Tento metodický pokyn je řídicím dokumentem společnosti NET4GAS, s.r.o.

Postupování třetím osobám je možné pouze se souhlasem jednatele společnosti nebo vlastníka procesu.

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

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

Tento dokument poskytuje přehled pravidel a zásad pro bezpečnou práci Dodavatele v prostředí ICT/IS společnosti NET4GAS, s.r.o. (dále jen „Společnost“) a při připojení pracovníků Dodavatele do prostředí Společnosti.

B Rozsah platnosti a kontrola

Tento řídicí dokument platí pro subjekty, které se zavázaly dodržovat Bezpečnostní dokumentaci Společnosti či jen dílčí bezpečnostní opatření Společnost v oblasti ICT/IS. Bezpečnostní požadavky a doporučení definované v tomto dokumentu jsou platné a závazné pro Dodavatele.

Kontrolu plnění tohoto metodického pokynu jsou oprávněni provádět pracovníci pověření útvarem IT Společnosti.

Za revizi a změny tohoto metodického pokynu a postupů v něm uvedených zodpovídá ve společnosti NET4GAS, s.r.o., vlastník procesu.

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.).
Autorizovaný Uživatel	Uživatel, který má určité právo nebo povolení pracovat v ICT/IS a s aplikacemi podle stanovených zásad přístupu.
Bezpečnostní dokumentace Společnosti	Obsahuje Bezpečnostní politika ICT/IS a nadřazené dokumenty Společnosti uvedené v kapitole D.1 tohoto dokumentu.
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 incident	Je jedna nebo více nechtěných nebo neočekávaných indikovaných bezpečnostních 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 organizaci Společnosti a jejich 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
Definovaná 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 organizaci. Takováto informace může pocházet i z více informačních zdrojů. Informační Aktiva ICT/IS 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.

Pojem / Zkratka	Definice
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.
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. Mobilní zařízení jsou chápána jako podmnožina Koncových zařízen, která jsou přenosná tj. mobilní.
Pracovní stanice	PC nebo notebook nebo technologické PC poskytující službu Uživateli, který má přímý fyzický přístup k tomuto zařízení.
Pracovníci	pracovníci Dodavatele včetně jejich subdodavatelů, kteří přistupují či mají v rámci sítě Dodavatele zajištěn přístup ICT/IS či přístup k datům/Informacím Společnosti
Přenosná média	přenosné paměťové nosiče datových informací (např. přenosný HDD, CD, DVD, USB disk atd.)
Service Desk	Jednotný bod servisní podpory Uživatelů, na který hlásí Uživatelé veškeré své požadavky ve spojitosti s ICT/IS s výjimkou požadavků na Řídicí systém a SCADA technologie pro které je provozován speciální service desk (kontaktní místo). *Poznámka: Historicky zaměstnanci Společnosti nazývají Service Desk jako „HelpDesk“. Z pohledu tohoto metodického pokynu Helpdesk=Service Desk včetně všech stávajících kontaktů a komunikačních kanálů na Helpdesk/Service Desk.*
Service Manager	Odpovědná osoba útvaru IT, která zodpovídá za chod Service Desku a úrovně jednotlivých služeb poskytovaných útvarem IT Uživatelům.
SM, Směrnice	Typ řídicího dokumentu, určuje metody, pravidla, postupy, prostředky pro výkon činností v procesech a jejich součinnost
Síťové disky	Definovaná úložiště na sdílených síťových discích
Společnost	Společnost NET4GAS, s.r.o
Subjekt	Jakákoliv osoba pracující s informacemi společnosti N4G 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, zaměstnanec třetí strany nebo jiná osoba, autorizovaná pro užití informací či zdrojů Společnosti ke svým pracovním povinnostem.
Windows doména	Mechanismus prosazování managementu a bezpečnosti na počítače s operačním systémem Microsoft 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

Společnost provozuje část kritické infrastruktury státu. Společnost je držitelem výhradní licence pro přepravu plynu (TSO) v České republice. Provozuje více než 3600 km plynovodů a její přepravní soustava je zárukou bezpečnosti a spolehlivosti, provozní dokonalosti a inovativních řešení, které respektují závazek Společnosti vůči budoucím generacím. Soustava Společnosti propojuje trhy do všech světových stran přeshraničními propoji. Společnost tak přispívá ke zvýšení energetické bezpečnosti nejen v České republice, ale v celém středoevropském regionu.

