systému mohou využívat:

- vlastník systému,
- provozovatel systému,
- servisní organizace,
- oprávněné osoby dané organizace,
- jiný subjekt na základě zákonného oprávnění, případně na základě IAŘ MV ČR.

Výdej dat:

- Data o registracích TR jsou pro organizace 1 a 2 pravidelně ukládána na server PP ČR – viz část 3.1. Požadavek na ostatní data vyžaduje oprávněná osoba cestou MV v písemné podobě.
- Oprávněné osoby jiných organizací uplatňují požadavek na výdej dat cestou MV v písemné podobě.
- V případech, kdy hrozí nebezpečí z prodlení (ztráta, problémy při komunikaci apod.), lze informace neprodleně sdělit oprávněné osobě telefonicky (reakce na vzniklou situaci) za předpokladu, že se jedná o data jeho vlastní organizace. O předání informace provede operátor TWP záznam v provozním deníku s uvedením důvodu a kontaktu na osobu, která informace požadovala.
- Pracovníci zajišťující správu a servis systému si data vyžadují na pracovní úrovni bez písemného požadavku v rámci plnění svých povinností

4 TPS, TWP, TMP a KMC

4.1 Obsluha TPS

Obsluha TPS je povinna vést a průběžně aktualizovat dokumentaci TPS a pravidelně zálohovat provozní data. Pro každou organizaci vede obsluha TPS „Provozní deník TPS“, kde zaznamená každou změnu provedenou v naprogramování TR. V případě, že obsluha TPS vede provozní deník v elektronické formě (databáze, WEB,…), je povinna dodržet základní strukturu provozního deníku. Obsluha TPS nesmí umožnit přístup k TPS jiným než oprávněným osobám (vyškolené obsluhy TPS, administrátor KMC). Při standardní práci používá přístup k programování TR v režimu maintenance. Je zakázáno měnit přístupová oprávnění k aplikaci a k PC. Ruční výmaz TR se provádí v režimu Administrátor.

Obsluhám TPS je zakázáno:

a) Jakkoliv měnit či modifikovat TS bez souhlasu administrátora KMC (NAKIT ORS). Obsluha TPS může měnit pouze vybrané položky definované v TS, které jsou pro modifikaci uvolněné administrátorem KMC.

b) Sdělovat uživatelům nastavení služby klíčové modifikátory, která umožňuje nastavit TR pro provoz s možností použití vlastního šifrování (přešifrování stávající šifrované komunikace pomocí vlastního nebo definovatelného klíče modifikátoru).

c) Externím uživatelům, kteří jsou začleněni do užívání systému na základě zvláštních smluv na poskytování služeb uzavřených mezi jimi a MV, měnit rozsah oprávnění TS definovaný v těchto smlouvách.

4.1.1 Provozní deník TPS

Provozní deník obsahuje následující položky:

- RFSI TR,
- logické číslo TR,
- výrobní číslo TR,
- datum změny (jakákoliv změna provedená v TR),
- provedené činnosti (mazání, konfigurace, změna TS, nahrání pamětí atd.),
- počet zbývajících klíčů TMK na datovém nosiči[14],
- podpis programujícího.

Provozní deník je archivován po dobu minimálně 5 let.

Zbývající počet klíčových proměnných z původního počtu, jež byly administrátorem KMC vygenerovány pro danou regionální síť a organizaci, musí souhlasit s počtem použitých klíčových proměnných obsluhou TPS pro konfiguraci TR uvedených v provozním deníku TPS.

Nesoulad počtu klíčových proměnných může být hodnocen jako bezpečnostní riziko. Administrátor KMC provádí namátkovou kontrolu klíčových proměnných a vedení provozního deníku. Při zjištění nesrovnalostí provede písemný záznam, který předá MV k řešení.

4.1.2 Třídy služeb

Podklad pro programování TR je vydáván v elektronické podobě jako dokument „Třídy služeb, personalizace koncových zařízení“ (viz Nařízení MV č. 25 ze dne 25. dubna 2012). Každá TS sestává z kombinace jednotlivých služeb. TS jsou koncipovány tak, aby byla zajištěna jejich kompatibilita ve všech regionálních sítích z hlediska zabezpečení součinnosti jednotlivých útvarů a aby akceptovaly požadavky oprávněných osob, se kterými jsou TS vytvářeny. Požadavky na změnu nebo vytvoření nové TS uplatňují oprávněné osoby u provozovatele systému.

