Tato směrnice je řídicím dokumentem společnosti NET4GAS, s.r.o.
Postupování třetím osobám je možné pouze se souhlasem jednatele společnosti.

	Zpracoval	Přezkoumal po věcné stránce	Přezkoumal po formální stránce	Schválil
Funkce	Senior specialista, IT	Ředitel, Informační technologie	Specialista, Korporátní záležitosti	Jednatel
Jméno	Ing. Radmila Jandová	Ing. Zdeněk Haloda	Daniela Kašparová	Ing. Hrach Václav, Ph.D.
Podpis	v.r.	v.r.	v.r.	v.r.
Datum	09.02.2015	11.02.2015	03.02.2015	18.02.2015

Změnový list

Označení části textu*	**Popis změny**
	Základní – výchozí verze dokumentu

** příp. odkaz na kapitolu, odstavec, …*

Rozdělovník

a) Typový:

- Jednatel společnosti - Výkonný ředitel, Finance
- Ředitel, Informační technologie
- Zpracovatel
- Specialista, Korporátní záležitosti - správce řízené dokumentace
- Zaměstnanci společnosti NET4GAS, s.r.o.

b) Individuální:

Útvar	Funkce

Obsah

A Účel

Společnost NET4GAS, s.r.o., (dále jen „Společnost“) tímto dokumentem deklaruje seznam požadavků na aplikování bezpečnostních standardů, norem a mechanismů používaných při provozu komunikačních technologií a informačních systémů (dále jen „ICT/IS“) ve všech prostorách, ve kterých dochází ke zpracování dat Společnosti.

Primárním účelem této směrnice je nastavení politiky a parametrů pro zabezpečení informací zpracovávaných v rámci ICT/IS a stanovení odpovídajících opatření pro jejich komplexní ochranu. Směrnice rozpracovává požadavky obecně závazných předpisů a požadavky „*Bezpečnostního řádu NET4GAS, s.r.o.*“, na řešení ochrany informací v prostředí Společnosti. Cílem je zajistit komplexní ochranu informací zpracovávaných v ICT/IS.

Dalším účelem této směrnice je zajištění bezpečnosti informací při práci v ICT/IS a seznámení všech subjektů s tím, co je při zpracování informací v ICT/IS povoleno nebo zakázáno.

Společnost si vyhrazuje právo modifikovat a doplňovat tuto směrnici podle aktuální potřeby. Tento dokument je dle potřeby doplňován o další metodické pokyny. Všechny subjekty pracující s ICT/IS budou o každé změně vhodným způsobem informováni před nabytím její platnosti.

Nedodržení bezpečnostní principů, zásad, opatření a postupů popsaných v této směrnici je považováno za závažné porušení povinnosti vůči Společnosti. Při výskytu takovýchto závažných porušení povinnosti bude Společnost postupovat v souladu s právními předpisy České Republiky a v maximální možné míře využije svých práv i možných sankcí uvedených například v zákoníku práce v případě zaměstnanců Společnosti či dalších smluvních vztahů v případě jejích dodavatelů.

Tento dokument se primárně zaměřuje na zpracování informací elektronickou formou, přesto jsou někdy uváděny i požadavky na komplexní ochranu informací neboť technologie ICT/IS poskytují nebo potřebují vstupy a výstupy i v neelektronické formě např. vytištění informací o konfiguraci firewallu, hesla v obálkách uložená na definovaných místech apod.

Za revizi a změny této směrnice a postupů v ní uvedených zodpovídá ve společnosti NET4GAS, s.r.o., vlastník procesu.

Kontrolu plnění této směrnice smí provádět zejména pracovníci úseku IT společnosti NET4GAS, s.r.o.

B Rozsah platnosti a kontrola

Tato směrnice je platná tam, kde dochází ke zpracování a uchovávání informací Společnosti nebo tam, kde jsou dislokovány prostředky ICT/IS v majetku Společnosti. Příkladem těchto prostor jsou např. místnosti uživatelů, datová centra (DC), prostory Service Desku a ostatní prostory Společnosti.

Osoby, které jsou zavázány jednat v souladu s touto směrnicí a všichni zaměstnanci Společnosti mají spoluzodpovědnost za zabezpečení informací. Proto musí mít k dispozici dokumenty definující bezpečnostní politiku v listinné nebo elektronické formě. Seznámení s bezpečnostní dokumentací stvrzují všechny subjekty a osoby pracující v ICT/IS svým podpisem (v dalším textu jsou všechny subjekty pracující v ICT/IS zahrnuty do pojmu Uživatel).

V době účinnosti této směrnice je bezpečnostní politika Společnosti definována skupinou interních dokumentů uvedených v kap. E.2.2 Řídicí dokumenty Společnosti.

Nadřazená bezpečnostní dokumentace:

- *Bezpečnostní řád NET4GAS s.r.o.*“
- „*Bezpečnostní pravidla pro ochranu informací*“
- „*Ochrana dat*“ - Metodický pokyn pro práci s klasifikovanou informací
- „*Řízení rizik v NET4GAS, s.r.o.*“

- *„Řízení fyzické bezpečnosti v N4G“*

Bezpečnostní dokumentace dále určená přímo pro ICT/IS:

- „*Bezpečnostní politika IT* “ (IT-SECPOL) - tento dokument / tato směrnice
- „*Metodický pokyn IT-SECPOL pro Uživatele*“
- „*Metodický pokyn IT-SECPOL pro Dodavatele*“
- „*Ochrana koncových stanic*“
- „*Metodika vedení IT projektů*“
- „*Řešení IT požadavků v rámci úseku Informační technologie NET4GAS, s.r.o*“
- „*Bezpečnostní pravidla pro práci s výpočetní technikou*“
- *„Metodický pokyn IT-SECPOL pro ŘS a SCADA systémy“* a další následně vydané metodické pokyny pro ICT/IS

Směrnice uvedené v bezpečnostní dokumentaci určené přímo pro ICT/IS dále doplňují další případné metodické pokyny, které řeší specifické oblasti bezpečnosti ICT/IS. Metodické pokyny jsou vydávány a schvalovány nezávisle na tomto dokumentu. Dokumentace určená přímo pro ICT/IS vychází z požadavku pro systém řízení bezpečnosti informací (dále jen ISMS) dle požadavků norem ISO/IEC 27001:2013 - ISO/IEC 27001:2013.

C Definice pojmů a zkratek

Pojem / Zkratka	Definice
Aktivum	Vše, co má pro organizaci hodnotu hmotnou (zaměstnanci, počítač, materiál, finanční hotovost apod.) nebo nehmotnou (programy, data, kvalita personálu apod.).
Aktivum ICT/IS	Zahrnuje Primární aktiva Společnosti ve formě ICT služeb a Podpůrná aktiva v rámci ICT/IS (tj. aktiva v přímé odpovědnosti útvaru IT či jeho pracovníků).
Analýza rizik	Proces, který slouží k odhadu ztrát, jež mohou vzniknout působením hrozeb na systém, a dává přehled o nebezpečnosti jednotlivých hrozeb, jejich zdrojích, zranitelnostech hodnoceného systému a rizikách, kterým je hodnocený systém vystaven.
Autorizovaný Uživatel	Uživatel, který má určité právo nebo povolení pracovat v IS a s aplikacemi podle stanovených zásad přístupu.
Bezpečnost informací	Vlastnost nebo stav ochrany informací proti potenciálním ztrátám. Opatření k zachování důvěrnosti, integrity, dostupnosti, autentičnosti, odpovědnosti, nepopiratelnosti, spolehlivosti a správnosti.
Bezpečnost ICT/IS	Vlastnost nebo stav ochrany informací proti potenciálním ztrátám. Opatření k zachování důvěrnosti, integrity, dostupnosti, autentičnosti, odpovědnosti, nepopiratelnosti, spolehlivosti a správnosti.
Bezpečnostní architekt ICT/IS	Bezpečnostní role, která odpovídá za propojování informačních systémů a jejich částí. Tato role pomáhá definovat požadavky na bezpečnost předávaných dat, rozhraní, klasifikaci systémů apod.
Bezpečnostní incident	Je jedna nebo více nechtěných nebo neočekávaných indikovaných bezpečnostní událostí, jimiž může být s vysokou pravděpodobností narušena podpora hlavních procesů organizace nebo díky nimž může dojít k narušení bezpečnosti IS.
Bezpečnostní opatření	Opatřením se rozumí procedura, postup nebo mechanismus, který snižuje riziko na požadovanou úroveň podle požadavků bezpečnostní politiky.
Bezpečnostní politika ICT/IS	Pravidla, směrnice a zvyklosti určující způsoby, pomocí kterých jsou v Společnosti a jejím ICT/IS chráněna, řízena a distribuována Aktiva.
Bezpečnostní událost	Identifikovaný stav informačního systému, služby nebo počítačové sítě, jež může narušit pravidla bezpečnostní politiky nebo selhání některého opatření nebo dříve neznámé nebo nepředpokládané situace, jež můžou ovlivnit bezpečnost.
Bezpečnostní výbor ICT/IS	Nejvyšší orgán rozhodující o prosazování bezpečnosti v systémech ICT/IS.
Centrální nákup	Část útvaru Nákupu a logistiky v rámci organizační struktury NET4GAS, s.r.o., který zajišťuje nákup od již schváleného POBJ přes výběr vhodného Dodavatele, uzavření smluvního vztahu vytvořením a podepsáním smlouvy nebo objednávky až po zajištění

Pojem / Zkratka	Definice
	kompletní dodávky materiálu či služby, včetně strategie pro jednotlivé nakupované komodity, řídí prodej majetku
DMZ	Demilitarizovaná zóna – část sítě společnosti provozující Aktiva ICT/IS dostupná z Internetu
Dodavatel	Třetí strana, která má se Společností schválený smluvní vztah na minimálně jednu z následujících činností: dodávku, provoz, monitoring a údržbu služeb a Aktiv ICT/IS.
Definované úložiště	Úložiště uvedená v seznamu Definovaných úložišť, spravovaným útvarem IT. Seznam definovaných úložišť je na Intranetu Společnosti.
HSSE	Health, Safety, Security, Environment - Útvar Procesy a organizace, bezpečnost a ŽP
Informační Aktivum	je definovatelná část informace, která může být uchovávaná v jakékoli formě a zároveň uznávána jako "hodnotná" pro Společnost. Takováto informace může pocházet i z více informačních zdrojů. Informační Aktiva musí splňovat alespoň některou z následujících podmínek: 1. Jsou považovány za hodnotné a přínosné pro Společnost. 2. Nejsou jednoduše nahraditelné bez nákladů na znalosti, čas, zdroje Společnosti nebo jejich kombinaci. 3. Váže se na ně image a pověst Společnosti. 4. Obsah, který nesou, je možno klasifikovat z pohledu utajení 5. Jejich ztráta negativně ovlivní výkon nebo to, jak je Společnost svým okolím vnímána. 6. Informační Aktiva je možné dále klasifikovat dle typu.
IM	Instant messaging – online komunikace mezi účastníky např. pomocí LYNC, SKYPE apod.
IRT – Incident Response Team	Tým řešící a reagující na výskyt bezpečnostního incidentu. Tento tým ustavuje Ředitel, Informační technologie a jsou v něm definováni členové v roli Správců ICT/IS. IRT tým přizvat k řešení incidentu jakoukoliv třetí stranu dle aktuální potřeby.
ISMS	Systém řízení bezpečnosti informací. Součást řízení Společnosti, zaměřená na řízení rizik a zlepšování bezpečnosti ICT/IS Společnosti (viz norma ISO/IEC 27001:2013).
Koncové zařízení	Jakékoliv elektronické a mechanické zařízení, které může uchovávat a zpracovávat informace Společnosti a nebo jakékoliv zařízení připojené do sítí ICT/IS. Příkladem může být pracovní stanice, notebook tablet, smartphone, odečtoměry, snímače a další. V návazných metodických pokynech bude provedena detailnější kategorizace koncových zařízení.
Klíčový uživatel ICT/IS	Je zaměstnanec Společnosti, který má zodpovědnost za správnou funkci dané aplikace z pohledu Uživatelů. Tento Uživatel pomáhá s rozvojem aplikace, schvaluje plánované výpadky, komunikuje s ostatními Uživateli dané aplikace, schvaluje přístupová práva k příslušné aplikaci atd.
MP, Metodický pokyn	Typ řídicího dokumentu, poskytuje detailní informace o tom, jak opakovaně provádět konkrétní činnosti
Mobilní zařízení	Jakékoliv elektronické zařízení, které může uchovávat a zpracovávat informace Společnosti a nebo jakékoliv zařízení připojené do sítí ICT/IS mimo specializovaných zařízení používaných pro přepravu plynu. Příkladem může být notebook tablet, smartphone, Blackberry telefon atd. V návazných metodických pokynech bude provedena detailnější kategorizace koncových zařízení. Mobilní zařízení jsou chápána jako podmnožina koncových zařízen, která jsou přenosná tj. mobilní.
Neautorizovaný uživatel ICT/IS nebo třetí strana	Uživatel ICT/IS nebo třetí strana užívající ICT/IS, která neprošla autentizací a autorizací v ICT/IS.
NDA	Non Disclosure Agreement – Dohoda o mlčenlivosti.
Pracovní stanice	PC nebo notebook nebo technologické PC poskytující službu koncovému Uživateli ICT/IS, který má přímý fyzický přístup k tomuto zařízení.
Primární aktivum	Primárním aktivem je informace nebo služba, kterou zpracovává nebo poskytuje ICT/IS.
Podpůrné aktivum	Podpůrným aktivem je technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti ICT/IS (technickým aktivem je technické vybavení, komunikační prostředky, programové vybavení a objekty ICT/IS).
Přenosná média	přenosné paměťové nosiče datových informací (např. přenosný HDD, CD, DVD, USB disk atd.).
Riziko	Potenciál, že daná hrozba využije zranitelností Aktiv ICT/IS nebo skupiny Aktiv a způsobí tak ztrátu Společnosti, zničení Aktiv nebo narušení jejich dostupnosti, integrity, utajení, autentičnosti, odpovědnosti, nepopiratelnosti, spolehlivosti a správnosti.
Řízení rizik	Souhrn všech činností a opatření sloužící k rozpoznání (identifikaci), analýze (měření), řízení a vykazování rizik na úrovni všech procesů probíhajících v Společnosti.

Pojem / Zkratka	Definice
ŘS	Řídicí systém pro kontrolu přepravy plynu.
SCADA	Klíčový systém pro řízení přepravy plynu.
Service Desk	Jednotný bod servisní podpory koncových Uživatelů, na který se hlásí všechny uživatelské požadavky a problémy. Výjimkou jsou systémy řízení SCADA, které provozují vlastní service desk.
SM, Směrnice	Typ řídicího dokumentu, určuje metody, pravidla, postupy, prostředky pro výkon činností v procesech a jejich součinnost.
Společnost	NET4GAS s.r.o.
Subjekt	Jakákoliv osoba pracující s informacemi Společnosti v ICT/IS. Příkladem jsou zaměstnanci společnosti, externí dodavatelé, poskytovatelé služeb.
Šifrování	Převod dat do nečitelné podoby pomocí šifrovacího algoritmu a klíče (hesla). Dešifrování je pak opětovný převod do původního stavu po zadání klíče (hesla).
Uživatel	Je zaměstnanec Společnosti, třetí strany nebo jinou osobou autorizovanou pro využívání informací společnosti v rámci ICT/IS ke svým pracovním povinnostem.
UPS	Zdroj nepřerušitelného napájení.
Windows doména či doména Windows	Mechanismus prosazování managementu a bezpečnosti na počítače s operačním systémem Windows, kteří jsou členy stejné Active Directory domény.
Zaměstnanec	Osoba, která má se společností NET4GAS, s.r.o., uzavřenu řádnou pracovní smlouvu.
ŽP	Životní prostředí

D Popis procesů a pravidel

Politika systému řízení bezpečnosti informací je uvedena v nadřazené bezpečnostní dokumentaci viz kapitola B. Předmětem tohoto dokumentu/směrnice je definice bezpečnostní politiky jen pro jednu z částí Společnosti a to ICT/IS, tj. tento document stanovuje bezpečnostní pravidla pro ICT/IS.

D.1 Bezpečnostní politika ICT/IS

Bezpečnostní politika ICT/IS řeší pouze oblast ICT/IS a je tvořena dílčími politikami pro jednotlivé oblasti ICT/IS viz obsah kapitoly D.1 až D.17 tohoto dokumentu a navazující metodické pokyny například „*Metodický pokyn IT-SECPOL pro Uživatele*“, „*Metodický pokyn IT-SECPOL pro Dodavatele*“ a další návazné metodické pokyny.

D.1.1 Cíle v oblasti bezpečnosti ICT/IS

Bezpečnostní politika ICT/IS společnosti si klade následující cíle:

- zpřístupňovat informace jen ověřeným a autorizovaným subjektům,
- udržovat důvěrnost, integritu a dostupnost informací,
- stanovit a testovat postupy pro krizové scénáře,
- udržovat informace a vzdělávat zaměstnance o systému řízení bezpečnosti informací,
- vyžadovat dodržování procesů definovaných systémem řízení bezpečnosti informací Společnosti,
- vyhodnocovat a ukládat informace o bezpečnostních incidentech,
- analyzování bezpečnostních incidentů a odpovídajících reakcí na ně,
- kontinuální zlepšování a revize bezpečnostních směrnic a dalších metodických pokynů.

Smyslem aplikování bezpečnostních zásad a opatření v ICT/IS je udržení a zdokonalení základní úrovně bezpečnosti komponent ICT/IS tj. koncových zařízení, aplikací, dat a sítě. Zásady, postupy a doporučení, které jsou uvedeny v tomto dokumentu, jsou závazné pro všechny Uživatele a třetí strany pracující s informacemi nebo Aktivy Společnosti. Ostatní subjekty (třetí strany) např. externí dodavatelé,

se k dodržování tohoto souboru bezpečnostních zásad musí výslovně zavázat formou písemného souhlasu a podepsáním NDA.