Ochrana Informačních Aktiv je zásadním principem i cílem Společnosti v oblasti bezpečnosti. Z tohoto pohledu podléhá Společnost regulaci a musí vyhovět mnoha zákonným normám a předpisům.

Tento metodický pokyn se zabývá ochranou Informačních Aktiv ICT/IS a ochranou vlastního zpracování Informačních Aktiv v rámci ICT/IS.

Veškeré nakládání s Informačními Aktivy je Dodavatel povinen podřídit pravidlům stanovených pro danou klasifikaci informací podle stupně jejich důvěrnosti. Třídu důvěrnosti informace stanoví vlastník Informačního aktiva. Tato pravidla definuje směrnice „Bezpečnostní pravidla pro ochranu informací“ vydaná útvarem Procesy a organizace, bezpečnost a ŽP Společnosti. Tato směrnice stanoví následující klasifikaci informačních aktiv podle stupně jejich důvěrnosti na Strategické, Určené, Interní a Veřejné. Pro každou z těchto klasifikačních tříd jsou ve zmíněné směrnici mimo jiné zavedena pravidla nakládání s informacemi patřícími do dané třídy/úrovně klasifikace. Z hlediska používání Informačních Aktiv ICT/IS jsou relevantní pravidla spočívající zejména v omezení předávání informací, označování dokumentů a principy ukládání informací.

D.1 Obecné postupy a pravidla pro ICT/IS

Oblast bezpečnosti ICT/IS je v rámci Společnosti popsána řadou dokumentů. Dodavatelé jsou povinní mimo tohoto metodického pokynu respektovat a postupovat v souladu s tím, co je uvedeno v následujících dokumentech (metodický pokyn je v tomto ohledu zjednodušeným výtahem aplikovaným pouze na oblast ICT/IS doplněným o konkrétní technické detaily). Dodavatelé a jejich zaměstnanci či pracovníci přistupující k ICT/IS musí dodržovat mimo jiné bezpečnostní zásady popsané v následujících interních řídicích dokumentech Společnosti:

(nadřazená bezpečnostní dokumentace):

- "*Bezpečnostní řád NET4GAS s.r.o.*“
- „*Bezpečnostní pravidla pro ochranu informací*“
- „*Ochrana dat*“ - Metodický pokyn pro práci s klasifikovanou informací
- „*Bezpečnostní směrnice ICT/IS*“
- „*Bezpečnostní politika IT*“ (IT-SECPOL)
- „*Metodický pokyn IT-SECPOL pro Uživatele*“
- *„Metodický pokyn IT-SECPOL pro ŘS a SCADA systémy“*

V následujících kapitolách je popsán seznam bezpečnostních požadavků a pravidel, které musí dodržovat Dodavatel. Pravidla jsou rozdělena do následujících oblastí:

- Základní odpovědnosti Dodavatele
- Nakládání s majetkem a Aktivy ICT/IS
- Přístup k ICT/IS
- Ochrana před škodlivým softwarem a ICT bezpečnostními riziky
- Reportování
- Kontrola a audit Dodavatele
- Ošetření výjimek.

D.2 Základní odpovědnosti Dodavatele

Dodavatel je při práci v ICT/IS společnosti NET4GAS, s.r.o., povinen:

a) dodržovat požadavky na bezpečnost informací v souladu s platnými předpisy Společnosti a ostatními normami – zákony ČR.

b) zajistit, že Pracovníci Dodavatele (včetně dalších subdodavatelů Dodavatele), kteří přistupují či mají přístup k ICT/IS budou postupovat v souladu s Bezpečnostní dokumentací Společnosti a to zejména v souladu s „*Metodickým pokynem IT-SECPOL pro Uživatele*“.

c) zajistit, že Pracovní stanice a obecně prostředí Pracovníků bude zabezpečeno v souladu s Bezpečnostní dokumentací Společnosti a to zejména v souladu s „*Metodickým pokynem IT-SECPOL pro Uživatele*“.

d) zajistit dodržování Bezpečnostní dokumentace (tj. zejména pravidel a opatření) na veškerých prostředcích v jeho odpovědnosti, které slouží nebo sloužily k zpracování, přístupu či uchovávání informací či dat Společnosti.