Obsluha TPS implementuje na pokyn administrátora KMC[1] aktualizované nebo nové TS do zařízení TPS. Dokument „Třídy služeb, personalizace koncových zařízení“ je umístěn na SharePoint MV: http://www.exresortmv.cz – sekce MV – menu “Activity“ – menu „PEGAS. Obsluhy TPS jsou o změnách v nastavení TS informovány prostřednictvím těchto webových stránek a současně také telefonicky.

4.1.3 Software koncových zařízení

Obsluha TPS (v souladu s dokumentací určenou pro TPS) instaluje základní SW koncových zařízení a aktualizaci project file do zařízení TPS. Obsluha TPS je povinna používat jen schválený SW, vystavený na SharePoint MV http://www.exresortmv.cz – sekce MV – menu “Activity“ – menu „PEGAS.

O uvolnění a nasazení aktualizovaného SW koncových zařízení jsou obsluhy TPS informovány s dostatečným časovým předstihem telefonicky nebo e-mailem pracovníkem NAKIT ORS – administrátorem KMC a následně písemnou formou cestou MV. Obsluha TPS je povinna poskytovat součinnost pracovníkům NAKIT ORS při testování nového SW.

4.1.4 Klíčové proměnné

Obsluha TPS uchovává klíčové proměnné (TMK, DMK, PK, KM) tak, aby je nebylo možné zneužít či poškodit. V případě poškození klíčových proměnných informuje bezodkladně administrátora KMC, který provede ve spolupráci s obsluhou TPS obnovu klíčových proměnných.

Je zakázáno jakkoliv modifikovat klíčové proměnné a používat média s vygenerovanými klíčovými proměnnými k jiným účelům než k přenosu klíčových proměnných do TR prostřednictvím zařízení TPS.

Obsluha TPS má k dispozici dvě média s klíčovými proměnnými:

a) klíčové proměnné pro konfiguraci TR,

b) klíčové proměnné pro obnovu v případě poškození původních klíčových proměnných.

Pokud na médiu s klíčovými proměnnými zbývá méně než 100 TMK klíčů, požádá obsluha TPS administrátora KMC o vygenerování dalších klíčových proměnných. V případě poškození klíčových proměnných postupuje dle pokynu administrátora KMC.

14 Položka key files v aplikaci TPS

4.1.5 Konfigurace TR

Konfigurace TR zahrnuje zadání jedinečného identifikačního čísla TR (RFSI), vložení klíčových proměnných atd. Při konfiguraci obsluha TPS definuje pomocné údaje pro identifikaci TR v databázi TPS. Pro sjednocení údajů všech regionálních databází TPS, je obsluha TPS povinna dodržovat následující strukturu údajů:

- Bar code: výrobní číslo TR
- Comments 1: informace o uživateli
- Comments 2: typ TR

4.1.6 Zavádění TR do systému

Po konfiguraci TR obsluha TPS vygeneruje zaváděcí soubor a předá jej operátorovi TWP k zavedení TR do systému. Zaváděcí soubory lze předávat:

- zabezpečenou vnitroresortní sítí MV,
- na přenosném médiu,
- internetem (soubor musí být zpracován archivačním programem a opatřen heslem).

4.2 Operátor TWP/TMP

4.2.1 Operátor TWP

Operátor TWP obsluhuje pracoviště taktického řízení regionální sítě v souladu s dokumentací jejího provozního nastavení. Provozní dokumentace dle „Nařízení MV č. 25/2012“ je umístěna na SharePoint MV – sekce PEGAS. Operátor TWP je povinen dodržovat a kontrolovat nastavené provozní parametry.

Změny provozního nastavení systému, včetně dočasných změn sloužících k zajištění mimořádných událostí (tzv. nestandardní změny provozního řešení), lze provádět pouze na pokyn nebo se souhlasem provozovatele nebo vlastníka systému.

V případech, kdy hrozí nebezpečí z prodlení, je operátor TWP oprávněn změnit parametry provozního nastavení i bez souhlasu vlastníka systému. O provedené změně je povinen provozovatele systému neprodleně informovat.