K zajištění bezpečnosti informací a podpory bezpečnosti informací ve Společnosti se tímto dokumentem:

- popisuje a vysvětluje bezpečnost informací prosazovaná v ICT/IS
- stanovují bezpečnostní cíle pro ICT/IS
- stanovuje rozsah a důležitost bezpečnosti informací zpracovávaných v rámci ICT/IS
- uvádí stručný výklad základních bezpečnostních zásad a opatření v rámci ICT/IS.

Hlavním bezpečnostním cílem Společnosti pro ICT/IS je zajištění utajení, integrity a dostupnosti Aktiv ICT/IS. Definice tohoto cíle je v následujícím přehledu:

- **Důvěrnost** (confidentality) – zajištění, že informace jsou přístupné pouze těm, kteří jsou k přístupu oprávnění.
- **Integrita** (integrity) – zajištění správnosti a úplnosti informací a metod jejich zpracování.
- **Dostupnost** (availability) – zajištění, že informace je pro oprávněné Uživatele přístupná v okamžiku její potřeby.

Primárním cílem všech Aktivit v oblasti prosazování bezpečnostní politiky je zajištění utajení, integrity a dostupnosti všech zpracovávaných informací přiměřeným a efektivním způsobem. Bezpečnostním cílem spojeným s bezpečností informací ve Společnosti je zajištění dostupnosti informačních Aktiv jen oprávněným osobám, správnosti a kompletnosti informací, důvěrnosti a bezpečnosti jejich zpracování a ochrany informací proti náhodnému nebo neoprávněnému zničení nebo náhodné ztrátě, proti neoprávněnému přístupu, změnám nebo šíření, a to v souladu se zákony a jinými právními předpisy ČR. Tyto cíle lze naplnit jen za aktivního přispění všech Uživatelů.

Přiměřenost a efektivnost je v tomto dokumentu chápána jako míra ochrany poskytovaná informacím a celému ICT/IS, která musí být úměrná jejich hodnotě a předpokládaným hrozbám, kterým jsou vystaveny. Bezpečnostní opatření musí být realizována vhodným způsobem tak, aby bylo dosaženo dostatečné bezpečnosti s optimálními náklady. Pro zajištění efektivní ochrany je ve společnosti budován systém řízení bezpečnosti informací (ISMS) dle požadavků norem ISO/IEC 27001:2013 – ISO/IEC 27002:2013.

D.1.2 Rozsah platnosti Bezpečnostní politiky ICT/IS

Tento dokument je závazný pro všechny Uživatele a třetí strany pracující s Aktivy ICT/IS Společnosti. Odpovědnost za dodržování a prosazování stanovených opatření na pracovišti mají vedoucí zaměstnanci. Bezpečnostní pravidla se vztahují rovněž na všechny další subjekty (třetí strany), které jakkoliv pracují s Aktivy Společnosti. Dodržení této směrnice je vyžadováno tam, kde dochází ke zpracování a uchovávání informací Společnosti nebo tam, kde jsou dislokovány prostředky ICT/IS v majetku Společnosti. Příkladem těchto prostor jsou např. místnosti Uživatelů, datová centra (DC), prostory Service Desku a ostatní prostory společnosti. Za revizi a změny této politiky a postupů v ní uvedených zodpovídá ve Společnosti Ředitel, Informační technologie.

Směrnice pokrývá politiku práce s informacemi v ICT/IS zpracovávaných elektronickou formou. Týká se rovněž informací umístěných na datových, papírových, magnetických nebo jiných nosičích používaných pro potřebu ICT/IS např. vytištěné mapy sítě s adresními rozsahy, USB flash disky s konfigurací koncového zařízení atd. Předmětem ochrany je rovněž informace přenášena v počítačových sítích a dalších komunikačních zařízeních. Ustanovení tohoto dokumentu jsou tedy platná i pro informace přenášené pomocí mailů, smartphonů atd.

D.1.3 Prosazování bezpečnostní politiky ICT/IS

Útvar IT a Společnost stanovuje vydáním dokumentu jasný směr pro naplňování požadavků informační bezpečnosti a demonstruje tak svou podporu a závazky pro naplnění požadavků bezpečnostní politiky ICT/IS.

Po uplynutí nejdéle dvou let bude obsah tohoto dokumentu znovu vyhodnocen a revidován bezpečnostním výborem ICT/IS tak, aby byla zajištěna aktuálnost bezpečnostní politiky ICT/IS. Kontrola přijatých bezpečnostních opatření přispívá k důslednému prosazování bezpečnostní politiky v rámci ICT/IS. Kontrolu a všechny změny iniciuje bezpečnostní výbor ICT/IS. Průběžná aktualizace a zdokonalování pravidel tohoto dokumentu a dalších návazných dokumentů se provádí na doporučení bezpečnostního výboru ICT/IS.

Zajištění shody reality s bezpečností politikou je popsáno v kapitole D.12.5 Zajištění shody.

D.1.3.1 Nezávislé hodnocení stavu bezpečnosti ICT/IS

Aplikování všech požadovaných bezpečnostních opatření v ICT/IS je posuzováno Vedoucím vnitřního auditu, specializovaným odborníkem nebo autoritou alespoň 1x za dva roky formou auditu jednotlivých částí ICT/IS. Auditora a rozsah auditu schvaluje bezpečnostní výbor. Dle požadavku norem rodiny ISO/IEC 27000 Společnost udržuje plán auditů schválený bezpečnostním výborem ICT/IS.

D.1.3.2 Prosazování informační bezpečnosti v rámci IT projektového řízení

Společnost užívá vlastní metodiku vedení projektů popsanou v dokumentu „*Metodika vedení IT projektů*“. Tato metodika obsahuje a definuje požadavky na řešení bezpečnostních opatření v rámci projektu. V rámci životního cyklu projektového řízení je pro každý projekt definována sada bezpečnostních zásad a opatření aplikovaných v rámci celého životního cyklu projektu. Tato bezpečnostní opatření jsou navrhována na základě analýzy rizik projektu. Výsledky analýzy rizik schvaluje Bezpečnostní architekt. Analýza rizik je prováděna na základě nadřazené dokumentace viz kapitola B a dokument „*Řízení rizik v NET4GAS, s.r.o.*“ Katalog rizik ze všech projektů a analýz udržuje a spravuje Specialista, Kvalita a bezpečnost IT v rámci procesu ISMS.

V rámci jednotlivých fází projektu se prosazují požadavky na bezpečnost informací. Výstupem fází projektu musí být seznam požadovaných opatření na zajištění utajení, integrity a dostupnosti informací, zpracovávaných v projektu. Za prosazování bezpečnostních opatření je zodpovědný Ředitel, Informační technologie, který může delegovat konkrétní zodpovědnosti na pracovníky útvaru IT. Za koordinaci bezpečnostních opatření mezi projekty je zodpovědný Bezpečnostní architekt.

D.2 Politika organizační bezpečnosti

D.2.1 Popis subjektů podílejících se na prosazování bezpečnosti v ICT/IS

Tento dokument definuje hlavní zásady a pravidla pro prosazování bezpečnostní politiky Společnosti v ICT/IS. Společnost definuje v tomto dokumentu základní povinnosti a pravomoci uživatelů, dodavatelů, poskytovatelů služeb a třetích stran pracujících v prostředí ICT/IS. Bezpečnostní opatření jsou v praxi prosazována všemi Uživateli ICT/IS pracujícími s Aktivy Společnosti. Za oblast prosazování bezpečnosti informací je primárně zodpovědný vrcholový orgán Bezpečnostní výbor ICT/IS.

D.2.1.1 Uživatelé Informačních Aktiv

Všichni Uživatelé používající Aktiva ICT/IS Společnosti mají povinnost a pravomoc:

- dodržovat ustanovení této směrnice a návazných metodických pokynů či dalších odkazovaných dokumentů,
- hlásit veškeré bezpečnostní incidenty prostřednictvím Service Desku Společnosti,
- mít jen určené pravomoci a takové přístupy k informacím, které nezbytně potřebují pro výkon své funkce,

- vykonávat další činnosti vyplývající z nadřazené a navazující bezpečnostní dokumentace, zejména interního řídicího dokumentu „*Metodický pokyn IT-SECPOL pro Uživatele*“,
- každý zaměstnanec má právo i povinnost podávat náměty na zlepšení a předcházení rizik v oblasti bezpečnosti informací.

D.2.1.2 Útvar Procesy a organizace, bezpečnost, ŽP

Ve vztahu k této směrnici má tento útvar následující práva a povinnosti:

- vykonává odbornou, metodickou a kontrolní činnost v oblasti zajištění ochrany informací v souladu s nadřazenou bezpečnostní dokumentací,
- sleduje příslušnou legislativu a aktualizuje nadřazenou bezpečnostní dokumentaci v návaznosti na změny; informuje dotčené zaměstnance/Uživatele o dopadech změny legislativy,
- je oprávněn provádět kontrolu dodržování pravidel stanovených v této směrnici,
- je oprávněn provádět audity a prověrky v ICT/IS, tyto prověrky schvaluje jednatel s příslušnou kompetencí na základě požadavku vedení útvaru Procesy a organizace, bezpečnost a ŽP,
- pravomoc stanovit závazné opatření, o tomto opatření reportuje jednatelům Společnosti,
- spravuje bezpečnostní incidenty v oblasti ochrany informací.

D.2.1.3 Útvar IT

Útvar IT je zodpovědný za prosazování bezpečnosti v rámci ICT/IS. Do jeho kompetencí spadá:

- zajištění podpory strategie Společnosti v návaznosti na bezpečnostní politiku platnou pro Společnost, kterou realizuje na základě potřeb strategického rozvoje a vývojových trendů v oblasti IT,
- realizuje strategie v oblasti informatiky,
- identifikace příležitostí, iniciace rozvojových projektů a zajišťování bezpečnostních opatření pro provoz informačního systému,
- zajišťování informační podpory pro jednotlivé procesy Společnosti efektivním využitím dostupných informačních technologií,
- zodpovídá za řízení dodavatelsko-odběratelských vztahů s Dodavateli,
- řízení požadavků na nákup (vlastní nákup je realizován útvarem centrálního nákupu), testování a schvalování všech komponent připojovaných do ICT/IS,
- zabezpečení správy, provozu a rozvoje stávajících informačních systémů,
- zajišťuje prosazování bezpečnosti ICT/IS v rámci prováděných projektů,
- zajišťuje vypracování a testování plánů obnovy funkčnosti ICT/IS,
- spolupracuje s dalšími organizacemi a dodavateli v otázkách bezpečnosti ICT/IS,
- sestavuje Incident Response Team – IRT pro řešení bezpečnostních incidentů.

D.2.1.4 Bezpečnostní výbor ICT/IS

Bezpečnostní výbor ICT/IS (výbor pro řízení kybernetické bezpečnosti) je zodpovědný za oblast prosazování bezpečnosti informací v ICT/IS. Bezpečnostní výbor ICT/IS má na starosti rozvoj a schvalování celkové koncepce prosazování bezpečnostních opatření v ICT/IS. Bezpečnostní výbor nevykonává každodenní operativní činnosti související s bezpečnosti ICT/IS. Ty jsou delegovány na další subjekty a role. Bezpečnostní výbor ICT/IS zřizují a schvalují jednatelé Společnosti. Bezpečnostní výbor ICT/IS skládající se z definovaných zástupců Společnosti viz příloha. Členové výboru mají dostatečné znalosti z řízení bezpečnosti informací a mají adekvátní technické znalosti včetně porozumění chodu ICT/IS ve Společnosti. Bezpečnostní výbor ICT/IS má následující zodpovědnosti a vykonává následující role:

- Definuje strategii a koncepci aplikování bezpečnostních opatření v ICT/IS,
- Plánuje nasazení nových komponent ICT/IS ve Společnosti,
- Spravuje a řídí systém řízení bezpečnosti informací v ICT/IS
- Definuje pravidla a procedury pro řízení bezpečnosti ICT/IS v ICT/IS

- Definuje a schvaluje plán auditu jednotlivých částí ICT/IS.

Bezpečnostní výbor ICT/IS se skládá z klíčových pracovníků ICT/IS a má toto složení stálých členů:

- Vedoucí výboru – Ředitel, Informační technologie
- Zástupce vedoucího výboru – Manažer, IT infrastruktura
- Koordinátor obnovy ICT/IS
- Architekt kybernetické bezpečnosti
- Specialista, Kvalita a bezpečnost IT

Na každé jednání Bezpečnostního výboru ICT jsou přizváni následující členové, jejichž přítomnost na jednání výboru je dobrovolná:

- Manažer bezpečnosti informací (Manažer kybernetické bezpečnosti)
- Manažer, SCADA provozní technologie
- Vedoucí interní auditor (Auditor kybernetické bezpečnosti)

Dle potřeby mohou být jmenování do bezpečnostního výboru i další Zaměstnanci nebo Uživatelé ICT/IS. Minimální počet členů bezpečnostního výboru ICT/IS je 3 a doporučený počet je 5. Bezpečnostní výbor se schází v pravidelných intervalech dle potřeby alespoň 1x za 3 - 6 měsíců.

D.2.1.5 Vrcholné vedení Společnosti / jednatelé

Jednatel Společnosti má ve vztahu k této směrnici následující práva a povinnosti:

- schvaluje znění této směrnice a její aktualizace,
- pověřuje útvar IT nastavením, udržováním a kontrolou dodržování pravidel stanovených touto směrnicí,
- schvaluje kontroly dle plánu předloženého vedením útvaru Procesy a organizace, bezpečnost a ŽP a útvaru Informační technologie,
- je oprávněn nařídit provedení mimořádného auditu bezpečnosti.

D.2.2 Role a jejich odpovědnosti v oblasti zabezpečování informací v ICT/IS

V následujícím přehledu je uveden seznam rolí, mezi něž je rozdělena odpovědnost za prosazování bezpečnostních opatření v ICT/IS.

D.2.2.1 Ředitel, Informační technologie

Ředitel, Informační technologie vykonává funkci vedoucího Bezpečnostního výboru ICT/IS. Zodpovídá za prosazování bezpečnostních opatření v rámci ICT/IS. Deleguje zodpovědnosti za prosazování bezpečnosti ICT/IS.

D.2.2.2 Manažer, IT infrastruktura

Manažer, IT infrastruktura vykonává funkci zástupce vedoucího bezpečnostního výboru ICT/IS. Zodpovídá za prosazování bezpečnostních opatření v rámci ICT/IS. Deleguje zodpovědnosti za prosazování bezpečnosti ICT/IS mezi správce a aplikační správce.

D.2.2.3 Specialista IT, Kvalita a bezpečnost IT

Specialista, Kvalita a bezpečnost IT zodpovídá za formální obsah bezpečnostní dokumentace útvaru IT a její návaznost. Role je vykonávána pracovníkem útvaru IT. Zajišťuje naplňování požadavků ISMS dle norem ISO/IEC 27001:2013 - ISO/IEC 27002:2013 v rámci útvaru IT např. udržuje katalog rizik.

D.2.2.4 Vedoucí interní auditor / Auditor kybernetické bezpečnosti

Vedoucí interní auditor (Auditor kybernetické bezpečnosti v terminologii zákona o kybernetické bezpečnosti) provádí pravidelné a nepravidelné kontroly, revize a audity dodržování bezpečnostních zásad a opatření v ICT/IS. Tato role je vykonávána osobou mimo útvar IT společnosti NET4GAS, s.r.o.

D.2.2.5 Architekt kybernetické bezpečnosti

Architekt kybernetické bezpečnosti zajišťuje a zodpovídá za propojování Aktiv ICT/IS, Aplikací a jejich částí. Tato role odpovídá za návrh a implementaci bezpečnostních opatření, požadavků na bezpečnost předávaných dat, rozhraní, klasifikaci ICT/IS komponent apod.

D.2.2.6 Koordinátor obnovy ICT/IS

Koordinátor obnovy ICT/IS zajišťuje plánování, koordinace a řešení krizových situací v ICT/IS. Zodpovídá za vypracování, obsah a testování plánů obnovy v rámci ICT/IS.

D.2.2.7 Manažer bezpečnosti informací / Manažer kybernetické bezpečnosti

Manažer bezpečnosti informací (Manažer kybernetické bezpečnosti v terminologii zákona o kybernetické bezpečnosti) je osoba odpovědná za systém řízení bezpečnosti informací a zodpovídá za prosazování systému řízení bezpečnosti informací v celé Společnosti. Role je vykonávána specialistou útvaru Procesy a organizace, bezpečnost a ŽP. Tato role definuje systém práce s klasifikovanými informacemi dle požadavků nadřazené dokumentace.

D.2.2.8 Správce

Chod ICT/IS je zajištěn a podporován aktivní činností správců, kteří jsou zodpovědní za svěřené komponenty nebo části ICT/IS. Správci zajišťují provoz a údržbu svěřených systémů a aplikací v ICT/IS. Správci rovněž definují a odpovídají za archivaci a zálohování dat ve svěřených systémech a aplikacích. Správci mohou tuto aktivitu delegovat na třetí osobu. Správci udržují a zajišťují nastavenou konfiguraci bezpečnostních systémů ve svěřených aplikacích a komponentách ICT/IS. Správci mají obvykle přístup ke všem datům uloženým v informačním systému nebo alespoň fyzický přístup k zařízením, pomocí nichž jsou tato data zpracovávána. Správci jsou zodpovědní za bezpečnost svěřené komponenty ICT/IS. Role správců je v této směrnici rozdělena na následující: Správce infrastruktury, Správce aplikací, Správce SCADA. V tomto dokumentu jsou tyto role kumulovány do pojmu „správce/správci“. Role správce může být vykonávána externím nebo interním subjektem nebo zajištěna jako služba u třetí strany.

D.2.2.8.1 Správce infrastruktury

Správce infrastruktury je správce vykonávající správu serverů, sítí, diskových úložišť a dalších Aktiv ICT/IS. Tato role je vykonávána zaměstnanci nebo třetími stranami na funkcích správců např. Správce systému, Správce sítě, Správce databáze. V dalším textu jsou označeni obecným pojmem „Správce infrastruktury“. Role správce infrastruktury může být vykonávána i osobami, které nejsou zaměstnanci Společnosti.