e) V případě, že je přímo propojena síť Dodavatele se sítí Společnosti, tak je Dodavatel povinen zajistit zabezpečení své Dodavatelské sítě v souladu s Bezpečnostní dokumentací Společnosti, tj. veškerá opatření obsažená v Bezpečností dokumentaci vztahující se k Prostředí Společnosti musí být splněna i pro prostředí Dodavatele. Za přímé propojení je z tohoto pohledu považováno jakékoliv propojení vyjma následujících přístupů:

   i. Přístup/připojení k veřejně dostupné části infrastruktury/služeb Společnosti (služby dostupné běžně z Internetu).

   ii. Přístup z individuálního počítače prostřednictvím VPN clienta (nikoliv site-to-site VPN, která je považovaná za metodu přímého propojení).

f) ukládat data Společnosti:

   i. v souladu s Bezpečnostní dokumentací Společnosti,

   ii. pouze na prostředky v majetku či přímé odpovědnosti Společnosti nebo požádat Společnost o udělení výjimky pro uložení těchto dat na prostředky mimo odpovědnost Společnosti.

   iii. na prostředky mimo majetek a/nebo odpovědnost Společnosti pouze na základě a v souladu se Společností písemně schválenou výjimkou.

Dodavatel je povinen akceptovat použití prostředků bezpečnostního auditu, které mohou být útvarem IT využity k sledování aktivit v prostředí ICT/IS či aktivity procházejících přes toto prostředí.

D.3 Nakládání s majetkem a Aktivy ICT/IS

D.3.1 Povolení užití majetku ICT/IS

V rámci zajištění poskytování služeb jsou Dodavateli v konkrétním případě na základě schválení Společnosti povoleny následující způsoby užití majetku ICT/IS:

- Pracovní stanice – Pracovní stanice se přiřazují do odpovědnosti konkrétní osoby Dodavatele. Dodavatel zajistí, že přidělenou pracovní stanici bude užívat pouze osoba, které byla tato přidělena. Tyto pracovní stanice jsou nakonfigurovány útvarem IT, tak se z nich bylo možné bezpečným způsobem připojit prostřednictvím VPN klienta do prostředí Společnosti. Administrativní úkony a správu stanice vykonává pouze útvar IT Společnosti. Osoba Dodavatel, které byla Pracovní stanice vydána je povinna užívat tuto Pracovní stanici v souladu s Bezpečnostní dokumentací Společnosti a to zejména v souladu s „Metodickým pokynem IT-SECPOL pro Uživatele“.
- Servery a ostatní majetek ICT/IS – užití tohoto majetku ICT/IS je povoleno pouze po uzavření právně závazného dokumentu (např. smlouvy) mezi Dodavatelem a Společností, který musí před vlastním podpisem za Společnost schválit Bezpečnostní výbor Společnosti či Manažer, IT infrastruktura Společnosti.

D.3.2 Převzetí, pohyb a vrácení Aktiv ICT/IS

Převzetí hmotného Aktiva stvrzuje Dodavatel svým podpisem „*Protokolu o předání hmotného a nehmotného majetku*“ při fyzickém převzetí informačního Aktiva. Podpisem tohoto protokolu Dodavatel potvrzuje, že převzal majetek od útvaru IT a že byl seznámen s pravidly užívání tohoto majetku, a že těmto pravidlům plně porozuměl a s jejich dodržováním souhlasí. Stejným mechanismem probíhá rovněž vrácení Aktiva útvaru IT. Požadavek na jakýkoliv přesun nebo poskytnutí Aktiv ICT/IS je realizován na základě žádosti příslušného Dodavatele předané na ServiceDesk.

Při zahájení smluvního vztahu s Dodavatelem je ve smlouvě nadefinován seznam Aktiv ICT/IS, která budou Dodavateli poskytnuta společností. Dodavatel poskytne na ServiceDesk potřebné informace pro předání Aktiv ICT/IS, S pracovníky ServiceDesk je následně domluven zejména čas a místo převzetí Aktiva ICT/IS.

Přesuny Aktiv ICT/IS mezi Dodavateli ICT/IS provádí pouze zaměstnanci útvaru IT na základě výše uvedeného postupu. Záznam o změně eviduje útvar IT ve své operativní evidenci v rámci Service Desku. Jakékoliv jiné nakládání s výjimkou prostého užití Aktiva ICT/IS Dodavatelem není povoleno.