Operátor TWP vede o činnosti na pracovišti „Provozní deník“, do kterého je mimo jiné povinen zaznamenat všechny provedené změny provozních parametrů.

Zápisy v „Provozním deníku“ vždy musí obsahovat následující údaje:

- datum,
- čas,
- popis události,
- kdo žádal,
- kdo provedl.

Operátor při zavádění TR do systému (prostřednictvím konfiguračního souboru vygenerovaného v TPS) provádí zálohování výstupní informace o zavedení TR do systému. Výstupní soubor je ukládán na plochu TWP do adresáře Klíčové proměnné_202x/měsíc/den ve formátu:

den_měsíc_rok_poř.č. zavedení dne

4.2.2 Operátor TMP

Operátor TMP zajišťuje technický dohled nad infrastrukturou systému, řízení jednotlivých prvků infrastruktury a nastavuje parametry organizací v souladu s provozní dokumentací dle „Nařízení MV č. 25/2012“, která je umístěna na SharePoint MV – sekce PEGAS. Vyhodnocuje a řeší alarmová hlášení automaticky generovaná systémem a zobrazovaná na TMP. Provádí zálohu dat podle části 3.1.

K řešení chybových stavů používá CA SD a další nástroje (AIF report, SIR,..).

5 Kryptografie

5.1 MSW

Hlavní rádiová ústředna obsahuje klíčové proměnné, které jsou uloženy na HDD a CHIF desce. Tyto klíčové proměnné jsou určeny pro distribuci a vzájemnou komunikaci v rámci systému. Klíčové proměnné jsou zaváděny administrátorem KMC[1] do MSW prostřednictvím zařízení KMC a KLU. Komponenty HDD a CHIF deska v MSW obsahující klíčové proměnné jsou před neoprávněnou manipulací zabezpečeny bezpečnostní plombou s hologramem, jejíž umístění znemožňuje manipulaci s výše uvedenými prvky, aniž by došlo k poškození hologramu. Označení zajišťuje administrátor KMC a bez jeho souhlasu je zakázáno s uvedenými prvky manipulovat. V každé regionální síti je k dispozici záložní HDD a přenosné médium pro obnovu klíčových proměnných včetně přístupových práv pro PACK TWP. Média jsou uložena v ochranném obalu, který je zabezpečen bezpečnostní plombou s hologramem. Použití záložních médií je povoleno výhradně se souhlasem administrátora KMC.

5.2 TPS

Klíčové proměnné pro zařízení TPS jsou generovány administrátorem KMC pomocí zařízení KMC a KLU. Klíčové proměnné pro TPS administrátor KMC předává obsluze TPS na přenosném médiu, které je označeno popisem a bezpečnostní plombou s hologramem. O předání je zpracován předávací protokol. Zacházení s klíčovými proměnnými pro TPS je řešeno v části 4.1.4.

5.3 KMC

Zařízení KMC je umístěno v zabezpečeném prostoru pracoviště NDP a je pod trvalým dohledem jeho operátora. Zařízení KMC má trvale připravenou provozní zálohu pro případ poruchy. Pro obsluhu zařízení KMC jsou definovány dvě přístupové úrovně:

- **Administrátor KMC** – zajišťuje management, instalaci, obnovu a distribuci klíčových proměnných. Definuje přístupová práva ke KMC.
- **Operátor KMC** – zajišťuje zálohování databáze a dále postupuje v rozsahu stanoveném dle pokynu administrátora KMC.

Instalační média, bezpečnostní plomby s hologramy, CAM Card a náhradní díly šifrových komponent KMC jsou umístěny v trezoru.

6 SW PEGAS - schvalování, distribuce, instalace a archivace

6.1 Schvalování a distribuce SW

Distribuce SW pro systém se týká koncových zařízení a provozních pracovišť systému, tj. TMP, TWP, MD, OMC, TPS, KMC a KLU. SW je dodáván výrobcem systému servisní organizaci, která po jeho odzkoušení a validování zajistí distribuci na NAKIT ORS. Před uvolněním SW jsou určenými pracovníky tohoto oddělení kontrolovány jeho základní funkce a proces odstranění chyb, které má SW řešit. Kontrola je prováděna pouze na dostupných koncových zařízeních. Určení pracovníci NAKIT ORS ne/akceptují nasazení dodaného SW.