D.2.2.8.2 Správce aplikací

Správce aplikací (aplikační správce) - tato role má na starosti specifické činnosti pro zajištění chodu svěřených aplikací např. vykonávají aplikační dohled, rozvoj aplikací, správu databází, podporu uživatelů aplikace, zálohování dat, přidělují přístupová práva do aplikace, provádí kontrolu aplikačního auditu atd. Role správce aplikace může být vykonávána i osobami, které nejsou zaměstnanci Společnosti.

D.2.2.8.3 Správce SCADA

Správce SCADA - vykonávající správu Řídicího systému a SCADA technologií.

D.2.2.9 Uživatel

Role Uživatele je vykonávána zaměstnanci Společnosti a ostatními uživateli pracujícími s Aktivy v ICT/IS. Jeho odpovědnosti jsou vymezeny v této směrnici a v „*Metodickém pokynu IT-SECPOL pro Uživatele*“.

D.2.2.10 Klíčový uživatel

Role Klíčový uživatel je vykonávána zaměstnanci Společnosti pracujícími s Aktivy v ICT/IS daného útvaru. Tato role pomáhá s rozvojem aplikace, schvaluje plánované výpadky, komunikuje s ostatními uživateli dané aplikace, schvaluje přístupová práva k příslušné aplikaci atd.

D.2.2.11 Vlastník Aktiva / Garant aktiva

Role Vlastník Aktiva (Garant aktiva v terminologii zákona o kybernetické bezpečnosti) zodpovídá za daný typ nebo skupinu informací nebo svěřenou komponentu ICT/IS. Vlastník rozhoduje o klasifikaci daného Aktiva. Přidělování přístupových práv k Aktivu může a také zpravidla provádí Správce pro vlastníka Aktiva.

D.2.3 Oddělení a omezení kumulace jednotlivých rolí

Odpovědnosti v ICT/IS jsou pomocí rolí rozděleny tak, aby žádný subjekt nemohl získat kompletní kontrolu nad zpracováním klasifikovaných informací v Aktivech ICT/IS Společnosti. Pro zajištění požadovaného dělení odpovědnosti je třeba obecně zajistit dodržování následujících zásad:

- Role správce aplikace se nesmí kumulovat s rolemi správců, spravujících infrastrukturní komponenty ICT/IS např. servery, síť, disková úložiště.
- Uživatel nesmí mít v aplikaci možnost nastavovat práva přístupu sám sobě. Definici práv v aplikacích zajišťuje správce aplikace.
- Správci aplikací nesmí vykonávat správu operačního systému serverů zajišťujících chod svěřené aplikace.
- Manažer, IT Infrastruktura definuje rozdělení odpovědnosti mezi správce zodpovídající za infrastrukturní komponenty ICT/IS např. sítě, servery, disková úložiště, virtualizační prostředí atd. Minimální počet správců infrastrukturních komponent ICT/IS je 3. Žádný správce nesmí mít administrátorská práva ke všem infrastrukturním komponentám ICT/IS ve Společnosti.
- Správa Aktiv ICT/IS je vykonávána různými správci. Každý správce se stará o jinou skupinu Aktiv ICT/IS. Mezi správci je zajištěna vzájemná zastupitelnost v rámci útvaru IT. Činnost správců je monitorována pomocí automatizovaného nástroje dohledu.
- Správa Řídicích systémů pro přepravu plynu je vykonávána jinými správci, než jsou správci sítě.
- Správci vykonávající dohled pomocí monitorovacího systému nesmí vykonávat správu v Řídicích systémech pro přepravu plynu.
- Role správců jednotlivých komponent ICT/IS může být delegována na externí subjekty.

Uvedený souhrn rozvržení odpovědností se může doplňovat nebo měnit na základě rozhodnutí bezpečnostního výboru ICT/IS. Útvar IT zajišťuje automatizované odesílání bezpečnostních logů na definovaná úložiště mimo Aktivum ICT/IS, kde byl log pořízen. Na toto definované úložiště nemají přístup správci, kteří vykonávají správu Aktiva ICT/IS, na kterém byly logy pořízeny. Centrální monitorovací systém sleduje rovněž Aktivity správců. Rozsah monitorování činnosti správců definuje Manažer, IT infrastruktura.

Pro Řídicí systém a SCADA technologie jsou pravidla oddělení a kumulace jednotlivých rolí uvedená v této kapitole pouze na úrovni doporučení. Řídicí systém a SCADA technologie mají svá specifika a jejich vlastní vyšší zabezpečení je zajištěno prostřednictvím jiných sofistikovanějších pravidel, mechanismů, technologií a opatření popsaných v samostatném metodickém pokynu pro Řídicí systém a SCADA technologie.

D.3 Politika řízení dodavatelů

Pravidla a principy výběru, hodnocení, kontroly dodavatelů včetně smluvních náležitostí jsou v odpovědnosti útvaru centrálního nákupu a jsou definovány nadřazenou bezpečnostní dokumentací. Z dílčího pohledu vlastního technického zajištění bezpečnosti informací v rámci ICT/IS jsou pravidla a povinnosti Dodavatelů popsána v návazných metodických pokynech tj. zejména v „*Metodickém pokynu IT-SECPOL pro Dodavatele*“ a „*Metodickém pokynu IT-SECPOL pro Uživatele*“.

Poznámka: dodavatel (s malým d) = libovolný dodavatel Společnosti. Dodavatel (s velkým D) = zjednodušeně „IT dodavatel“ viz kapitola C nazvaná Definice pojmů a zkratek.

Cílem bezpečnostních opatření v této kapitole a navazujících dokumentech je snížení rizik a zvýšení zajištění bezpečnostních opatření u Aktiv ICT/IS, ke kterým mají přístup Dodavatelé. Činnost útvaru IT je ve velké míře závislá na podpoře Dodavatelů, protože útvar IT má jen nezbytně nutný počet zaměstnanců Společnosti. V následujícím přehledu je uveden seznam zodpovědností útvaru IT:

- Útvar IT zodpovídá za řízení dodavatelsko-odběratelských vztahů s Dodavateli.
- Útvar IT zodpovídá za kontrolu kvality Dodavatelem poskytovaných služeb.
- Útvar IT zodpovídá za definování bezpečnostních opatření ve smlouvách s Dodavateli.
- Útvar IT zodpovídá za poskytování potřebných informačních Aktiv ICT/IS Dodavatelům.
- Útvar IT zodpovídá za správné začlenění Dodavatele do procesů útvaru IT.
- Útvar IT zodpovídá za provozování nástrojů pro kontrolu a řízení SLA parametrů smluv s Dodavateli.
- Útvar IT zodpovídá za management změn u služeb zajišťovaných Dodavateli.

Za ostatní činnosti odpovídají další útvary Společnosti, se kterými útvar IT spolupracuje.

D.4 Politika klasifikace Aktiv

Účelem klasifikace a řízení Informačních Aktiv je udržovat přiměřenou ochranu Informačních Aktiv.

Primární aktiva Společnosti jsou určena, hodnocena/klasifikována, evidována a řízena dle nadřazené bezpečnostní dokumentace. Klasifikace Primárních aktiv určuje způsob zacházení s informacemi s ohledem na jejich ochranu. Informační Aktiva Společnosti musí být klasifikována tak, aby byla určena jejich potřebnost, důležitost a stupeň ochrany při manipulaci s nimi. Klasifikaci stanoví vlastníci Informačních Aktiv, kteří odpovídají i za periodické přezkoumávání této klasifikace a její aktualizaci. Pravidla pro klasifikaci definuje nadřazená bezpečnostní dokumentace.

Podpůrná aktiva v rámci ICT/IS jsou určena a evidována útvarem IT. Vazba mezi primárními a podpůrnými aktivy je útvarem IT pravidelně vyhodnocována, tak aby byla zajištěna konzistence ochrany Podpůrných aktiv v souladu s aktuálními Primárními aktivy.

Aktiva ICT/IS (viz definice v kapitole C) jsou Aktiva v přímé odpovědnosti útvaru IT či jeho pracovníků.

D.4.1 Inventarizace a evidence Aktiv ICT/IS

Jednotlivá Aktiva ICT/IS musí být řádně evidována a inventarizována. Pro každé důležité Aktivum ICT/IS se definuje a stanoví jeho garant/vlastník. Jde zejména o:

- Informační Aktiva: databáze a datové soubory, systémová dokumentace, uživatelské manuály, školící materiály, provozní nebo podpůrné procedury, havarijní plány a podobně.
- Programová Aktiva: aplikační programové vybavení, systémové programové vybavení, vývojové nástroje, utility a podobně.
- Fyzická Aktiva: počítače a komunikační zařízení, magnetická média (pásky a disky), další technická zařízení (napájecí zdroje, klimatizační zařízení), nábytek, prostory a podobně.
- Služby: počítačové a komunikační služby, další technické a podpůrné služby (topení, osvětlení, napájení, klimatizace a podobně).

Útvar IT udržuje přehled o důležitých Aktivech ICT/IS (dále označeno jako „Hlavní Aktiva ICT/IS“) ve formě souborů a tabulek uložených na definovaném úložišti útvaru IT. Všechna zařízení ICT/IS jsou rovněž vedena v centrální evidenci společnosti a jsou v případě potřeby označena štítkem nebo popisem. Všechna zařízení v ICT/IS musí být vybavena jedinečným označením (identifikátorem), tak aby mohla být řádně a efektivně provedena fyzická inventura. Za toto označení zodpovídá pověřená osoba Společnosti. V pravidelném intervalu 12 měsíců musí být kontrolovány identifikátory. Tuto kontrolu provádí pověřené osoby Společnosti.

D.4.2 Vlastníci Aktiv ICT/IS a jejich odpovědnost

Veškerá Aktiva ICT/IS musí mít určeného vlastníka - garanta, který je za ně zodpovědný. Převzetí Aktiva ICT/IS ve formě majetku stvrzuje Uživatel svým podpisem „*Protokolu o předání hmotného a nehmotného majetku*“ při převzetí informačního Aktiva. Součásti protokolu jsou následující informace:

- Evidenční číslo
- Název položky
- Výrobní číslo (pokud je relevantní povaze Aktiva ICT/IS)
- doba poskytnutí Aktiva
- místo uložení

Podpisem tohoto protokolu Uživatel potvrzuje, že převzal Aktivum ICT/IS a že byl seznámen s pravidly užívání tohoto Aktiva ICT/IS, a že těmto pravidlům plně porozuměl a s jejich dodržováním souhlasí. Stejným mechanismem probíhá předání či vrácení Aktiva ICT/IS jinému Uživateli či útvaru IT. V případě, kdy neexistuje či není dohledatelný předávací protokol k Aktivu ICT/IS, je za vlastníka daného Aktiva ICT/IS považován Ředitel, Informační technologie.

Uživatel je vyrozuměn, že s Aktivem ICT/IS musí zacházet v souladu s pravidly stanovenými v tomto dokumentu, návazných metodických pokynech a byl seznámen s bezpečností práce s IT technikou, bezpečnostními směrnicemi IT a s IT směrnicemi umístěnými na (http://intranet.net4gas.cz).

D.4.3 Klasifikace Informačních Aktiv

Pro účely indikace potřeb a priorit bezpečnostní ochrany se musí používat bezpečnostní klasifikace. V ICT/IS se zpracovávají různé druhy informací související s činností společnosti. Konkrétní forma zpracování je předpokládána ve formě souborů, tabulek, grafů, WWW stránek, objektů v databázi, fyzických dokumentů a jiných forem kancelářského zpracování. Protože některé informace je třeba zpracovávat s odlišnými bezpečnostními požadavky, jsou prosazovány pro informace různé formy bezpečnostních mechanismů na základě jejich dělení – klasifikace.

Klasifikace informací je jedním ze základních požadavků pro prosazování bezpečnosti v ICT/IS. Všechny informace a komponenty ICT/IT musí mít stanovenu úroveň klasifikace z hlediska utajení dle nadřazené bezpečnostní dokumentace. Nadřazená bezpečnostní dokumentace definuje následující klasifikační úrovně:

- „Veřejné“ – bez zkratky
- „Interní“ – zkratka II
- „Určené“ – zkratku UI
- „Strategické“ – zkratka SI

ICT/IS se také zpracovávají informace chráněné dle zákonů ČR např. Zákona o ochraně osobních údajů, Zákona o ochraně utajovaných skutečností a dalších zákonů.

Detailní popis uvedených klasifikačních stupňů obsahuje nadřazená bezpečnostní dokumentace zejména:

- „*Bezpečnostní pravidla pro ochranu informací*“
- „*Ochrana dat*“ - Metodický pokyn pro práci s klasifikovanou informací
- „*Bezpečnostní pravidla pro práci s výpočetní technikou*“

Všichni Uživatele jsou povinni dodržovat opatření platná pro daný klasifikační stupeň, a dbát zvýšené opatrnosti zejména při manipulaci s dokumenty stupně „Strategické“ a „Určené“ dle pokynů nadřazené bezpečnostní dokumentace.

D.4.4 Práce v ICT/IS s klasifikovanou informací stupně „Interní“ a vyšší

Při práci s klasifikovanými informacemi stupně „Interní“ a vyšší je třeba dodržovat následující postupy a zásady:

1. Za stanovení klasifikace je jednoznačně zodpovědný vlastník Informačního Aktiva, který musí stanovit klasifikaci Informačního Aktiva ihned při jeho vytvoření v ICT/IS. Informační Aktivum musí nést klasifikační návěští v záhlaví nebo na jiném viditelném místě.
2. Pokud během provozu informačního systému v minulosti vznikla množina dokumentů, u kterých není klasifikační návěští, je nutno i u těchto historických dokumentů/Informačních Aktiv navrhnout správně klasifikační stupeň. Za provedení klasifikace již existujících Informačních Aktiv v ICT/IS jsou zodpovědní vlastníci Informačních Aktiv.
3. Infrastruktura ICT/IS zajišťuje kontrolu přístupu ke všem Informačním Aktivům a nabízí doplňkové techniky pro ochranu Informačních Aktiv např. formou šifrování.
4. Před přístupem k informacím označeným klasifikačním návěštím Společnosti musí být Uživatelé proškoleni o bezpečnostních postupech a o následcích v případě, že by se klasifikované informace dostaly úmyslně nebo v důsledku nedbalosti do nepovolaných rukou. Parametry a způsob školení Uživatelů je definován směrnicí SM_I04_07_01.
5. Nadbytečné nebo vyřazené informační Aktiva, nebo jejich ICT/IS nosiče, včetně odpadu jako např. pokažených kopií, pracovních návrhů apod. jsou zničeny do nerozpoznatelné a nerekonstruovatelné podoby ve skartačních zařízeních. Skartovací zařízení pro skartaci CD, DVD je k dispozici na vybraných pracovištích. Pro potřeby likvidace a mazání informačních Aktiv v ICT/IS definuje Manažer IT infrastruktura povolené techniky a nástroje pro výmaz. Tyto nástroje následně schvaluje bezpečnostní výbor ICT/IS.
6. Aktivita Uživatelů během zpracování Informačních Aktiv v ICT/IS je monitorována útvarem IT. Bezpečnostní výbor ICT/IS schvaluje použití technických prostředků bezpečnostního auditu v ICT/IS.
7. Fyzické nosiče Informačních Aktiv nesoucích klasifikované informace nesmí být ponechány bez dozoru vlastníkem informačního Aktiva. Jejich přeprava se řídí nadřazenou směrnicí SM_I04_07_01. Klasifikovaná Informační Aktiva ICT/IS umístěná na fyzickém nosiči musí být šifrována pomocí šifrovacích technik schválených Bezpečnostním výborem ICT/IS.

D.5 Politika bezpečnosti lidských zdrojů

Politika bezpečnosti lidských zdrojů je definována nadřazenou bezpečnostní dokumentací. Následující podkapitoly řeší detailně problematiku bezpečnosti lidských zdrojů v kontextu ICT/IS.

D.5.1 Dohoda o dodržování mlčenlivosti

Veškeré subjekty a osoby pracující s Aktivy ICT/IS jsou povinny dodržovat zásady ochrany Aktiv ICT/IS Společnosti i po ukončení pracovního poměru nebo smluvního vztahu, po stanovenou dobu mlčenlivosti. V případě neuvedení konkrétní doby mlčenlivosti u konkrétní informace se za dobu mlčenlivosti považuje doba, dokud se nestanou veřejně známými. Doba mlčenlivosti může být upravena pracovní smlouvou pro konkrétního Zaměstnance, který musí stvrdit seznámení a souhlas s touto dobou svým podpisem.

D.5.2 Školení Uživatelů

Všichni Uživatelé musí být adekvátně proškoleni pro výkon své role v ICT/IS. Uživateli je zřízen přístup do ICT/IS a následně musí absolvovat školení alespoň formou e-learningu ukončené testem do 1 měsíce od získání přístupu. Bez proškolení a úspěšného absolvování testu bude Uživateli přístup následně odebrán. Uživatelé musí být vyškoleni v aplikaci bezpečnostních postupů a ve správném způsobu používání Aktiv ICT/IS alespoň 1x za 2 roky např. v rámci školení o bezpečnosti práce. Uživatel ICT/IS může absolvovat školení rovněž formou e-learningu. Každé školení je ukončeno výstupním testem a Uživatel musí splnit bodová kritéria testu. Toto školení může být prováděno přímo na pracovišti nebo u třetí strany. V případě, že se uživatel nezúčastnil školení nebo neabsolvoval školení formou e-learningu déle než 2 roky, bude mu zablokován přístup ke službám ICT/IS.

D.5.3 Ukončení pracovního poměru nebo změna pracovní pozice

Začlenění každého nového Uživatele do ICT/IS a jeho ukončení činnosti v ICT/IS je provázeno souhrnem organizačních a technických opatření prováděných útvarem IT. Řízení přístupu je popsáno v

kapitole D.7 nazvané Politika řízení přístupu v rámci ICT/IS. Při ukončení pracovního poměru musí Uživatel vrátit veškerá Aktiva ICT/IS, která mu byla poskytnuta útvarem IT.