Pozor: Při ukončení smluvního vztahu Dodavatel zajistí vrácení všech Aktiv ICT/IS.

D.3.3 Způsob a procedury předávání informací a dat v rámci ICT/IS

Pro přenos dat mezi Dodavatelem a subjekty pracujícími v sítích společnosti, lze použít pouze schválená technologie. Mezi schválené technologie patří zejména:

- Přenos zpráv pomocí el. pošty
- Přenos zpráv pomocí datových schránek (není řešeno v tomto MP)
- Sdílení souborů na Definovaných úložištích
- Předávání dat pomocí médií USB flash disky, CD/DVD a další

Pro uvedené technologie přenosu jsou nadefinovány bezpečnostní zásady v „*Metodickém pokynu IT-SECPOL pro Uživatele*“. Pro ochranu elektronického přenosu dat přijímá útvar IT speciální bezpečnostní opatření. Za adekvátní způsob ochrany se považuje šifrování dat, kryptografické podepsání dat nebo fyzická ochrana médií přenášených Dodavatelem ICT/IS.

D.3.4 Zpracování či uchování dat a Informací Společnosti na ICT prostředcích Dodavatele

Zpracování či uchování dat a Informací Společnosti na ICT prostředcích Dodavatele není s výjimkou informací klasifikovaných jako **Veřejné** obecně povoleno. Zpracování či uchování Informací stupně **Interní a vyšší** je povoleno pouze po uzavření právně závazného dokumentu (např. smlouvy) mezi Dodavatelem a Společností, který musí před vlastním podpisem za Společnost schválit:

- pro Informace klasifikované jako **Interní** Manažer, IT infrastruktura nebo Ředitel, Informační technologie;
- pro Informace klasifikované jako **Určené** Ředitel, Informační technologie;
- pro informace klasifikované jako **Strategické** Bezpečnostní výbor.

Součástí právně závazného dokumentu (např. formou rozšířeného NDA – vlastní NDA je typicky pouze o mlčenlivosti viz kapitola D.3.5) musí být také závazek Dodavatele zajistit zabezpečení dat a Informací na ICT prostředcích Dodavatele minimálně na shodné úrovni zabezpečení jak předepisuje Bezpečnostní dokumentace Společnosti pro zabezpečení dat a Informací v rámci ICT/IS včetně řádné implementace všech opatření obsažených v Bezpečnostní dokumentaci Společnosti.

Pokud Dodavatel zpracovává či uchovává data/Informace klasifikovaná na stupeň Interní či vyšší, tak je navíc povinen tato data/informace a infrastrukturu ve které se nacházejí zabezpečit v souladu s technickými dodatky vydanými Společností a platnými v daném čase. Dodavatel obdrží relevantní technické dodatky od manažera, IT infrastruktura Společnosti s dostatečným předstihem před zahájením jejich platnosti či s dostatečným předstihem před vlastním zpracováním dat/informací Společnosti na ICT prostředcích Dodavatele.

Společnost má obecné právo auditu prostředí Dodavatele za účelem ověření dodržování Bezpečnostní dokumentace Společnosti či za účelem ověření zabezpečení dat a informací na ICT prostředcích Dodavatele a to minimálně 1x za 12 měsíců. Toto právo Společnosti musí být součástí právně závazného dokumentu mezi Dodavatelem a Společností. V případě zpracování dat/informací klasifikovaných na stupeň *Interní* a vyšší na ICT prostředcích Dodavatele má Společnost obecně právo provést 1x za 24měsíců předem neohlášený audit. Obecné právo neohlášeného auditu může být upraveno právně závazným dokumentem mezi Dodavatelem a Společností (např. v případě, kdy takový neohlášený audit není prakticky proveditelný z důvodů bezpečnostních opatření na straně Dodavatele) a v takovém případě schvaluje právně závazný dokument před podpisem za Společnost výhradně Bezpečnostní výbor Společnosti.