V případě jeho schválení dále zajišťují distribuci a umístění SW na webové stránky vlastníka systému SharePoint MV, http://www.exresortmv.cz – sekce MV – menu “Activity“ – menu „PEGAS“. V případě neschválení není SW uvolněn k použití a je zpracován AIF report na řešení zjištěných chyb. Pokud jsou zjištěny SW chyby po nasazení SW do systému je na pokyn NAKIT ORS stažen SW z provozu a řešen cestou AIF.

6.2 Instalace SW

- Instalace SW pro koncová zařízení je pro obsluhy TPS závazná vystavením SW na webových stránkách PEGAS umístěných na serveru vlastníka systému (viz http://www.exresortmv.cz – sekce MV – menu “Activity“ – menu „PEGAS“).
- SW aplikace TPS instaluje servisní organizace nebo pracovník NAKIT ORS.
- Instalaci SW pro zařízení KMC, TWP, KLU, TMP_{remote} zajišťuje administrátor KMC nebo servisní organizace.
- Instalaci SW pro zařízení TMP, MD, OMC zajišťuje servisní organizace.

Webové stránky vlastníka systému jsou určeny k urychlení procesu instalace aktuálního SW. Přístup na webové stránky je dostupný jen oprávněným osobám (obsluha TPS, vlastník systému, zástupci uživatelů, NAKIT ORS). Správa sekce PEGAS na SharePoint MV a správa přístupových oprávnění je v kompetenci NAKIT ORS.

6.3 Archivace SW

Médium (DVD, CD ROM) obsahující dodaný SW je uloženo v SW archivu na NAKIT ORS společně s kopií předávacího protokolu a spisu po dobu minimálně 5 let. SW archiv vede určený pracovník NAKIT ORS. Originál předávacího protokolu a spisu je uložen v souladu s pokyny pro spisovou službu.

7 Gesční souhlas vlastníka systému

Pro schvalování zavedení typově nového příslušenství, zařízení nebo SW komponenty do systému, které nebylo dodáno dodavatelem systému nebo se souhlasem dodavatele systému, platí od 1. 9. 2020 z důvodu zajištění bezpečnosti systému a garance zachování správné funkčnosti systému následující postup:

- Uživatel, dodavatel nebo výrobce takového příslušenství, zařízení nebo SW komponenty je povinen ještě před jeho zavedením do systému vyžádat si gesční souhlas vlastníka systému s jeho zavedením a používáním v systému.
- Na základě žádosti uživatele, dodavatele nebo výrobce takového příslušenství, zařízení nebo SW komponenty podané vlastníkovi systému o vydání gesčního souhlasu provede servisní organizace otestování, resp. posouzení takového příslušenství, zařízení nebo SW komponenty s cílem zjistit a vyhodnotit, zda jeho používání v systému i v návaznosti na funkčnost služeb nebo technologických částí systému tyto neohrožuje, neupravuje nebo neomezuje z pohledu jejich správné funkce.
- V případě vyhodnocení, že používání takového příslušenství, zařízení nebo SW komponenty ne/ohrožuje, ne/upravuje nebo ne/omezuje správnou funkčnost systému, zpracuje servisní organizace protokol se závěrem, že předmětné příslušenství, zařízení nebo SW komponentu je/není možno zavést a používat v systému.
- Na základě kladného závěru protokolu servisní organizace vydá vlastník systému uživateli, dodavateli nebo výrobci gesční souhlas s jeho používáním. Tento souhlas je platný vždy pouze pro testovanou verzi nebo revizi příslušenství, zařízení nebo SW komponenty. V případě nové verze příslušenství, zařízení nebo SW komponent je třeba testy opakovat.
- V případě změny verze firmware systému může servisní organizace vyzvat k přetestování příslušenství, zařízení nebo SW komponenty. Dodavatel nebo výrobce příslušenství, zařízení nebo SW komponenty je povinen poskytnout bez zbytečného odkladu veškerou součinnost servisní organizaci v těchto testech. V případě neposkytnutí součinnosti informuje servisní organizace vlastníka systému, který gesční souhlas odejme.
- V případě vyhodnocení, že používání takového příslušenství, zařízení nebo SW komponenty ohrožuje, upravuje nebo omezuje správnou funkčnost systému, pak vlastník systému souhlas s jeho používáním nevydá. To znamená, že neschválené používání takového příslušenství, zařízení nebo SW komponenty není vlastníkem systému povoleno a ten, kdo neschválené příslušenství, zařízení nebo SW komponentu do systému připojil, odpovídá právně i hmotně za odstranění vzniklých následků v systému samotném i v návazných technologických celcích, které využívají jeho služeb (např. AVL, IOS, databáze a další).
- Používání nepovolených komponent či komponent bez gesčního souhlasu je bráno jako bezpečnostní riziko ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti, v platném znění, a to se všemi důsledky z toho vyplývajícími.