Vždy, když je Uživatel nastálo přeložen na jinou funkci nebo pokud ukončil pracovní poměr, dochází k úpravě jeho oprávnění (odebrání či přidání oprávnění) a uživatelského účtu (případné zablokování či výmaz účtu). Při přeložení na jinou funkci provede útvar IT rekonfiguraci přístupových práv na základě nové žádosti o zajištění přístupu do ICT/IS. Tuto žádost zasílá na Service Desk nový nadřízený zaměstnanec Uživatele (v případě externího pracovníka zaměstnanec odpovědný za externího pracovníka). Schvalování požadovaných práv a přístupů probíhá hierarchicky v souladu s pracovním zařazením Uživatele a všechny žádosti o poskytnutí práv schvaluje přímý nadřízený Uživatele ICT/IS v rámci rozsahu své kompetence. Konkrétní postup přidělování a odebírání přístupových práv do ICT/IS je popsán v kapitole D.7 nazvané Politika řízení přístupu v rámci ICT/IS.

D.5.4 Pravidla pro řešení případů porušení Bezpečnostní politiky ICT/IS

Nedodržení zásad bezpečnosti informací a zásad i opatření popsaných v této politice Uživatelem je považováno za porušení povinností vyplývajících z právních předpisů České Republiky a řídí se zákoníkem práce nebo dalšími smluvními vztahy s třetími stranami. Porušení těchto zásad či opatření zaměstnancem Společnosti je mimo jiné chápáno jako hrubé porušení pracovních povinností vyplývajících z právních předpisů vztahujících se k zaměstnancem vykonávané práci.

V případě, že identifikováno porušení Bezpečnostní politiky ICT/IS, tak je postupováno dle následujících pravidel:

I. Každé porušení Bezpečnostní politiky ICT/IS musí být:
   a. Řádně evidováno
   b. Projednáno na Bezpečnostním výboru při jeho nejbližším zasedání

II. Bezpečnostní výbor ke každému porušení Bezpečnostní politiky ICT/IS navrhne přiměřenou reakci na toto porušení spočívající typicky v protiopatření a/nebo sankci.
   a. V případě, kdy je schválení reakce v kompetenci Bezpečnostního výboru, tak Bezpečnostní výbor společně s návrhem zároveň návrh/reakci schvaluje k realizaci.
   b. V případě, kdy schválení navržené reakce překračuje kompetence Bezpečnostního výboru, tak je Bezpečnostní výbor jako orgán odpovědný za zajištění řádného průchodu schvalováním procesem odpovědné autority a eskalaci odpovědné autoritě.

III. V případě porušení Bezpečnostní politiky ICT Uživatelem bude tomuto Uživateli útvarem IT do řádného projednání Bezpečnostním výborem maximálně možným způsobem omezen přístup k ICT/IS s ohledem na zajištění cílů Společnosti (tj. omezení nemusí být totální např. v případě, pokud by totálním omezením přístupu vznikla Společnosti větší škoda/riziko než škoda/riziko způsobené původním porušením Bezpečnostní politiky ICT/IS).

IV. V rámci porušení Bezpečnostní politiky Dodavatelem se postupuje obdobným způsobem jako v případě porušení Uživatelem.

V. Každé porušení Bezpečnostní politiky ICT/IS Dodavatelem či Uživatelem bude nejpozději v okamžiku schválení přiměřené reakce (viz bod II.) hlášeno:
   a. odpovědné osobě (typicky zaměstnanci) v rámci Společnosti tj. nadřízenému Uživatele či odpovědné osobě za Dodavatele a
   b. odpovědnému útvaru v rámci společnosti tj. v případě zaměstnance útvaru odpovídajícímu za Lidské zdroje a v případě dodavatele útvaru odpovídajícímu za centrální nákup.

D.6 Politika řízení provozu a komunikací ICT/IS

Účelem politiky řízení bezpečnosti provozu a komunikací je zajistit správný a bezpečný provoz Aktiv ICT/IS pro zpracování informací, minimalizovat riziko selhání systému, chránit integritu a dostupnost programů, dat a ICT/IS, chránit důvěrnost informací a zajistit adekvátní ochranu počítačových sítí. Pro splnění uvedených cílů je v ICT/IS aplikována sada bezpečnostních opatření popsána v následujících

podkapitolách. Útvar IT je zodpovědný za sadu procesů zajišťujících efektivní chod ICT/IS. Procesy jsou shrnuty v následujícím přehledu:

- Proces vytváření a udržování řízené dokumentace ICT/IS
- Proces plánování a provádění změn v ICT/IS.
- Proces kapacitního plánování ICT/IS.
- Proces rozvoje ICT/IS.

Útvar IT průběžně vyhodnocuje efektivitu a kvalitu jednotlivých procesů souvisejících s provozováním a užíváním ICT/IS, včetně citlivostní analýzy. Navrhuje změny zaměřené na zvyšování kvality, bezpečnosti a ekonomické efektivity jednotlivých procesů.

D.6.1 Provozní dokumentace, směrnice a zodpovědnosti

Součástí ICT/IS jsou závazné postupy řízení jeho rozvoje, správy, údržby, provozování, užívání a krizového řízení, jejichž popis je součástí navazujících směrnic a souvisejících metodických pokynů viz kapitola B. Pro řízení a provoz všech Aktiv ICT/IS jsou útvarem IT ustanoveny provozní postupy a adekvátní přidělení zodpovědnosti za prosazování těchto postupů. Veškerá dokumentace s IT směrnicemi je umístěna na (http://intranet.net4gas.cz).

Pro zabezpečení provozu všech Aktiv ICT/IS existují písemné směrnice, metodické pokyny, nařízení a procedury, s kterými se musí seznámit definovaní Správci. Jsou zavedeny postupy pro plánování a provádění změn v ICT/IS. Za změny a jejich provádění je zodpovědný útvar IT.

D.6.2 Řízení změn ICT/IS

Požadavek na změnu je vyhodnocen útvarem IT z ekonomického hlediska, z pohledu strategie informatiky, citlivostní / bezpečnostní analýzy, závazných architektur a standardů. Všechny změny musí projít procesem plánování, schvalování a testování (procesy jsou popsány separátními dokumenty viz kapitola B). Rozhodnutí o schválení či zamítnutí požadavku změny je v kompetenci Ředitele, Informační technologie a Manažera, IT Infrastruktura. V rámci tohoto procesu je zavedeno aplikování urgentní změny, která může být aplikována při výskytu mimořádné situace nefunkčnosti Aktiv ICT/IS.

Změny v aplikací jsou řízeny standardním procesem viz kapitola D.11.5 nazvaná Postupy pro řízení změn při vývoji a změn aplikací. V průběhu nebo po ukončení definice funkčních nebo technických specifikací musí být provedeno hodnocení citlivosti aplikace a z toho plynoucí návrh bezpečnostních opatření v nově vyvíjené aplikaci.

Správci systému musí zdokumentovat všechny změny konfigurace Hlavních Aktiv ICT/IS. Je zavedeno řízení dokumentace změn v konfiguraci ICT/IS pro různé skupiny Aktiv ICT/IS. O provedených změnách musí být vyrozuměni ostatní správci.

D.6.3 Plánování kapacity

Útvar IT provádí dlouhodobé plánování kapacit Hlavních Aktiv ICT/IS. Cílem tohoto plánování je zajistit s předstihem adekvátní a dostatečnou rezervu výkonu služeb ICT/IS. Hlavní Aktiva nesmí být kapacitně dlouhodobě přetěžována přes 80 procent a vždy musí být zajištěna částečná rezerva výkonu a kapacity Aktiv ICT/IS. Správci monitorují využití Aktiv ICT/IS pomocí dohledových nástrojů. Cílem tohoto monitorování je zabránit selhání částí ICT/IS vinou nedostatečné kapacity Aktiv ICT/IS. K tomuto účelu používají správci dohledový systém umožňující nastavení různých prahových úrovní a přepínačů s možností automatického vyrozumívání správců pomocí mailů/SMS při jejich překročení. Správci pravidelně informují Manažera, IT infrastruktura o využívání jim svěřených Aktiv a poskytují mu grafy a statistiky o využití kapacit jednotlivých Aktiv ICT/IS v čase.

V rámci tohoto procesu je řešena i sada doplňkových opatření dle následujícího seznamu:

- pravidelné mazání zastaralých informací z diskových úložišť
- optimalizace databázových dotazů

- optimalizace aplikační logiky u aplikací, které spotřebovávají nepřiměřené kapacity
- optimalizace dávkového zpracování mimo období zatížení Aktiv
- používání nástrojů pro omezení vyčerpání přenosového pásma uživateli ICT/IS atd.

Za tyto činnosti jsou zodpovědní správci. Dlouhodobé plánování kapacit Hlavních Aktiv ICT/IS schvaluje Manažer, IT infrastruktura.

D.6.4 Oddělení vývojových, testovací a provozních prostředí

Vývojová a testovací prostředí jsou oddělena od provozních prostředí s Aktivy ICT/IS. Cílem tohoto oddělení je zabránit riziku neautorizovanému přístupu k informačním Aktivům nebo provedení neautorizovaných změn v provozním prostředí. Za tímto účelem jsou útvarem IT využívány postupy transferu software z vývojového do provozního prostředí, jejichž základní pravidla jsou popsané v „Metodice vedení IT projektů“. Tato oddělení i návazná opatření jsou závazné pro Hlavní Aktiva ICT/IS např. systém SAP a pro ostatní systémy je toto oddělení pouze doporučené.

Útvar IT zajišťuje vytvoření odděleného prostředí pro vývoj aplikací (pokud vývoj probíhá v prostředí Společnosti), testování aplikací a provoz aplikací a Aktiv ICT/IS. Vlastní testování může probíhat na Aktivech ICT/IS v útvaru IT nebo u Dodavatele. Před nasazením nových Aktiv ICT/IS musí proběhnout testování nových Aktiv ICT/IS v prostředí odděleném od provozního prostředí. O rozsahu testování rozhoduje útvar IT. Testovací prostředí se musí co nejvíce blížit reálnému provoznímu prostředí. Útvar IT může používat pro testování vzorky dat z provozního prostředí. Testovací provoz je ukončen teprve na základě úspěšných akceptačních a bezpečnostních testů. Jejich rozsah a formu definuje útvar IT před zahájením testovacího provozu. Výsledky testů musí schválit aplikační správce a klíčový uživatel, kteří jsou zodpovědní za danou aplikaci. Teprve po tomto souhlasu může být zahájen ostrý provoz v provozním prostředí.

Útvar IT rozhoduje o budování a implementování vývojového prostředí provozovaného útvarem IT. Pro některé aplikace musí útvar IT vytvořit oddělené prostředí i pro vývoj aplikace. Příkladem je prostředí SAP aplikací, které vyžadují oddělené vývojové, testovací a provozní prostředí. Transfer aplikací a dat z vývojového do testovacího prostředí a z testovacího do provozního prostředí je řízen aplikačním správcem daného modulu SAP. Teprve po otestování SAP aplikací klíčovým uživatelem v testovacím prostředí může být SAP aplikace předána do produkce.

Opatření pro vývojová a testovací prostředí:

a) Pro potřeby testování a vývoje se používají oddělená prostředí např. s dedikovaným hardwarem. nebo virtualizačními nástroji. Takto oddělené prostředí je následně poskytnuto aplikačním správcům pro vývoj a testování.
b) V provozním prostředí je použita pouze otestovaná verze software, hardware nebo aplikace. Změny jsou nejprve otestovány mimo provozní prostředí a výjimku z tohoto povinného testování může pro urgentní změny schválit pouze Ředitel, Informační technologie. Před uvedením nových Aktiv ICT/IS do trvalého provozu se musí provést otestování funkčnosti. Za testování je zodpovědný aplikační správce, správce nebo Dodavatel aplikace. Výsledky testování schvaluje i Klíčový uživatel, který bude následně používat Aktiva ICT/IS v provozním prostředí. Detailní pravidla pro přechod do produkčního či provozního prostředí a pro zahájení ostrého provozu jsou stanovena v projektové metodice Společnosti a navazujících dokumentech.
c) Testování v produkčním prostředí je možné pouze ve výjimečných případech a za výjimečných okolností vždy však pouze se souhlasem Ředitele, Informační technologie.
d) Vývojové nástroje a obecně funkčnosti pro vývoj by neměly být dostupné v provozním prostředí, pokud to není požadováno z nějakého jasně identifikovaného konkrétního důvodu.
e) Uživatelům je doporučeno pracovat v testovacím prostředí pod jiným uživatelským profilem než v produkčním prostředí (obsahově může být tento profil shodný) pro omezení možných chyb spočívajících v záměně testovacího a provozního prostředí. Zároveň je pro systémy umístěné do vývojového a testovacího prostředí doporučeno zobrazování jednoznačné identifikace či upozornění (např. TEST či DEV).
f) Data užívaná v testovacím či vývojovém prostředí musí být očištěna o citlivá data (tj. eliminace citlivých dat z testovacích a vývojových prostředí např. anonymizací osobních údajů či jiným odstraněním citlivých dat z pohledu legislativy i z pohledu Společnosti).

D.6.5 Ochrana proti škodlivému kódu a programům

Ve Společnosti se používá pouze schválený antivirový software. Antivirový software je používán pro odstranění a blokování škodlivého kódu a programů. Antivirový software je nainstalován na všech Aktivech ICT/IS určených útvarem IT. Výjimku může udělit pouze Manažer, IT infrastruktura. Útvar IT zajišťuje pravidelnou aktualizaci definic antivirového software a centrální management antivirového nástroje. Pravidelná aktualizace definic antivirového software je dostupná ve vnitřních sítích i z Internetu. Útvar IT je zodpovědný za zaškolení Uživatelů v používání antivirového software na pracovních stanicích. Za správnou konfiguraci antivirového software na serverech jsou zodpovědní správci. Správce může vypnout, či úplně odinstalovat antivirový SW, vyžádá-li si to provozní situace, resp. zajištění provozu ICT/IS. Správce daného Aktiva ICT/IS může rovněž nastavovat výjimky pro rezidentní štít a jeho pravidelnou kontrolu.

U SCADA systémů má správce systému SCADA přístup do konzole antivirového software a může zde měnit nastavení skupiny Aktiv ICT/IS pod kontrolou antivirového systému podle provozních potřeb.

D.6.6 Zaznamenávání událostí

Bezpečnostní logy se automatizovaně ukládají na koncovém zařízení nebo mimo něj. Správci provádí kontrolu aplikačních a systémových logů koncových zařízení dle provozních potřeb. Útvar IT zajišťuje automatizované odesílání logů na definovaná úložiště mimo Aktivum ICT/IS, kde byl log pořízen. Na toto definované úložiště nemají přístup správci, kteří vykonávají správu Aktiva ICT/IS, na kterém byly logy pořízeny. Centrální monitorovací systém sleduje rovněž Aktivity správců.

Útvar IT udržuje prostřednictvím Service Desku záznamy o provedených konfiguračních změnách a Aktivitách prováděných na koncových zařízeních. Rovněž provádí pravidelnou kontrolu logů a událostí z Aktiv ICT/IS dle potřeb pomocí centralizovaného monitorovacího systému. Nastavení tohoto monitorovacího systému schvaluje Manažer, IT infastruktura.

Chyby v konfiguraci Aktiv ICT/IS musí hlásit Uživatelé na ServiceDesk. Service Desk provede identifikaci chyby standardním procesem a přidělí provedení opravné akce konkrétnímu správci Aktiva ICT/IS. Systémy SCADA používají oddělený systém hlášení poruch a závad v oddělených aplikacích.

Útvar IT vytvořil postupy pro sledování využívání a zatížení Aktiv ICT/IS Správci mají povinnost sledovat a monitorovat jim svěřená Aktiva ICT/IS a zajišťovat zpětnou vazbu o využívání Aktiv ICT/IS. Aplikační správci provádí tuto činnost v jim svěřených aplikacích.

D.6.7 ICT/IS bezpečnostní audit

Všechna Hlavní Aktiva ICT/IS musí mít nakonfigurován a aktivován bezpečnostní audit. Za bezpečnostní opatření v této oblasti je zodpovědný útvar IT prostřednictvím správců. Bezpečnostní audit musí řešit sběr minimálně následujících událostí:

- Uživatelská a administrátorská přihlášení a odhlášení,
- Použití administrátorských práv,
- Použití práv bezpečnostního managementu např. změna členství ve skupinách, přidělení práv administrátora účtu atd.
- Vypnutí/zapnutí a změna konfigurace auditu

Útvar ICT/IS udržuje záznamy bezpečnostního auditu operačního systému serverů, operačního systému pracovních stanic, síťových prvků a útvarem IT stanovených dalších koncových zařízení po útvarem IT definovanou minimální dobu. Tato doba je stanovena pro jednotlivé kategorie Aktiv ICT/IS a může se lišit pro různé části ICT/IS.

Konfigurace auditu jednotlivých Aktiv ICT/IS je útvarem IT prověřována pro Hlavní Aktiva ICT/IS alespoň 1x ročně.

D.6.8 Synchronizace strojových hodin

Strojový čas v koncových zařízeních musí být centrálně synchronizován vůči schválenému zdroji času v Internetu. Tato synchronizace je zajištěna prostřednictvím domény Windows, kde je definován centrální etalon času tj. řadič domény nakonfigurovaný jako PDC emulátor. Centrální zdroj času Společnosti je k dispozici rovněž v síťovém prostředí. Za synchronizaci času je zodpovědný útvar IT prostřednictvím správců, kteří nastavují konfiguraci času na jim svěřených Aktivech ICT/IS. Uživatelé nesmí modifikovat nastavení času na svých Pracovních stanicích. V případě, že je rozdíl času na pracovní stanici a v doméně Windows delší než 5 minut Uživatel ICT/IS neprojde procesem přihlášení do ICT/IS.