D.3.5 Dohoda o mlčenlivosti (NDA/CA)

Dodavatel se před vlastním **přístupem** k datům a informacím Společnosti musí zavázat mlčenlivostí. Tzn., že platí povinnost Dodavatele se zavázat a také povinnost pracovníků Společnosti zavázat Dodavatele a nezpřístupnit data a informace Dodavateli dříve, než dojde k jeho závazku mlčenlivosti (tj. podpisu NDA – Non Disclosure Agreement či CA – Confidentiality Agreement).

Dohoda o mlčenlivosti musí obsahovat minimálně:

- definici důvěrných informací
- definici závazku mlčenlivosti
- stanovení sankce při porušení mlčenlivosti
- způsoby sdělování a zaznamenávání důvěrných informací
- účel poskytnutí důvěrných informací
- možnost zproštění mlčenlivosti.

D.4 Přístup k ICT/IS

Pro účely autentizace Dodavatelů ICT/IS se používá účinný mechanismus pro práci s hesly aplikovaný na celou sadu svěřených koncových zařízení spravovaných ve Windows doméně. Přihlášení Dodavatele do sítě Společnosti musí podléhat kontrole přístupu na základě autorizace po předchozí autentizaci, včetně autentizace přes VPN v případě užití VPN klienta. Přihlašovací proces do VPN a do Windows domény poskytuje základní bezpečnostní funkce – nikdy se nezobrazuje vkládané heslo a heslo není nikde přenášeno a ukládáno v nezašifrované formě. Přístup ke službám ICT/IS je vždy zajištěn přes proces autentizace, autorizace a bezpečnostního auditu. Tyto bezpečnostní opatření prosazují rovněž aplikace používané ve Společnosti.

Vlastní přihlašovací proces je popsán v rámci interního řídicího dokumentu „*Metodický pokyn IT-SECPOL pro Uživatele*“.

D.4.1 Nestandardní provozní procedury ICT/IS

Při provozu Aktiv ICT/IS jsou útvarem ICT/IS maximálně dodržovány dohodnuté zásady a standardy. Přesto nejde vyloučit nutnost použití nestandardních postupů např. během výskytu bezpečnostního incidentu. Dodavatel stvrzuje svým podpisem při převzetí Aktiv ICT/IS, že byl seznámen s bezpečností práce s IT technikou, bezpečnostními směrnicemi IT a s IT směrnicemi umístěnými na Intranetu Společnosti. V těchto směrnicích je uveden seznam postupů, jak jsou řešeny běžné každodenní situace v infrastruktuře ICT/IS.

D.5 Ochrana před škodlivým softwarem a ICT bezpečnostními riziky

Ochrana před škodlivým softwarem je rozdělena do tří oblastí:

I. Ochrana Uživatele a jeho Pracovní stanice – zde musí Dodavatel vyhovět veškerým požadavkům a implementovat veškerá opatření uvedená v dokumentu „*Metodický pokyn IT-SECPOL pro Uživatele*“. V případě užití Pracovní stanice Společnosti opatření realizovaná nastavením na Pracovní stanici zajistí útvar IT Společnosti (upozornění: *jedná se pouze o část opatření*).

II. Ochrana celého prostředí Dodavatele – Dodavatel je povinen:

   a. Centrálně organizovat zabezpečení koncových stanic v připojeních do jeho infrastruktury (např. řízení personálních firewallů, antivirového SW atd.) a to minimálně na úrovni standardů Společnosti.

   b. Obsahem antivirové ochrany jsou taková opatření technického a administrativního charakteru, která vedou k detekci a následnému odstranění infiltrujícího software u všech prostředků provozovaných v rámci infrastruktury Dodavatele.

   c. Dodavatel musí na své straně definovat zásady bezpečného užívání Internetu a s těmito zásadami seznámit veškerý personál užívající ICT prostředky infrastruktury Dodavatele.

   d. Dodavatel musí na pracovních stanicích v jeho odpovědnosti zajistit bezpečné nakonfigurování prohlížečů obsahu Internetu (např. www prohlížeče).

   e. Hesla nezbytná k přístupu do pracovníků Dodavatele na zdroje Dodavatele i Společnosti nesmí být v sítí přenášena v otevřené podobě.

   f. Hesla pracovníků Dodavatele nebudou zaznamenávána v otevřené podobě.