Poznámka:

Gesční souhlas vlastníka systému je kladné rozhodnutí vlastníka systému o možnosti užívání typově nového příslušenství, zařízení nebo SW komponenty určité verze nebo revize v systému, a to na základě provedených testů, prokazujících vlastnosti a funkce kompatibilní s danou verzí technologie systému.

8 Kontrolní činnost

Kontrolu nad dodržováním „Bezpečnostních postupů“ jsou oprávněni provádět určení pracovníci vlastníka a provozovatele systému, kteří se prokazují pověřením ředitele odboru provozu informačních technologií a komunikací MV. Za vlastníka systému se jedná o pracovníky oddělení komunikací a za provozovatele systému o pracovníka NAKIT ORS – administrátora KMC[1]. O provedené kontrolní činnosti je výše uvedenými pověřenými pracovníky sepsán záznam, který se ukládá u vlastníka systému. Při zjištění porušení „Bezpečnostních postupů“ je toto porušení řešeno cestou vlastníka systému.

9 Referenční dokumenty

- Technical Management – Regional Network Operating Manual [PS8593 nebo PS8594, PS11127]
- Tactical Management – Regional Network Operating and Maintenance Manual [PS8597 nebo PS8598]
- Systém Delivery Note [PSxxxx v závislosti na projektu]
- Taktické řízení – provozní a údržbový manuál regionální sítě [PS8595 nebo PS8596]
- TWP – technický manuál [PS8669]
- Obecné představení systému [PS10322g]
- Programovací stanice terminálu – TPS technický manuál [PS10517]
- Technical Management – technické řízení, údržbový manuál regionální sítě [PS10251]
- KLU technical Manual [PS8420]
- Operating Procedures for Security Functions [PS8459]
- Nařízení MV č. 25/2012
- Provozní dokumentace uvedená v Nařízení MV č. 25/2012

10 Formuláře

Příloha č. 1: Regionální evidence stažení RAM

Příloha č. 2: Regionální evidence ztracených TR

Příloha č. 3: Regionální evidence poškozených, zničených TR

Příloha č. 4: Provozní deník TPS

Příloha č. 5: Protokol o nedepersonalizovaném TR

Příloha č. 6: Formulář o depersonalizovaném TR

Příloha č. 7: Servisní zpráva

Příloha č. 8: Národní evidence ztracených a odcizených TR vedených v CA SD

Příloha č. 1: Regionální evidence stažení RAM

Regionální evidence stažení RAM							
Datum stažení	***RFSI TR***	***Stažení RAM provedl***	***Operátor***	***Datum přeprogramování TR***	***Datum Vymazání TR***	***Přeprogramování / vymazání provedl***	***Poznámka***

Příloha č. 2: Regionální evidence ztracených TR

Regionální evidence ztracených terminálů						
Datum / čas ztráty	***Ztrátu hlásil***	***Kontakt***	***Zákaz provozních práv datum / čas***	***Operátor TWP***	***Anocod 10012 Datum / čas***	***Zákaz přístupových práv datum / čas***
Operátor	***Anocod 10017 Datum / čas***	***Vymazání z TWP Datum / čas***	***Operátor TWP***	***Vymazání z TPS Datum / čas***	***Obsluha TPS***	***Poznámka***