V systému SCADA a ŘS jsou za synchronizaci času zodpovědní jednotliví správci SCADA, či ŘS.

D.6.9 Management technických slabin

Útvar IT zajišťuje vlastními silami nebo prostřednictvím Dodavatelů sledování technických slabin a zranitelností pro provozovaná Aktiva ICT/IS. Správci sledují zveřejněné slabiny používaných operačních systémů, databází a dalších komponent ICT/IS . Útvar IT po zjištění slabiny využitelné v prostředí společnosti přijímá nápravná opaření prostřednictvím správců. Za opatření je zodpovědný Manažer, IT infrastruktura pro Aktiva infrastruktury. Pro aplikace a ŘS je za opatření zodpovědný Bezpečnostní architekt.

D.6.10 Autorizační postup pro zařízení provozovaném v rámci ICT/IS

Instalace všech typů zařízení v ICT/IS musí být technicky schválena a oprávněna bezpečnostním výborem. Všechny typy zařízení připojovaných do ICT/IS prochází technickým posouzením a testováním útvarem IT a jsou zakoupena dle metodiky útvaru nákupu. Typy zařízení, která prošla technickým posouzením a testováním předkládá Manažer, IT infrastruktura ke schválení bezpečnostnímu výboru ICT/IS. Objednávka všech zařízení ICT/IS probíhá přes útvar IT. Útvar IT zajišťuje připojení schválených zařízení do ICT/IS vlastními silami nebo s pomocí externích dodavatelů. Útvar IT řeší rovněž opravy a výměnu porouchaných komponent ICT/IS a jejich havárie na základě dohodnutých servisních smluv a důležitosti porouchané komponenty ICT/IS.

D.6.11 Spolupráce s ostatními organizacemi

Útvar IT poskytuje správcům možnost kontaktovat externí dodavatele a organizace, které se zabývají bezpečnosti a můžou poskytnout odbornou pomoc např. během napadení Aktiv Společnosti z Internetu. Útvarem IT definované osoby (zpravidla správci) mohou spolupracovat na řešení bezpečnostních událostí např. s dodavatelem antiviru, detekce narušení nebo firewallu. Útvar IT může rovněž spolupracovat s dalšími autoritami v ČR např. Národním bezpečnostním úřadem, Českým telekomunikačním úřadem a dalšími organizacemi. Rovněž může útvar IT využívat služeb mezinárodních organizací např. ISACA, CERT a další. Útvar IT si zajišťuje vlastními silami nebo smluvně přes dodavatele, odběr informací o bezpečnostních problémech a slabinách v používaných produktech od renomovaných firem např. Microsoft, VmWare, SAP, Oracle a další. Tyto informace jsou vyhodnocovány útvarem IT a následně jsou přijímaná bezpečnostní opatření v ICT/IS např. jsou aplikovány bezpečnostní záplaty.

D.6.12 Vzdálená práce v ICT/IS a propojení poboček

Aktiva Společnosti jsou provozována na mnoha místech i v prostorech, které nejsou pod fyzickou správou Zaměstnanců společnosti. Rovněž je ve společnosti používán vzdálený přístup k Aktivům ICT/IS z jiných sítí mimo sítě Společnosti. Příkladem jsou např. datová centra, pracoviště dodavatelů, pracoviště Uživatelů při práci z domova atd. Proto je v následujícím přehledu uveden seznam bezpečnostních opatření používaných při propojování různých lokalit:

- Pro vzdálené připojení musí Uživatelé použít pouze schválené technologie a schválená pravidla či postupy jejich užití. např. VPN klienta. Konkrétní technologie schvaluje Bezpečnostní výbor ICT/IS.
- Propojování lokalit řeší konkrétními technologiemi útvar IT. Konkrétní technologie schvaluje Bezpečnostní výbor ICT/IS.
- Před navázáním vzdáleného přístupu musí Uživatel projít dodatečnou autentizací a autorizací.

- Veškerá komunikace pro vzdálené přístupy Uživatelů přes veřejné přístupné médium je šifrována po celou dobu spojení.
- Uživatel musí používat na koncovém zařízení firewall a ochranu proti malware.
- Aktivita uživatele na síťové vrstvě může být útvarem IT monitorována technickými prostředky auditu

Upřesnění opatření a pravidel pro oblast ICT/IS je uvedeno v návazných metodických pokynech tj. „*Metodickém pokynu IT-SECPOL pro Uživatele*“ a „*Metodickém pokynu IT-SECPOL pro Dodavatele*“.

D.7 Politika řízení přístupu v rámci ICT/IS

Přístup ke službám a datům ICT/IS je řízen na základě minimálních práv, které potřebují uživatelé ICT/IS ke své práci s informačními Aktivy ICT/IS. Přístupová práva k informačním Aktivům ICT/IS definují jejich vlastníci na základě obchodních potřeb Společnosti. V aplikacích Společnosti je aplikován přístup na bázi aplikačních rolí. Uživatelé mají v aplikaci konkrétní roli, jejíž práva nastavuje aplikační správce. Pro aplikování požadované kontroly přístupu k Aktivům ICT/IS jsou aplikovány následující principy:

- „**Nutná potřeba znát**“ – Uživatelům je povolen přístup k informačnímu Aktivu ICT/IS pouze tehdy, když je tento přístup nutný pro zajištění plnění pracovních úkolů a Uživatel má tento přístup schválen nadřízeným s danou kompetencí.
- „**Nutná potřeba užít**“ - Uživatelům je povolen přístup k Aktivu ICT/IS pouze tehdy, když je tento přístup nutný pro zajištění plnění pracovních úkolů a Uživatel je pro tento přístup autorizován.

Z technického pohledu je nastavování politiky přístupu rozděleno do logických vrstev infrastruktury ICT/IS viz následující přehled:

- Nastavení práv v Active Directory,
- Nastavení práv v operačních systémech,
- Nastavení práv v aplikacích,
- Nastavení práv v databázích,
- Nastavení politiky přístupu na síťových aktivních prvcích.

Detailní nastavení pravidel politiky řízení přístupu v rámci ICT/IS je uvedeno v následujících podkapitolách a zejména v návazných metodických pokynech.

D.7.1 Přístup k síti a síťovým službám

Uživatelé mohou získat přístup k síti a síťovým službám pouze tehdy, když jsou pro tento přístup autorizováni. Technické nastavení politiky přístupu zajišťuje útvar IT prostřednictvím správců. Útvar IT definuje základní minimální politiku přístupu, která je aplikována na každého Uživatele. Minimálně má každý Uživatel zřízen účet v Active Directory a je členem předdefinovaných skupin (práva minimální politiky). Předdefinované skupiny konfiguruje útvar IT prostřednictvím správců. Následně jsou práva z minimální politiky přístupu rozšířena o práva, která daný Uživatel ICT/IS potřebuje ke své práci a která mu schválil oficiálním postupem jeho nadřízený nebo jiný subjekt s oprávněním schvalovat práva.

V rámci Společnosti jsou aplikována následující bezpečnostní opatření:

- Veškerému přiřazení práv musí předcházet proces autentizace Uživatele. Autentizace může být zesílena např. vlastněním autentizačního předmětu Uživatelem nebo užitím biometrických informací. O použití zesílené autentizace rozhoduje útvar IT na základě provedené bezpečnostní analýzy.
- Veškerá aktivita Uživatelů může být monitorována prostředky bezpečnostního auditu.
- Útvar IT udržuje přehledy o tom, komu byla přidělena konkrétní práva k aktivům ICT/IS. Za dokumentaci práv v aplikacích jsou zodpovědní správci dané aplikace.

D.7.2 Procedura řízení přístupu

Nadřízený Uživatele (v případě zaměstnanců Společnosti) či odpovědná osoba za Uživatele (v případě dodavatelů) musí definovat a schválit požadavky na řízení přístupu pro Uživatele ve své kompetenci. Nadřízený či odpovědná osoba za Uživatele ICT/IS odesílá žádost o nastavení politiky přístupu na Service Desk. Žádost schvaluje na straně útvaru IT definovaný správce nebo manažer, IT infrastruktura. Konkrétní nastavení práv provedou správci po obdržení oficiálního požadavku od Service Desku. Práva přístupu ke klasifikovaným informacím na stupeň vyšší než „Interní" podléhají schválení Bezpečnostním manažerem viz nadřazená bezpečnostní dokumentace.

D.7.3 Řízení přístupu Uživatele do ICT/IS

Správci dle principů registrace/deregistrace Uživatelů nastavují a odebírají schválená práva Uživatelům. Tyto principy zahrnují následující bezpečnostní opatření:

- Uživatel dostává v ICT/IS jedinečný identifikátor, který nesmí být přidělen jinému subjektu.
- Po obdržení žádosti o ukončení pracovního poměru nebo smluvního vztahu se Společností jsou vypínány účty dotčených Uživatelů.
- Pravidelně dochází ke kontrole uživatelských účtů a blokování inaktivních uživatelských účtů v rámci ICT/IS. Účty, u kterých nebyla nalezena aktivita za poslední 2 měsíce, jsou blokovány. Kontrolu inaktivity provádí správci a Vedoucí interní auditor dle potřeby minimálně však 2x ročně.
- Útvar IT užívá definované postupy pro předání dat vypnutých či blokovaných Uživatelů určeným Uživatelům (nově příchozím, zastupujícím atd. dle definovaných postupů).
- Útvar IT udržuje přehled o právech přidělených konkrétnímu Uživateli.
- Útvar IT je zodpovědný za konfiguraci šetřiče obrazovky na koncových zařízeních ve Windows doméně, který se Aktivuje automatizovaně po definované nečinnosti koncového zařízení (viz Metodický pokyn pro Uživatele).
- Útvar IT provádí po instalaci/implementaci komponent ICT/IS změnu a rekonfiguraci standardních (default) hesel na těchto komponentách ICT/IS.
- Útvar IT provádí konfiguraci předávání autentizačních informací mezi různými Aktivy ICT/IS.
- Útvar IT nastavuje omezení pro automatické přerušení spojení k Aktivům ICT/IS po dosažení doby neaktivity klienta na 15 minut.
- Přidělování počátečních hesel je konfigurováno tak, že Uživatel si musí změnit heslo při následném přihlášení do ICT/IS.
- Obecný princip ve Společnosti je, že obecný Uživatel ke své práci nepotřebuje práva administrátora. Výjimky schvaluje Manažer, IT infrastruktura na základě schváleného registračního procesu. Útvar IT udržuje přehled o vydaných výjimkách pro užití práv administrátora.
- Hesla jsou v ICT/IS ukládána vždy v zašifrovaném stavu.
- Použití přidělených práv může být monitorováno útvarem IT pro potřeby bezpečnostního auditu.
- Přihlašovací proces Uživatelů je založen na bezpečnostních mechanismech v prostředí domény Windows. Z tohoto důvodu jsou obecně všechny Pracovní stanice Společnosti součástí domény Windows. Výjimky definuje útvar IT.
- Přihlašovací proces do domény Windows poskytuje základní bezpečnostní funkce – nikdy se nezobrazuje vkládané heslo a heslo není nikde přenášeno a ukládáno nezašifrovaně.
- Správce má právo přerušit aktivitu Uživatele nebo omezit jeho činnost v ICT/IS a o tomto kroku jej bezodkladně informovat.
- Útvar IT je oprávněn pomocí prostředků bezpečnostního auditu dohledat jakoukoliv aktivitu Uživatele v operačním systému, aktivních prvcích sítě a databázích. Činnost Uživatelů je rovněž sledována v aplikacích formou aplikačního auditu.
- V případě, kdy Uživatel přistupuje k Řídícímu systému či SCADA technologiím, tak je jeho přístup řízen v souladu s *Metodickým pokynem IT-SECPOL pro ŘS a SCADA systémy*.

Další opatření a postupy související s řízením přístupu Uživatele do ICT/IS jsou uvedeny v navazujících metodických pokynech (zejména v „*Metodickém pokynu IT-SECPOL pro Uživatele*“).

D.7.4 Politika hesel a konfigurace managementu hesel

Pro účely autentizace Uživatelů se v rámci Společnosti používá účinný mechanismus pro práci s hesly aplikovaný na celou sadu koncových zařízení spravovaných v doméně Windows. Konkrétní politiku hesel v doméně schvaluje bezpečnostní výbor a následně ji prosazuje útvar IT. Aktuální politika hesel a nastavení hesel je uvedeno v návazném metodickém pokynu viz „*Metodický pokyn IT-SECPOL pro Uživatele*“.

Politiku hesel a parametry pro práci s heslem prosazuje do praxe útvar IT pomocí mechanismů Active Directory v prostředí domény Windows. Zamykání účtů se netýká servisních účtů a netýká se účtů správců. Konkrétní detaily např. volbu kvalitních hesel řeší návazný metodický pokyn „*Metodický pokyn IT-SECPOL pro Uživatele*“.

D.7.5 Řízení přístupu k síti a aplikacím

Přihlášení Uživatele do sítě Společnosti musí podléhat kontrole přístupu na základě autorizace. Uživatel se nesmí přihlásit k prostředkům ICT/IS bez nutnosti zadat login jméno a heslo. Přístup ke službám ICT/IS je vždy zajištěn přes proces autentizace, autorizace a bezpečnostního auditu. Tyto bezpečnostní opatření prosazují rovněž aplikace používané ve Společnosti. Pro aplikace udržují aplikační správci přehledy Uživatelů a jejich aktuální přidělení práv v aplikaci. Každý Uživatel má v rámci dané aplikace pouze omezená práva. Pouze správci aplikací mají práva pro administraci aplikace. Je povoleno a používáno předávání autentizačních informací mezi jednotlivými Aktivy ICT/IS tzv. Single Sign ON.

Aplikace prosazují další management hesel na úrovni aplikací. Přístup k některým aplikacím a datům provozovaným v rámci ICT/IS je umožněn pouze po zadání hesla a login jména k této konkrétní aplikaci. Uživatel ICT/IS musí před použitím aplikace projít běžným přihlášením do operačního systému Pracovní stanice. Uživatel je povinen splnit politiku hesel dané aplikace. Konkrétní nastavení managementu hesel v aplikacích konfigurují správci aplikací. Nastavitelné parametry hesel v aplikacích, které neužívají autentifikace Uživatelů prostřednictvím Active Directory, nemusí splňovat parametry uvedené či odkazované v kapitole D.7.4. Konkrétní nastavení pro danou aplikaci definuje útvar IT podle technických možností aplikace.

Další opatření a postupy související s řízením přístupu Uživatele do sítě a k aplikacím jsou uvedeny v navazujících metodických pokynech zejména v „*Metodickém pokynu IT-SECPOL pro Uživatele“*.

D.7.6 Autentizace a autorizace vzdáleného Uživatele a počítače

Připojení vzdálených Uživatelů a koncových zařízení prostřednictvím veřejné sítě může být provedeno pouze po předchozí autentizaci a autorizaci pomocí VPN klienta. Způsob vzdáleného připojení definuje útvar IT. Pro autentizaci vzdáleného Uživatele jsou používány stejné autentizační informace, jako v doméně Windows. Další bezpečnostní opatření pro autentizaci a autorizaci definuje útvar IT. Útvar IT udržuje přehled o schválených a povolených přístupech pomocí VPN pro všechny subjekty pracující v ICT/IS. Útvar IT udržuje přehled o povolených službách a k jakým Aktivům ICT/IS mohou Uživatelé přistupovat přes VPN spojení. Připojení vzdálených Uživatelů a koncových zařízení prostřednictvím veřejné sítě je po 15 minutách nečinnosti klienta přerušeno. Tímto opatřením se omezuje zbytečné plýtvání kapacit a zdroji Aktiv ICT/IS. Za konfiguraci je zodpovědný útvar IT.

Další opatření a detaily jsou uvedeny v navazujícím metodickém pokynu viz „*Metodický pokyn IT-SECPOL pro Uživatele*“.

D.7.7 Použití systémových programů a zdrojových kódů

Přístup k systémovým programům a knihovnám je umožněn pouze správcům. Běžný Uživatel nesmí modifikovat systémové soubory operačního systému ani u své Pracovní stanice. Veškeré konfigurace serverů, aktivních prvků sítě a Pracovních stanic provádí správci. V případě, že je pro konfiguraci používán specializovaný SW, může tento SW používat pouze správce. Použití specializovaného SW je

útvarem IT monitorováno pomocí automatizovaného nástroje dohledu. V případě, že společnost vlastní zdrojové kódy k aplikacím, musí mít přístup k těmto zdrojovým kódům pouze aplikační správci dané aplikace.

D.8 Politika bezpečného chování Uživatelů

Politika bezpečného chování Uživatelů je specifikována v „*Metodickém pokynu IT-SECPOL pro Uživatele*“.

D.9 Kontinuita ICT/IS a politika zálohování/obnovy

Záměrem vedení Společnosti je zajistit připravenost ICT/IS k řešení krizových situací a zachování základních funkcí ICT/IS v rozsahu fungování Hlavních Aktiv ICT/IS. Bezpečnostním cílem je zajištění přípravy, proškolení a připravenosti určených Uživatelů po odborné stránce k výkonu činností spojených s řešením krizových situací, ochranou zdraví a života zaměstnanců a ochranou Aktiv ICT/IS.

D.9.1 Aspekty a proces plánování kontinuity ICT/IS

Ve Společnosti jsou k dispozici plány zachování kontinuity operací ICT/IS. Primární odpovědnost za obnovu komponent ICT/IS nese útvar IT. Plány zachování kontinuity ICT/IS pomohou ochránit kritické služby ICT/IS před dopady větších výpadků nebo nehod. Za řešení problematiky obnovy ICT/IS jsou spoluzodpovědní všichni Uživatelé. Veškeré operace v rámci obnovy ICT/IS iniciují členové bezpečnostního výboru. Vlastní obnovu řídí koordinátor obnovy.

V útvaru IT je k dispozici řízený postup, podle kterého se vyvíjí a udržují plány pro zachování kontinuity ICT/IS. Za plány a jejich vypracování, údržbu a testování je zodpovědný koordinátor obnovy. Za realizaci a testování plánů obnovy v případě obnovy zodpovídají Správci definováni v plánu obnovy.

V procesu plánování kontinuity činností se zejména zvažuje:

- Určení a odsouhlasení všech odpovědností a nouzových postupů.
- Zavedení nouzových postupů tak, aby bylo možné dokončit zotavení a obnovu v požadovaných lhůtách. Zvláštní pozornost je třeba věnovat ohodnocení vnějších závislostí společnosti a existujícím smlouvám.
- Dokumentace odsouhlasených procedur a postupů.
- Vhodné proškolení Uživatelů o odsouhlasených havarijních procedurách a postupech, včetně krizového řízení.
- Testování a aktualizace plánů.

D.9.2 Systém plánování kontinuity ICT/IS

U plánování kontinuity ICT/IS dodržuje útvar IT pevný systém a strategii obnovy schválenou Bezpečnostním výborem ICT/IS. Bezpečnostní výbor definuje základní strategii obnovy a požadavky na obnovu. Pro návrh strategie obnovy se vychází z provedené citlivostní analýzy rizik pro jednotlivé aplikace.

D.9.3 Testování plánů na zachování kontinuity ICT/IS

Plány na zachování kontinuity obchodních operací se musí otestovat alespoň 1x za 2 roky. Termíny a obsah testování schvaluje bezpečnostní výbor. Správci Aktiv ICT/IS testují obnovovací procedury definované v plánu alespoň 1x ročně.

D.9.4 Aktualizace plánů na zachování kontinuity ICT/IS

Plány na zachování kontinuity ICT/IS musí pravidelně aktualizovat alespoň 1x ročně koordinátor obnovy. Za aktualizaci plánů je zodpovědný Koordinátor obnovy. Na plánech jsou povinni spolupracovat dle potřeby všichni aplikační správci a další správci definováni Manažerem, IT Infrastruktura.

D.9.5 Redundance

Pro naplnění strategie obnovy z technického pohledu jsou útvarem IT používány technické prostředky zajišťující chod služeb ICT/IS s minimálními výpadky. Útvar IT využívá zejména:

- Záložní datová centra
- Virtualizaci Aktiv ICT/IS a jejich obnovu na jiném hardware
- Clustering aplikací a databází
- MPLS síť s automatickou rekonfigurací
- Prostředky load balancingu
- Zrcadlení (Mirroring) databází a diskových prostorů
- Distribuované filesystémy

Hlavní Aktiva ICT/IS jsou k dispozici v záložní lokalitě nebo jsou konfigurována tak, že jejich činnost může být automatizovaně převedena na jiná Aktiva ICT/IS.

D.9.6 Politika zálohování a obnovy

Pravidelně se provádějí zálohy informačních Aktiv ICT/IS uložených na útvarem IT definovaných úložištích. Konfiguraci zálohování koncových zařízení provádí pouze útvar IT dle zálohovacího plánu prostřednictvím správců. Útvar IT udržuje plán zálohování a pravidelně testuje čitelnost záloh a obnovitelnost ze záloh.

Uživatel ukládá informační Aktiva ICT/IS na definovaná úložiště. Útvar IT nenese zodpovědnost za zálohování a obnovu dat uložených mimo definovaná úložiště. Útvar IT je odpovědný za obnovu dat v případě potřeby. Rozsah možností obnovy dat na poškozených definovaných úložištích vychází ze zálohovacích plánů.

Zálohovací plán ICT/IS udržuje útvar IT a jeho obsahem jsou:

- Požadavky na zálohování a obnovu
- Pravidla a postupy zálohování
- Pravidla bezpečného uložení záloh
- Pravidla a postupy obnovy
- Pravidla a postupy testování zálohování a obnovy

Další pokyny a pravidla pro zálohování a obnovu dat Uživatele a Společnosti jsou uvedena v navazujícím metodickém pokynu viz „*Metodický pokyn IT-SECPOL pro Uživatele*“.

D.10 Politika bezpečného předávání a výměny informací

Politiku bezpečného předávání a výměny informací definuje a řeší nadřazená bezpečnostní dokumentace. V rámci Bezpečnostní politiky ICT/IS jsou upřesněny pravidla pro předávání informací v síti nebo na elektronických médiích v rámci ICT/IS či v rámci zajištění provozu ICT/IS. Definice těchto upřesněných pravidel pro oblast ICT/IS je součástí této kapitoly a zejména návazných metodických pokynů tj. „*Metodického pokynu IT-SECPOL pro Uživatele*“ a „*Metodického pokynu IT-SECPOL pro Dodavatele*“.

D.10.1 Dohody pro elektronickou výměnu a sdílení dat

Každý subjekt, který chce komunikovat se Společnosti tak musí činit na základě vzájemně odsouhlaseného a dohodnutého formátu dat. Součásti vzájemné dohody o výměně a sdílení dat musí být alespoň následující ujednání:

- Formát dat např. ZIP archiv obsahující textové soubory.
- Procedury popisující ochranu proti škodlivému kódu.

- Aplikování technických bezpečnostních opatření, zejména šifrování dat, výměna šifrovacích klíčů a autentizace.
- Požadavky na audit a monitorování.
- Způsob mazání dat.
- Možnosti předávání dat dalším subjektům.
- NDA a požadavky na utajení.
- Zodpovědnost subjektů participujících na výměně.

Útvar IT řeší konkrétní návrh bezpečnostních opatření pro každou realizovanou výměnu dat dle potřeby Společnosti. Útvar IT řeší popis bezpečnostních mechanismů realizovaných v rámci výměny formou předschválené šablony, kterou schválil Manažer, IT infrastruktura.

D.10.2 Zabezpečení elektronické pošty a nástrojů pro IM

Ochrana elektronické pošty je útvarem IT zajišťována pomocí technických opatření. Uživatelé můžou podepisovat el. poštu svým certifikátem a můžou šifrovat zprávy el. pošty pomocí certifikátů příjemců el. pošty. Při přístupu k poštovní schránce z Internetu musí Uživatel projít autentizačním procesem. Autentizační proces může vyžadovat použití autentizačního předmětu.

Konkrétní požadavky pro zabezpečení el. pošty jsou uvedeny v „*Metodické pokynu IT-SECPOL pro Uživatele*“.

D.11 Politika řízení vývoje, podpory a provozu aplikací/SW

Účelem kapitoly je prosadit bezpečnost informací do celého životního cyklu provozovaných Aktiv ICT/IS od fáze návrhu, vývoje, testování až po vlastní provoz a údržbu. Implementace a změny Aktiv ICT/IS Společnosti jsou spojeny s definováním a stanovením vhodných bezpečnostních požadavků na Aktiva ICT/IS.

Bezpečnostním cílem je zajištění ochrany prostřednictvím opatření v následujících oblastech:

a) analýza a specifikace bezpečnostních požadavků – určení bezpečnostních požadavků v klíčových fázích životního cyklu ICT/IS zajistí, že bezpečnostní opatření jsou nedílnou součástí životního cyklu ICT/IS;
b) aplikování bezpečnostních opatření v aplikačních službách dostupných z veřejných sítí – zajištění míry záruk za aplikace Společnosti nabízené v DMZ;
c) zajištění transakcí v aplikacích a spolehlivosti zpracování dat v aplikacích a kryptografických opatřeních – utajení a kontrola Informačních Aktiv ICT/IS má spolu s kryptografickými opatřeními za cíl předcházet ztrátě, neoprávněné modifikaci nebo zneužití dat v aplikacích;
d) bezpečnost při prosazování změn v ICT/IS – je nutné definovat, prosadit a kontrolovat postupy vývoje a podpory, včetně formalizovaného postupu řízení změn;
e) správa testování – je nutné vhodnými opatřeními zajistit testování nových Aktiv ICT/IS před jejich použitím v produkci

Vývoj a údržba ICT/IS v rozsahu infrastruktury Společnosti a uživatelsky vyvinutých aplikací je podle stanovené působnosti zajišťována dodavateli jednotlivých aplikací, včetně zajišťování implementace bezpečnostních opatření v oblasti ICT/IS. Za finální konfiguraci a aplikování bezpečnostních opatření v aplikacích jsou zodpovědní aplikační správci.

D.11.1 Vývoj a požadavky na bezpečnost aplikací

U nově vyvíjených aplikací nebo před rozšířením/změnou stávajících aplikací zpracovávajících informace stupně „Strategické“ a „Určené“ musí být analyzovány požadavky a dopady na bezpečnosti ICT/IS. Za tímto účelem musí být definovány konkrétní požadavky na ochranu aplikačního prostředí jako výsledek analýzy rizik, prováděné v rámci standardní metodiky řízení projektů. Tuto analýzu provádí útvar IT vlastními silami. Schvalování výsledků analýzy provádí Bezpečnostní architekt. Specialista, Kvalita a bezpečnost IT dokumentuje zjištěná rizika v Katalogu rizik útvaru IT. Tato analýza musí být provedena pro všechny aplikace zpracovávající informace stupně „Strategické“ a „Určené“. U

ostatních aplikací rozhoduje o provedení analýzy útvar IT. Výstupem analýzy je návrh bezpečnostních opatření pro aplikaci a její provozní prostředí v infrastruktuře ICT/IS. Za implementaci navržených opatření je odpovědný útvar IT a smluvní Dodavatelé.

D.11.2 Bezpečnostní opatření v aplikačních službách v rámci DMZ

Pro aplikace provozované v rámci DMZ jsou útvarem IT přijímaná dodatečná opatření. Pro aplikaci je útvarem IT definováno rozhraní do dalších sítí jak vnitřních LAN, tak do Internetu. Aplikace musí používat v DMZ pouze schválené komunikační protokoly a přenášet pouze schválené formáty dat. Útvar IT definuje protokoly a formáty dat. Jejich následné schválení provádí Bezpečnostní výbor ICT/IS. Komunikace s Aktivy ICT/IS ve vnitřní síti musí procházet firewallem, jehož pravidla udržuje a dokumentuje správce. Pro aplikaci v DMZ musí být zdokumentovány všechny způsoby komunikace do/z Internetu. Pravidla firewallu povolují komunikaci z DMZ pouze ke schváleným zdrojům v Internetu. Provoz na všechna Aktiva ICT/IS v DMZ je kontrolován několika firewally, proxy servery a systémem detekce narušení. Ty můžou přerušit podezřelou komunikaci, kterou vyhodnotí jako potenciální narušení. Aplikování bezpečnostních opatření v DMZ je pravidelně kontrolováno útvarem IT pomocí penetračních testů a testování zranitelností. Útvar IT provádí toto testování rovněž před uvedením aplikace do provozu v případě, že zpracovávají informace stupně „Strategické“ a „Určené“.

D.11.3 Zabezpečení transakcí v aplikacích

Pro aplikační transakce zpracovávající Informační Aktiva stupně „Strategické“ a „Určené“ musí být zajištěno, že nedojde k neautorizovanému přístupu k přenášeným datům, neoprávněné modifikaci, přehrání nebo duplikování dat transakce. Za tímto účelem musí útvar IT používat schválené techniky pro šifrování a kryptografické podepisování dat viz kapitola D.16. Rovněž musí být použity techniky pro oddělení Aktiv ICT/IS zajišťujících běh transakce. Veškerá aktivita na úrovni aplikačních transakcí musí být svázána s činnosti Uživatele, který prošel autentizací a autorizaci pro tuto činnost. Aktivity vybraných transakcí jsou sledovány prostředky bezpečnostního auditu na úrovni aplikací a infrastruktury ICT/IS. Aplikační správce definuje rozsah sledovaných transakcí v jemu přidělených aplikacích.

D.11.4 Zajištění bezpečného vývoje, testování a dokumentace

Vývoj je prováděn v rámci standardní „*IT metodiky vedení projektů*“. Součástí projektových fází je definice výstupů pro zajištění bezpečnosti ICT/IS v jednotlivých fázích. Útvar IT provádí vlastními silami vyhodnocení výstupů jednotlivých fází. Schvalování výsledků provádí Bezpečnostní architekt.

Útvar IT rozhoduje o provádění změn a rozsahu analýzy rizik při změně operačních systémů nebo databázových systémů a verzí aplikací u již provozovaných Aktiv ICT/IS. Pro tyto změny musí útvar IT zajistit dostatečný čas a Aktiva pro testování. Útvar IT rozhoduje o tom, zda testování je řešeno na Aktivech ICT/IS Společnosti nebo u Dodavatele.

Aplikační správci udržují pro jednotlivé aplikace podpůrné nástroje, verze aplikace a dokumentaci. Aplikační správci rovněž provádějí schválené změny v implementaci bezpečnostních opatření během vývoje a testování aplikací. Aplikační správci rovněž zajišťují ochranu dat používaných během testování a vývoje. Testovací a vývojová data jsou ukládána pouze na schválená úložiště definovaná útvarem IT. Aplikační správce je zodpovědný za aplikování ochrany proti škodlivému kódu ve vývojovém a testovacím prostředí. Aplikační správci zajišťují ochranu všech používaných a instalovaných SW Aktiv ICT/IS, která jim byla svěřena útvarem IT. Veškerý SW distribuovaný do provozního prostředí musí procházet kontrolou na výskyt škodlivého kódu a kontrolou integrity např. pomocí kontrolních součtů nebo hashovacích funkcí viz kapitola D.16.

Útvar IT je zodpovědný za vzájemnou kompatibilitu SW a provozního prostředí Aktiv ICT/IS. Útvar IT rozhoduje o aplikování bezpečnostních opatření v aplikacích provozovaných ve více vrstvách (prezentační, aplikační, datová, infrastrukturní). Nové technologie ICT/IS jsou útvarem IT analyzovány z pohledu bezpečnostních rizik. Výslednou infrastrukturu a design Aktiv ICT/IS schvaluje Bezpečnostní architekt.

Bezpečnostní opatření jsou útvarem IT aplikovány rovněž formou vzájemných dohod uzavřených s Dodavateli Aktiv ICT/IS. Součástí dohod musí být definování pravidel pro kontrolu kvality, testování a způsob přebíraní a akceptování dodávaných Aktiv ICT/IS. Součástí dohod musí být definování pravidel pro licencování vyvíjených aplikací, a zda je vyvinutý kód majetkem společnosti.

Vstupní data v aplikacích se musí kontrolovat a prověřovat samotnou aplikací hned při pořizování a vstupu dat. Uživatelé ICT/IS jsou povinni informovat Service Desk, v případě, že aplikace akceptuje nesprávné vstupní formáty dat. Service Desk informuje o této skutečnosti daného aplikačního správce. Ten zajistí opravu vlastními silami nebo u Dodavatele.

D.11.4.1 Testování zabezpečení

Bezpečnostní funkcionality systémů jsou testovány již ve fázi vývoje systémů.

Opatření pro testování bezpečnostní funkcionalit:

a) Nová a aktualizované systémy jsou důkladně testovány již během svého vývoje, tj. minimálně existuje harmonogram činností v rámci testování, testují se vstupy a očekávané výstupy za různých podmínek.
b) Testování by mělo být provedeno nezávislou stranou (nikoliv pouze vlastním vývojovým teamem).
c) Rozsah testování by měl být vždy stanoven vzhledem k povaze a významu daného systému. Hlavní principy a pravidla testování jsou stanovena interním dokumentem útvaru IT „*Metodika testování a nasazení na produktivní prostředí*“.

D.11.4.2 Dokumentace k aplikacím a projektům

Pro každou aplikaci nebo projekt nad komponentami ICT/IS zpracovávajícími informace stupně „Strategické“ a „Určené“ musí existovat dokumentace popisující konfiguraci nastavení bezpečnostních funkcí a popis provozního prostředí. Pro ostatní aplikace a projekty definuje rozsah dokumentace útvar IT dle provozních požadavků. Dokumentace aplikaci nebo projektů nad komponentami ICT/IS zpracovávajícími informace stupně „Strategické“ a „Určené“ musí obsahovat alespoň následující obsah definovaný v šabloně umístěné na sdílených zdrojích útvaru IT:

- Popis infrastruktury aplikace pro provoz, vývoj a testování
- Popis konfigurace autentizace, autorizace a auditu
- Popis konfigurace dohledu
- Popis nastavení požadavků na konfiguraci sítě a firewallů
- Popis nastavení přístupových práv, členství ve skupinách a rolích
- Plán zálohování a archivace
- Další popis nezbytný pro bezpečné provozování aplikace, systému nebo projektu.

Pro ostatní aplikace a projekty, které nezpracovávají informace stupně „Strategické“ a „Určené“ definuje rozsah požadované dokumentace útvar IT.

D.11.5 Postupy pro řízení změn při vývoji a změn aplikací

Aplikační správce musí dodržovat oficiální postupy, kterými se řídí změnová řízení v aplikacích. Veškeré změny v ICT/IS musí být dokumentovány. Aplikační správce musí zajistit, že změny budou akceptovány klíčovými uživateli ICT/IS před jejich aplikováním v provozním prostředí. K tomu musí aplikační správce zajistit souhlas klíčového uživatele se změnou a termínem provedení změny. Aplikační správce zodpovídá za aktualizaci veškeré dokumentace související se změnou. Formální postup pro aplikování změn definuje útvar IT. Proces řízení změn je detailně v dokumentu „*Řešení IT požadavků v rámci úseku Informační technologie NET4GAS, s.r.o*“.

D.12 Politika dodržování licencování, norem, zákonných ustanovení a shody

Útvar IT pravidelně provádí přezkoumání souladu všech oblastí ICT/IS s bezpečnostní dokumentaci Společnosti, zákonnými požadavky, ostatními požadavky na bezpečnost a také s příslušnými standardy a normami ČR. Je třeba ve Společnosti zajistit dodržování právních norem, soulad s legislativními předpisy, dodržování smluvních a bezpečnostních požadavků.