Příloha č. 3: Regionální evidence poškozených, zničených TR

Regionální evidence zničených, poškozených terminálů						
Datum / čas nahlášení znič. TR	***Zničení nahlásil***	***Kontakt***	***Zákaz přístup. práv datum / čas***	***Zákaz provedl Operátor - jméno***	***Anocod 10017 Datum / čas***	***Operátor***
Protokol od uživatele doručen dne	***Terminál doručen dne***	***Posouzení provedl / číslo servisní zprávy***	***Vymazání TR z TWP Datum/čas/operátor***	***Vymazání TR z TPS Datum/čas/operátor***	***Terminál vrácen uživateli dne***	***Poznámka***

Příloha č. 4: Provozní deník TPS

Organizace č. …

Datum	R F S I Terminálu	Seriové číslo (log. číslo)	Výrobní číslo	Typ změny	Počet klíčů	Jméno operátora	Poznámka
Dne *12.12.2019* - zůstatek původních klíčových proměnných v počtu : *39* kontrolu provedl: *Jan Beneš* Dne *12.12.2019* - nové klíčové proměnné v počtu : *1000*							
14. 12. 2019	*101 111 125*	*25525500*	*123456789*	*R, K, TS*	*999*	*Koudelka*	*Po stažení RAM*

Legenda pro položku „TYP ZMĚNY“ :

TS - třída služeb **R** - reset TR **SW** - změna SW **K** - update klíčů, nový klíč po resetu **N** - nový TR **T** – test

Poznámka:

- výrobní číslo / posledních 9 čísel /,
- příklad vedení deníku – vyznačen červeným písmem

Příloha č. 5:

Protokol o nedepersonalizovaném TR

Protokol o neresetovaném terminálu	
Pořadové číslo	RN – poř.č./ org - rok
Uživatel	PČR / HZS /…event. útvar
Typ TR	BER, HH G2 – S, E, E+,…
RFSI	RRR FSS III
Výrobní číslo	
Logické číslo	
Reset na TPS dne:	dd.mm.rrrr
Reset provedl:	Jaroš
Reset na TWP dne:	dd.mm.rrrr
Reset provedl:	Hložek
Poznámka	
Předáno uživateli – MěP **nebo** *Předáno do servisního střediska*	
Datum dd.mm.rrrr	***Podpis***

Příloha č. 6:

Formulář o depersonalizovaném TR

Formulář o resetovaném terminálu			
Pořadové číslo		RN – poř. č./ měsíc - rok	
Seznam TR			
Typ terminálu	V.č.	Popis závady	Poznámka
TPH 700	123456789	Nefunkční displej	I-125236
Seznam příslušenství			
Typ	V.č.	Popis závady	Poznámka
Nabíječka TPH 700	4564564A01	nenabíjí	I-253526
Reset TR na TPS dne:		dd.mm.rrrr	
Reset provedl:		Jaroš	
Poznámka			
Předáno zpět uživateli – MěP **nebo** *Předáno do servisního střediska cestou NAKIT*			
Datum	dd.mm.rrrr	***Předal:***	
Datum	dd.mm.rrrr	***Převzal:***	

Příloha č. 7: Servisní zpráva

SERVISNÍ ZPRÁVA číslo:

xx /2020

Hlavička servisního střediska

1. ZÁKLADNÍ ÚDAJE

Druh zařízení: vozidlová radiostanice
Typ: BER RA 1585
Výrobní číslo: RA 1585CA04 001404929
RFSI: 101 125 123

2. UŽIVATEL

Útvar: OIKT Praha III
Zadavatel: Votýpka Alois

3. POPIS ZÁVADY

Terminál nejde zapnout, poškození logické desky, problém s konfigurací SW, terminál byl přejet vozidlem,…

4. VYJÁDŘENÍ SERVISNÍHO TECHNIKA

- Terminál odeslán do výrobního závodu na opravu požadavek KZ – 42 /07), terminál byl vrácen jako neopravitelný.
-Terminál je poškozen korozí, patrně utopen nebo poškozen vodou. Oprava je nerentabilní.

NAVRHUJI VYŘADIT Z PROVOZU A EVIDENCE.

Datum: …… 2020 Zpracoval:

Příloha č. 8: Národní evidence ztracených a odcizených TR vedených v CA SD