D.12.1 Dodržování zákonných požadavků

Tvorba, provoz a použití ICT/IS musí vyhovovat zákonným a smluvním bezpečnostním požadavkům závazných ve Společnosti. Společnost provozuje aplikace, ve kterých se zpracovávají také data dle následujících zákonů:

- Zákon č. 101/2000 Sb., o ochraně soukromých údajů,
- Zákon č. 121/2000 Sb., o ochraně duševního vlastnictví,
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti,
- Zákon č. 240/2000 Sb., krizový zákon,
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě,
- Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu),
- Zákon č. 89/2012 Sb., občanský zákoník.

Pro aplikace pracující s daty podléhající výše uvedeným zákonům jsou aplikovány dodatečná bezpečnostní opatření vyžadována těmito zákony. Společnost musí zajistit soulad s legislativou ČR, která se bude vyvíjet i v budoucnu např. účinnost zákona o kybernetické bezpečnosti a k němu náležící vyhlášky NBU. Požadavky nové legislativy budou zapracovány v budoucnu do tohoto dokumentu dle potřeby.

D.12.2 Dodržování autorských práv a licenčních podmínek

Společnost dodržuje ustanovení o autorském právu a podmínky licenčních ujednání dodavatelů programového vybavení. Kopírování software, na který existuje legální autorská oprávnění, je nutno provádět jen v souladu s platnými licenčními ujednáními. Uživatelé nesmí používat SW, který nesplňuje požadavky a na který není zakoupena řádná licence. Uživatelé ICT nesmí šířit nelegální SW. Detailní zásady platné pro Uživatele jsou uvedeny v metodickém pokynu viz „*Metodický pokyn IT-SECPOL pro Uživatele*“.

D.12.3 Zabezpečování dlouhodobých záznamů organizace

Důležité záznamy společnosti se musí chránit před ztrátou, zničením a falzifikací. Musí být zajištěna dlouhodobá archivace dat dle zákonných požadavků ČR, konkrétně Zákon o archivnictví a spisové službě. Útvar IT poskytuje technologie a Aktiva ICT/IS pro dlouhodobé ukládání informačních Aktiv. Uživatelé IT musí ukládat data pro dlouhodobou archivaci na definovaná úložiště.

D.12.4 Ochrana osobních údajů

Aplikace, které pracují s osobními údaji jednotlivců, musí vyhovovat zákonu o ochraně osobních údajů. Uživatelé ICT/IS pracující s osobními daty zaměstnanců Společnosti:

- splňují podmínku ”need-to-know”,
- jsou autorizovaní pro přístup k osobním informacím prostřednictvím dané aplikace,

D.12.5 Zajištění shody

V případě zjištění nesouladu se zákonnými a legislativními požadavky iniciuje útvar IT sadu činností, konkrétně musí útvar IT:

- určit příčiny nesouladu;
- vyhodnotit potřebu přijetí opatření k nápravě;

- určit a implementovat nápravná opatření;
- přezkoumat přijatá nápravná opatření;
- zdokumentovat závěry z přezkoumání a přijatá nápravná opatření.

D.12.5.1 Bezpečnostní posudky ICT/IS

Bezpečnost ICT/IS se musí pravidelně hodnotit a prověřovat vnitřní nebo nezávislou autoritou 1x ročně. Nezávislou autoritu schvaluje Ředitel, Informační technologie. Pravidelné kontroly dle plánu auditu ISMS provádí Vedoucí interní auditor. Audity provozních Aktiv ICT/IS a jejich rozsah se musí plánovat a předem odsouhlasit bezpečnostním výborem ICT/IS.

D.12.5.2 Zajištění nástrojů auditu

Útvar IT používá auditovací nástroje pro hodnocení provozních Aktiv ICT/IS umožňující nezávislý audit ICT/IS. Přístup k nástrojům bezpečnostního auditu je umožněn pouze členům bezpečnostního výboru, definovaným správcům a osobám pověřeným auditem. Alespoň 1x ročně je třeba provést penetrační testování aplikací v DMZ provozovaných v rámci ICT/IS.

D.12.5.3 Výjimky

Případné výjimky z pravidel obsažených v tomto dokumentu musí být s vysvětlením jejich opodstatnění předloženy ke zvážení Specialistovi, Kvalita a bezpečnost IT, který může pro jejich posouzení iniciovat proces analýzy rizik. Specialista, Kvalita a bezpečnost IT provádí evidenci výjimek. Výjimka může být udělena jen v odůvodněných případech. Pokud jsou výjimky uděleny, musí být minimálně každých 6 měsíců přezkoumány, zda nepominuly důvody pro jejich udělení a zda se nemění úroveň rizik. Neakceptovatelné zvýšení rizik je důvodem pro neudělení nebo zrušení výjimky.

Základní pravidla životního cyklu výjimky:

- Každá žádost o výjimku musí být evidována (typicky v Service Desk nástroji). Žádost o výjimku může podat kdokoliv.
- Pokud tento dokument a návazné metodické pokyny specifikují schvalovatele konkrétní výjimky, tak tuto výjimku schvaluje specifikovaný schvalovatel. V případě, kdy není v dokumentaci uveden pro konkrétní typ výjimky schvalovatel, tak obecně je takovou výjimku oprávněn schválit pouze Bezpečnostní výbor.
- Po uplynutí 6 měsíců od schválení výjimky je automaticky spuštěn proces opětovného schválení výjimky (přezkum výjimky). V případě, kdy nedojde do 2 měsíců od spuštění procesu opětovného schválení (přezkumu výjimky) k opakovanému schválení výjimky (potvrzení výjimky), tak je tato výjimka považována za nepotřebnou a bude zrušena. Útvar IT je odpovědný za řízení zrušení takové výjimky.

D.13 Politika fyzické bezpečnosti

Politika fyzické bezpečnosti Společnosti je stanovena v rámci nadřazené bezpečnostní dokumentace. Fyzická bezpečnost budov a místností ve Společnosti je řešena směrnicí SM_I04_04_01 Řízení fyzické bezpečnosti v NET4GAS, s.r.o. a jejími navazujícími metodickým pokyny. Útvar IT zajišťuje budování zabezpečených oblastí pro provozování Hlavních Aktiv ICT a k nim vedoucích kabelových tras.

D.13.1 Zabezpečené oblasti pro ICT/IS

Zařízení a prostředky ICT/IS, které podporují klíčové služby ICT/IS, jsou umístěny v bezpečných prostorech s definovanou kontrolou přístupu - jde o prostory serveroven a datových center. Samostatný přístup do těchto prostor mají pouze správci. Všechna datová centra a serverovny jsou koncipovány jako bezobslužná pracoviště bez trvalé přítomnosti správců. Společnost provozuje rovněž oblasti, kde je zajištěn směnný provoz v režimu 24x7. Příkladem je např. pracoviště dohledu SCADA, velíny, TELCO dispečink a Technický dispečink Společnosti. Všechny tyto oblasti jsou v dalším textu označeny jako „Režimová pracoviště“. Ostatní prostory společnosti jsou chápány jako nerežimová pracoviště a v dalším textu jsou označena jako „Pracoviště“.

D.13.2 Prvky fyzické ochrany Režimových pracovišť

Na Režimová pracoviště jsou z pohledu fyzické bezpečnosti aplikována následující bezpečnostní opatření:

- Režimová pracoviště jsou oddělena od ostatních prostor Společnosti obvodovou ochranou.
- Režimová pracoviště jsou trvale uzamčena a chráněna kontrolou přístupu např. na vstupní kartu.
- Vstup na režimová pracoviště mají pouze Správci a osoby doprovázené správcem nebo jinou autorizovanou osobou. Vstup do režimového pracoviště je zaznamenáván správcem v knize návštěv nebo automatizovaně s použitím karetního systému.
- V Režimovém pracovišti je aplikována protipožární ochrana dle platné legislativy.
- V Režimovém pracovišti se nesmí umisťovat snadno hořlavé materiály.
- V Režimovém pracovišti jsou použity prostředky pro chlazení Aktiv ICT/IS, snímání vlhkosti, teploty, automatizované osvětlení atd.
- V Režimovém pracovišti je napájení Aktiv ICT/IS chráněno pomocí UPS nebo jiným způsobem např. dieselagregátem.
- Umístění/vynesení jakéhokoliv Aktiva ICT/IS v režimovém pracovišti musí podléhat kontrole a autorizaci útvarem IT a konkrétním správcem, který provede umístění/vynesení Aktiva ICT/IS.
- Kabelové trasy do režimových pracovišť používají jako bezpečnostní opatření ochranu zábranou nebo polohou. Nepoužívané kabely a zásuvky sítě nesmí být připojeny k Aktivním prvkům. Přístup k rozvaděčům s kabeláží mají jenom definovaní Správci.

D.13.3 Umístění a ochrana Aktiv ICT/IS

Aktiva ICT/IS se musí umísťovat a chránit na Pracovišti tak, aby se snížilo riziko poškození, vzájemného ovlivňování Aktiv a neoprávněného přístupu k nim. Aktiva ICT/IS lze umisťovat mimo kontrolu společnosti jenom se souhlasem Manažera, IT infrastruktura nebo jím explicitně delegovaného Správce. Aktivum ICT/IS, které je Uživatelem ponecháno bez dozoru v objektu v majetku Společnosti či objektu k tomu určeném, musí být chráněno dodatečnými bezpečnostními opatřeními a musí být automaticky odhlášeno z ICT/IS a následně uzamčeno technickými prostředky po definované době neaktivity.

D.13.4 Napájecí zdroje

Aktiva ICT/IS jsou chráněna před výpadky napájení nebo jinými elektrickými anomáliemi. Rozmístění těchto prostředků definuje útvar IT a Uživatelé jsou povinni používat definovaný způsob napájení přidělený na Pracovišti Uživatele ICT/IS.

D.13.5 Údržba Aktiv ICT/IS

Aktiva ICT/IS musí mít odpovídající údržbu, kterou zajišťuje definovaný správce nebo vlastník Aktiva. V režimových pracovištích zajišťují údržbu Aktiv ICT/IS pouze správci. Plánování údržby Aktiv ICT/IS umístěných v Režimových pracovištích provádí útvar IT prostřednictvím správců.

D.13.6 Bezpečné znehodnocování Aktiv ICT/IS

Před plánovaným zničením nebo předáním Aktiva ICT/IS mimo kontrolu Společnosti musí být vymazány všechny informace Společnosti. Postupy mazání schvaluje bezpečnostní výbor ICT/IS. Útvar IT používá postupy a techniky pro vícenásobné přepisování. Konkrétní technologie navrhuje ke schválení bezpečnostnímu výboru ICT/IS Manažer, IT infrastruktura nebo jim definovaný správce. V případech, kdy nejde použít vícenásobné přemazání informací, může být použito prostředků pro fyzickou likvidaci Aktiva.

D.14 Politika bezpečnosti sítě

Speciální pozornost vyžaduje bezpečnostní řízení počítačových sítí, které tvoří základ všech ICT/IS operací ve Společnosti. Termínem počítačová síť se rozumí všechny technické a programové prostředky, které slouží jak k propojení počítačů, tak k využití tohoto propojení. Posláním počítačové sítě je datové propojení jednotlivých počítačů společnosti a jejich napojení do LAN/WAN/WiFI pro účely

zajištění provozu a informační podpory společnosti. Sítě Společnosti jsou mezi sebou vzájemně propojovány pouze pomocí schválených oddělovacích členů a firewallů.

Bezpečnostní mechanismy sítě, úroveň služeb a požadavky na monitoring sítě musí být jasně identifikovány a popsány útvarem IT. Pro bezpečnost sítového prostředí musí být aplikovány následující zásady:

- Dokumentace sítě
- Ochrana fyzického přístupu k aktivním prvkům sítě
- Ochrana logického přístupu ke konfiguraci prvků sítě
- Dodržování zásad pro práci v síti
- Používání doplňkových bezpečnostních mechanismů – šifrování a zesílené autentizace
- Oddělování a segmentace sítě na menší části
- Použití doplňkových bezpečnostních opatření pro WIFI sítě
- Trvalý monitoring sítě pomocí automatizovaných nástrojů
- Definování a dodržování pravidel pro předávání informací v síti nebo na médiích

D.14.1 Dokumentace sítě

Všechna fyzická a logická propojení sítě musí být zdokumentována v mapě sítě, v aplikacích a v pravidlech propojovacích členů. Za dokumentaci sítě je zodpovědný útvarem IT nadefinovaný správce sítě. Za dokumentaci síťových spojení v aplikacích jsou zodpovědní aplikační správci. Dokumentace sítě musí být chráněna před neoprávněným přístupem a všechny modifikace může provádět pouze správce. Součástí dokumentace musí být rovněž technické rozhraní a perimetr dané části sítě.

D.14.2 Přístup a konfigurace aktivních prvků sítě

Fyzický přístup k aktivním prvkům sítě a možnost jejich konfigurace mají pouze správci. Útvar IT je zodpovědný za správnou konfiguraci aktivních prvků sítě. Aktivní prvky sítě jsou fyzicky umisťovány do režimových pracovišť. V případě, že aktivní prvek sítě není umístěn v režimovém pracovišti, musí útvar IT zajistit pro toto aktivum uzamykatelný rozvaděč, do kterého musí být aktivní prvek umístěn. Konfiguraci aktivních prvků sítě nesmí provádět aplikační správci.

V případě Řídícího systému a SCADA technologií konfiguraci aktivních prvků v síti SCADA provádí Správce SCADA.

D.14.3 Oddělování v sítích

Síť Společnosti tvoří jako celek velkou množinu Aktiv, která jsou dislokována po celé ČR. Proto musí být její administrace a provozování rozděleno na menší logické části. Toto oddělování se děje používáním technických komponent např. firewallů, VPN bran, směrovačů, přepínačů a jiných oddělovacích členů. Útvar IT používá rovněž logické oddělování částí sítě pomocí bezpečnostních opatření v Active Directory Windows domén. Konkrétní způsoby oddělování v sítích definuje útvar IT. Útvar IT musí pro každou síť nadefinovat jasné rozhraní a perimetr sítě. Útvar IT spolupracuje při konfiguraci oddělovacích členů s Dodavateli. Útvar IT zodpovídá za rozmístění Aktiv ICT/IS do různých částí sítě tak, aby nemohlo dojít k výpadku všech Aktiv ICT/IS ve Společnosti. Do samostatných sítí jsou umisťována Aktiva ICT/IS zajišťující přepravu plynu.

D.15 Politika ochrany před škodlivým kódem

Opatření pro ochranu před škodlivým kódem jsou popsána v jednotlivých částech Bezpečnostní politiky ICT/IS (tohoto dokumentu) a z pohledu Uživatele či Dodavatele pak zejména v návazných metodických pokynech tj. „*Metodickém pokynu IT-SECPOL pro Uživatele*“ a „*Metodickém pokynu IT-SECPOL pro Dodavatele*“

D.16 Politika bezpečného používání kryptografické ochrany

Jedno ze základních bezpečnostních opatření v ICT/IS je používání kryptografických služeb v produktech společnosti Microsoft a CISCO. Útvar IT využívá kryptografické techniky pro následující bezpečnostní mechanismy:

- Šifrování disků Pracovních stanic pomocí technologie BitLocker - povinné u mobilních zařízení a doporučené u všech Pracovních stanic
- Šifrování souborů a adresářů pomocí Encrypted Filesystem - volitelné
- Infrastruktura veřejných klíčů (dále jen PKI) a používání certifikátů - volitelné
- Infrastruktura IPSec pro zajištění komunikace v doméně Windows nebo mezi doménami - volitelné
- Šifrování vzdálených přístupů pomocí CISCO VPN klienta - povinné
- Doplňkové šifrování v aplikacích pro mezibankovní styk - povinné
- Doplňkové šifrování v prostředí aplikace SAP - volitelné
- Zesílená dvoufaktorová autentizace - volitelné

Jako povinný bezpečnostní mechanismus je vyžadováno šifrování disků Pracovních stanic a šifrování vzdálených přístupů. Výjimky z tohoto opatření schvaluje Bezpečnostní výbor ICT/IS. Další bezpečnostní mechanismy s využitím kryptografie používá útvar IT dle provozních potřeb.

D.16.1 Politika použití kryptografických opatření

ICT/IS zajišťuje kontrolu přístupu ke všem informačním Aktivům a nabízí doplňkové techniky pro ochranu informačních Aktiv formou šifrování. Všechny používané kryptografické techniky schvaluje Bezpečnostní výbor ICT/IS. Útvar IT prosazuje do praxe nasazení kryptografických technik dle provozních potřeb.

Útvar IT prosazuje následující politiku kryptografických opatření:

- Všechny kryptografické klíče musí mít minimální délku 2048 B.
- Jako minimální hashovací funkce musí být použit algoritmus SHA-2. Doporučený algoritmus pro hashování je SHA-256.
- Preferované algoritmy pro šifrování vycházejí ze standardu AES
- Je zakázáno použití hashovacích funkcí SHA1,MD5 a starších.

D.16.2 Management klíčů

ICT/IS ve společnosti využívá mechanismy PKI dostupné v doméně Windows. Útvar IT je zodpovědný za provoz vlastních certifikačních autorit (dále jen „CA“) a vydává certifikáty dle potřeb Společnosti. Útvar IT využívá funkce autoenrollmentu certifikátů pro stanice a uživatele. Je povoleno automatické obnovování certifikátů vydaných vlastní CA v doméně Windows. Zálohování, archivaci a likvidaci vydaných certifikátů zajišťuje útvar IT vlastními silami. V případě potřeby může útvar IT využívat služeb veřejně dostupných CA a jejich certifikátů. Činnosti Uživatelů využívajících služeb vnitřní CA jsou monitorovány prostředky bezpečnostního auditu. Kryptografická ochrana a její popis musí být součástí smluvních vztahů s dalšími subjekty, v případě, že je mezi smluvními stranami využíváno bezpečnostních opatření na bázi kryptografie.

D.17 Politika detekce/vyhodnocení událostí a management bezpečnostních incidentů

Management bezpečnostních událostí a incidentů Společnosti je obecně popsán nadřazenou bezpečnostní dokumentací. V rámci této kapitoly je detailněji popsán management událostí a incidentů v rámci ICT/IS jako subproces, který je v souladu s nadřazenou dokumentací a je platný v rámci ICT/IS.

Cílem managementu bezpečnostních incidentů v ICT/IS je zvládnutí konzistentního a efektivního přístupu pro řešení nestandardních událostí, které by mohly vážně narušit chod Aktiv ICT/IS společnosti. Cílem managementu bezpečnostních incidentů v ICT/IS je zejména:

- stanovit typové postupy řešení bezpečnostních incidentů,
- vymezit role v procesu řešení incidentů a s nimi stanovit jejich pravomoci a odpovědnosti,
- vymezit nejdůležitější kategorie bezpečnostních incidentů.

D.17.1 Základní pojmy

Pro správné pochopení celého procesu řízení bezpečnostních incidentů v ICT/IS je nutné správně pochopit dva základní pojmy. V následujícím textu je uveden rozdíl mezi bezpečnostní události a incidentem.

- „**Bezpečnostní událost**“ – kterou lze označit za identifikovaný stav informačního systému, služby nebo počítačové sítě, jež může narušit pravidla bezpečnostní politiky nebo selhání některého protiopatření nebo dříve neznámá nebo nepředpokládaná situace, jež může ovlivnit bezpečnost ICT/IS. Samotný vznik bezpečnostní události není ještě incidentem. Teprve vyhodnocená bezpečnostní událost může být kvalifikována jako bezpečnostní incident.
- „**Bezpečnostní incident**“ je jedna nebo více nechtěných nebo neočekávaných indikovaných bezpečnostních událostí, jimiž může být s vysokou pravděpodobností narušena podpora hlavních nebo podpůrných procesů organizace nebo díky nimž může dojít k narušení bezpečnosti ICT/IS. S bezpečnostní událostí přichází obvykle do prvního kontaktu běžný Uživatel ICT/IS.

D.17.2 Organizační struktury a odpovědnosti spojené s řešením bezpečnostních incidentů v ICT/IS

Pro řešení bezpečnostních incidentů se sestavuje z pracovníků útvaru IT specializovaný tým řešení bezpečnostních incidentů – Incidents Response Team tzv. IRT (dále jen „IRT“). Jedná se o organizační strukturu, která se používá výhradně pro potřeby řešení incidentů a událostí. Jeho členy se stávají zkušení správci, kteří mají zkušenosti s řešením takových situací. Ti se věnují řešení incidentů po celý jejich životní cyklus až do závěrečné etapy vyhodnocení a zobecnění jeho závěrů.

V některých případech je tento tým posilován o externí specialisty nebo jiné zaměstnance společnosti. Pokud dojde ve společnosti vinou bezpečnostnímu incidentu ke krizové situaci, je IRT posílen experty podle povahy zjištěného incidentu. Vedoucí týmu je Ředitel, Informační technologie. Tým IRT má své trvalé členy a členy, kteří jsou do něj jmenováni pro řešení určitých konkrétních incidentů. Trvalé členy IRT schvaluje bezpečnostní výbor ICT/IS. Po obdržení hlášení o bezpečnostní události na Service Desk, je spuštěna procedura vyrozumívání trvalých členů IRT.

Konkrétní zodpovědnosti IRT jsou uvedeny v následujícím přehledu:

- Členové IRT jsou zodpovědní za kategorizaci a klasifikaci bezpečnostních událostí.
- Členové IRT jsou zodpovědní za koordinaci řešení bezpečnostního incidentu mezi sebou a dalšími subjekty.
- Členové IRT jsou zodpovědní za důslednou dokumentaci bezpečnostního incidentu a jeho řešení. Dokumentace musí být vedena tak, aby mohla být použita jako důkaz při soudním líčení.
- Členové IRT jsou zodpovědní za vyřešení bezpečnostního incidentu a jeho dopadů.
- Členové IRT mohou úkolovat ostatní správce a Uživatele pro splnění úkolů souvisejících s bezpečnostním incidentem.

- Členové IRT přijímají a doporučují nápravná opatření, která zamezí opětovnému výskytu bezpečnostního incidentu.
- Členové IRT přebírají informaci o výskytu bezpečnostní události od Service Desku. Uživatelé ICT/IS hlásí výskyt bezpečnostních událostí na Service Desk.

Service Desk je zodpovědný za příjem hlášení o bezpečnostní události a její prvotní identifikaci. Následně je ServiceDesk zodpovědný za vyrozumívání Uživatelů o stavu řešení bezpečnostního incidentu.

D.17.3 Použití technických prostředků pro management bezpečnostních incidentů v ICT/IS

Řízení bezpečnostních incidentů a monitorování bezpečnosti se opírá o získávání detailních informací souvisejících s fungováním infrastruktury Aktiv ICT/IS, což není možné efektivně zajistit bez podpory technických nástrojů. Pro detekci bezpečnostních událostí může útvar IT používat následující kategorie monitorovacích nástrojů:

- nástroje dohledu Aktiv ICT/IS – systémy pro standardní monitoring běhu a vytížení infrastruktury sítě a služeb.
- systémy detekce průniku IDS (Intrusion Detection System) – nástroje pro odhalení pokusů o průnik do sítě nebo do jiných Aktiv ICT/IS včetně upozornění na nestandardní stavy prostředí,
- systémy prevence průniku IPS (Intrusion Prevention System) – varianta technologie IDS, u které jsou prohloubeny schopnosti pro-Aktivní reakce na bezpečnostní incidenty,
- centralizované sledování antivirových nástrojů,
- systémy pro management bezpečnostních informací a událostí SIEM (Security Information and Event Management) – nástroje pro sběr, korelaci, analýzu a vyhodnocení různých typů bezpečnostních událostí (firewall, IDS, antivirové systémy, VPN brány atd.).

Všechny uvedené kategorie nástrojů používá útvar IT dle provozních potřeb pro vyřešení bezpečnostního incidentu.

D.17.4 Kategorie bezpečnostních incidentů v ICT/IS

Pro potřeby zvládání bezpečnostních incidentů v ICT/IS se podle následků a negativních projevů bezpečnostní incidenty v ICT/IS dělí do následujících kategorií:

- **Kategorie I** – méně závažný bezpečnostní incident v ICT/IS, při kterém dochází k méně významnému narušení bezpečnosti poskytovaných služeb nebo Informačních Aktiv. Jeho řešení vyžaduje zásahy obsluhy s tím, že musí být vhodnými prostředky omezeno další šíření bezpečnostního incidentu v ICT/IS včetně minimalizace vzniklých škod.
- **Kategorie II** – závažný bezpečnostní incident v ICT/IS, při kterém je narušena bezpečnost poskytovaných služeb nebo Informačních Aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být vhodnými prostředky zabráněno dalšímu šíření incidentu v ICT/IS včetně minimalizace vzniklých škod.
- **Kategorie III** – velmi závažný bezpečnostní incident v ICT/IS, při kterém je přímo a významně narušena bezpečnost poskytovaných služeb nebo Informačních Aktiv. Jeho řešení vyžaduje neprodlené zásahy obsluhy s tím, že musí být všemi dostupnými prostředky zabráněno dalšímu šíření bezpečnostního incidentu v ICT/IS včetně minimalizace vzniklých i potenciálních škod.

Konkrétní kategorizaci bezpečnostních událostí provádějí členové IRT. Celý postup eliminace bezpečnostního incidentu koordinuje Ředitel, Informační technologie nebo jím pověřený pracovník.

D.17.5 Typy bezpečnostních incidentů v ICT/IS dle příčiny a dopadu

Podle příčiny jsou bezpečnostní incidenty rozděleny do následujících typů:

a) bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb,

b) bezpečnostní incident způsobený škodlivým softwarem nebo kódem,
c) bezpečnostní incident způsobený kompromitací technických opatření,
d) bezpečnostní incident způsobený porušením organizačních opatření a
e) ostatní bezpečnostní incidenty způsobené kybernetickým útokem.

Podle dopadu jsou bezpečnostní incidenty rozděleny do následujících typů:

a) bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv,
b) bezpečnostní incident způsobující narušení integrity primárních aktiv,
c) bezpečnostní incident způsobující narušení dostupnosti primárních aktiv,
d) bezpečnostní incident způsobující kombinaci dopadů uvedených v písmenu a) až c).

D.17.6 Hlášení bezpečnostních událostí a slabin v ICT/IS

Bezpečnostní události musí Uživatel neprodleně hlásit na ServiceDesk (viz „*Metodický pokyn IT-SECPOL pro Uživatele*“). V rámci útvaru IT je aplikována eskalační procedura zajišťující pronikání informace o bezpečnostní události na trvalé členy IRT. Uživatel vždy kontaktuje Service Desk a postupuje podle pokynů Service Desku. Pracovníci Service Desku provedou sběr informací pro klasifikaci a prioritizaci bezpečnostní události, kterou následně provede IRT. V případě mimořádné situace nesouvisející s provozem ICT/IS kontaktuje Service Desk pracovníky oddělení Procesy a organizace, bezpečnost a ŽP.

Obdobným způsobem jako se hlásit bezpečnostní událost/slabinu, musí Uživatel hlásit na Service Desk i nalezení bezpečnostní slabiny (viz „*Metodický pokyn IT-SECPOL pro Uživatele*“). Bezpečnostní slabiny nemají přímý dopad na chod hlavních Aktiv ICT/IS, ale jejich další zneužití by mohlo vést k bezpečnostnímu incidentu. Service Desk kontaktuje IRT nebo aplikační správce a ve spolupráci s Manažerem, IT infrastruktura rozhodnou o dalším postupu eliminace slabiny. Jako bezpečnostní slabinu může identifikovat Uživatel např. neočekávanou reakci aplikace na vstupní data ve formuláři, získání přístupových práv do databáze, které nesouvisí s výkonem funkce Uživatele a podobně.

D.17.7 Reakce na výskyt bezpečnostního incidentu v ICT/IS

Členové IRT přebírají plnou zodpovědnost za reakci na výskyt incidentu. IRT řeší následující Aktivity:

- Detekce bezpečnostních událostí – IRT definuje příčinu vzniku incidentu, místo vzniku a Aktiva ICT/IS dotčená incidentem).
- Detailní identifikace a klasifikace, rozhodnutí, příprava řešení.
- Řešení bezpečnostního incidentu.
- Následná analýza a vyhodnocení řešení incidentu.

Po stanovení dopadů, kategorizaci a prioritizaci bezpečnostní události musí co nejrychleji rozhodnout, zda jde o bezpečnostní incident. Následně eskalují výskyt incidentu na členy Bezpečnostního výboru ICT/IS a informují ServiceDesk. Členové IRT důsledně zaznamenávají všechny Aktivity související s bezpečnostním incidentem a jeho řešením na sdíleném úložišti Společnosti (sharepoint) formou dokumentů MS Office a příloh. Přístup k úložišti mají jen členové IRT. V případě, že IRT nedokáže incident vyřešit vlastními silami musí být spuštěny obnovovací procedury dle plánů obnovy (viz. kapitola D.9).

Formální uzavření bezpečnostního incidentu provádí Service Desk, který následně informuje o uzavření rovněž uživatele dotčené bezpečnostním incidentem. Po vyřešení incidentu následuje opětovné posouzení průběhu řešení incidentu, zda tým IRT reagoval a postupoval efektivně. Rovněž Ředitel, Informační technologie či jím pověřená osoba vyhodnotí silné a slabé stránky odstraňování dopadů incidentu a provede jeho finální vyhodnocení.

D.17.8 Vyhodnocování incidentu v ICT/IS

Vyhodnocováním bezpečnostního incidentu přechází útvar IT od pasivní/reaktivní úlohy k úloze aktivní, resp. proaktivní. Vyřešením incidentu jsou zažehnány aktuální potíže Společnosti. Následná analýza a rozbor incidentu by měly přinést organizaci užitek z překonaných potíží. To znamená poučení z příčin vzniku incidentu a pak následná aktualizace analýzy bezpečnostních rizik. Na jejím základě jsou pak rizika přehodnocena. Obsahem etapy vyhodnocování incidentu jsou zejména:

- hlubší analýza bezpečnostního incidentu a její závěry,
- aktualizace dat o vyřešených bezpečnostních incidentech,
- poučení z incidentu pro potřeby zvyšování bezpečnostního povědomí v organizaci,
- dopady incidentu na proces i obsah řízení bezpečnostních incidentů.

Při pravidelném vyhodnocování bezpečnosti ICT/IS v organizaci jsou pak závěry získané z bezpečnostních incidentů využívány pro rozvoj a zdokonalování systému řízení bezpečnosti ICT/IS ve Společnosti.

D.17.9 Rozvoj systému řízení bezpečnostních incidentů v ICT/IS a jeho zlepšování

V této etapě jsou zkušenosti získané při řešení bezpečnostního incidentu zahrnuty do celého ISMS – tedy nejen do systému řízení bezpečnosti IS/ICT. Cílem je zejména zobecnit z bezpečnostního incidentu získané poznatky. Hlavními činnostmi jsou:

- zobecnit závěry z bezpečnostního incidentu směrem k analýze rizik, jejímu provedení a řízení,
- zobecnit dopady incidentu na řízení bezpečnosti ICT/IS Společnosti - aktualizace obsahu bezpečnostní dokumentace apod.,
- identifikovat a zavést případné změny do systému řízení bezpečnosti ve Společnosti.

E Související dokumentace a procesy

E.1 Vystavené dokumenty a záznamy

Název dokumentu	Forma („P“ – papírová / „E“ – elektronická)	Zpracovatel	Místo uložení	Doba uchování
-	-	-	-	-
-	-	-	-	-

E.2 Navazující dokumentace

E.2.1 Základní obecně závazné právní předpisy

Rozumí se ve znění pozdějších předpisů, tj. včetně všech novelizací, kterými se tyto zákony mění a doplňují:

- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
- Zákon č. 262/2006 Sb., zákoník práce

E.2.2 Řídicí dokumenty Společnosti

Řád:

- Organizační řád NET4GAS, s.r.o.
- Podpisový řád NET4GAS, s.r.o.
- Pracovní řád NET4GAS, s.r.o.
- Bezpečnostní řád NET4GAS s.r.o.

Směrnice:

- SM_I04_04_01 Řízení fyzické bezpečnosti v N4G
- SM_I04_07_01 Bezpečnostní pravidla pro ochranu informací
- N4G_SM_A09_02 Řízení rizik v NET4GAS, s.r.o.

Metodický pokyn:

- MP_C10_08_05 Ochrana dat (MP_I04_06_01_06)
- N4G_MP_A09_02_01 Řízení rizik v NET4GAS, s.r.o.
- MP_H01_00_02 Vzdělávání a rozvoj zaměstnanců

Bezpečnostní dokumentace dále určená přímo pro ICT/IS:

- SM_I04_06_02 Bezpečnostní politika IT / IT-SECPOL
- MP_I04_06_02_01 Metodický pokyn IT-SECPOL pro Uživatele
- MP_I04_06_02_02 Metodický pokyn IT-SECPOL pro Dodavatele
- MP_I04_06_02_03 Metodický pokyn IT-SECPOL pro ŘS a SCADA systémy
- MP_C10_08_06 Ochrana koncových stanic
- MP_H04_01_01_01 Metodika vedení IT projektů
- MP_H04_01_01_02 Řešení IT požadavků v rámci úseku Informační technologie NET4GAS, s.r.o.
- MP_H04_01_01_03 Řešení IT incidentů v rámci úseku Informační technologie NET4GAS, s.r.o
- SM_I04_06_01 Bezpečnostní pravidla pro práci s výpočetní technikou
- SM_I02_00 Směrnice nákupu a logistiky

POZNÁMKA: Čísla řídicí dokumentace uvedená v závorce odpovídají novému procesnímu uskupení.

E.2.3 Související procesy v procesní skupině

C.01 – Rozvoj procesů a organizace

C.01.07.7 – Audit POB

C.02 – Řízení rizik

F.03 – SCADA provozní technologie

H.01 – Lidské zdroje

H.04 – IT a Telco management

I.03 – Audit

I.04 – Bezpečnostní služby

I.04.03 – Krizové řízení a BCM

I.04.04 – Fyzická bezpečnost

I.04.06 – Řízení IT bezpečnosti

I.04.07 – Řízení bezpečnosti informací

F Závěrečná a přechodná ustanovení

Revizi tohoto dokumentu provádí Ředitel, Informační technologie minimálně jednou za dva roky. Revize může být provedena také na základě výsledků bezpečnostního auditu nebo jako důsledek významné změny bezpečnostních potřeb ICT/IS, vyvolané změnou legislativy, společenských nebo technologických podmínek.

Všechny revize jsou projednány v útvaru IT a útvaru SCADA provozní technologie, který je předkládá ke schválení bezpečnostnímu výboru ICT/IS.

Všechny změny musí být včas a řádně promítnuty do souvisejících procesů a dokumentace. Přijaté změny slouží jako podklady pro aktualizaci stávajících a přípravu nových interních předpisů společnosti.

Za přípravu, zpracování a revize řídicí dokumentace v rámci IT odpovídá Specialista IT, Kvalita a bezpečnost IT, ten také odpovídá za soulad řídicí dokumentace s nadřazenou dokumentací.

Směrnice nabývá účinnosti po schválení jednatelem Společnosti.

Metodické pokyny, týkající se správy ICT/IS a souvisejících nakupovaných služeb, nabývají účinnosti schválením Ředitele, Informační technologie.

Přechodné ustanovení: Po dobu 12 měsíců od prvotního schválení Bezpečnostní politiky ICT/IS (IT-SECPOL) platí přechodné období, během kterého musí útvar IT zajistit realizaci všech opatření uvedených v Bezpečnostní politice ICT/IS. Případná porušení politiky ze strany útvaru IT, která mají svou příčinu v nutnosti implementovat nová opatření definovaná touto politikou, budou po dobu přechodného období pouze evidována na úrovni Ředitele, Informační technologie a nejsou obecně považována za nesoulad s Bezpečnostní politikou ICT/IS či za bezpečnostní událost/incident v ICT/IS.

P Přílohy

Bez příloh.