III. Vzájemná spolupráce a komunikace mezi Dodavatelem a Společností při řešení ICT bezpečnostní rizik

   a. Dodavatel bezprostředně informuje Společnost o bezpečnostních incidentech v rámci jeho infrastruktury viz kapitola D.6 tohoto MP.

   b. V případě, kdy se vyskytne v prostředí Dodavatele či na jeho rozhraní potenciální hrozba, kterou by mohl být zasažena i Společnost, tak je Dodavatel povinen bezprostředně tuto hrozbu reportovat Společnosti viz kapitola D.6.

   c. Pracovníci Dodavatel přistupující do IT prostředí Společnosti reportují nestandardní situace, identifikované slabiny a bezpečnostní události při práci v ICT/IS Společnosti viz kapitola D.6.

   d. Dodavatel řádně reaguje na informace o bezpečnostních incidentech obdržené od Společnosti a implementuje patřičná opatření v souvislosti s těmito bezpečnostními incidenty.

D.6 Reportování

D.6.1 Reportování nestandardních situací a slabin v prostředí Společnosti

Dodavatel je povinen reportovat / hlásit:

- nestandardní situace při práci v ICT/IS;
- bezpečnostní události nad ICT/IS;
- bezpečnostní slabiny v ICT/IS

Hlášení nestandardních situací, událostí a slabin v prostředí Společnosti je popsáno metodickým pokynem pro Uživatele viz „*Metodický pokyn IT-SECPOL pro Uživatele*“.

D.6.2 Reportování nestandardních situací a slabin v prostředí Dodavatele

Dodavatel je povinen reportovat relevantní bezpečnostní incidenty ze svého ICT prostředí Bezpečnostnímu výboru Společnosti.

- V případě, kdy přistupují pracovníci Dodavatele pouze individuálně do ICT/IS Společnosti prostřednictvím VPN klienta, tak za relevantní bezpečnostní incident jsou považovány veškeré incidenty týkající se klientského prostředí (tj. koncových pracovních stanic).
- V případě, kdy je propojena infrastruktura Společnosti s infrastrukturou Dodavatele (např. prostřednictvím site-to-site VPN) či Dodavatel zpracovává či uchovává na svých ICT prostředcích data/Informace Společnosti, tak za relevantní jsou považovány veškeré bezpečnostní incidenty v prostředí Dodavatele.

D.7 Kontrola a audit Dodavatele

Společnost má obecné právo auditu prostředí Dodavatele za účelem ověření dodržování Bezpečnostní dokumentace Společnosti či za účelem ověření zabezpečení dat a informací na ICT prostředcích Dodavatele a to minimálně 1x za 12 měsíců. V případě zpracování či uchování dat/informací Společnosti na ICT prostředcích Dodavatele je právo auditu dále rozšířeno a upraveno kapitolou D.3.4 „Zpracování či uchování dat a Informací Společnosti na ICT prostředcích Dodavatele“.

V případě, kdy Dodavatel plní část ICT služeb prostřednictvím svého subdodavatele, tak musí:

a) zajistit nejen přenos povinnosti zabezpečení, mlčenlivost atd., ale i vymahatelnost práva auditu ze strany Společnosti vůči tomuto subdodavateli a to v plném rozsahu a
b) pravidelně minimálně na roční bázi pravidelně provádět audity svých subdodavatelů a předkládat relevantní výstupy a zjištění auditu Bezpečnostnímu výboru Společnosti.

V případě, kdy je propojena infrastruktura Společnosti s infrastrukturou Dodavatele (např. prostřednictvím site-to-site VPN) či Dodavatel zpracovává či uchovává na svých ICT prostředcích data/Informace Společnosti, tak musí Dodavatel překládat výstupy a zjištění bezpečnostního auditu svého prostředí/infrastruktury Bezpečnostnímu výboru Společnosti.

Útvarem IT je běžně prováděn monitoring aktivit Uživatelů tj. i monitoring aktivit Uživatelů z řad pracovníků Dodavatele a to v souladu s dodržováním práv na ochranu soukromí zaměstnanců/pracovníků. Důvodem monitorování aktivit Uživatelů je ochrana zájmů Společnosti a kontrola využívaní svěřených Aktiv ICT/IS. V rámci ICT/IS jsou prakticky všechny činnosti Dodavatelů zaznamenávány nejen na úrovní operačního systému (přihlášení do sítě, špatně zadané heslo, atd.) ale také na úrovní aplikací (přihlášení, vložení, úprava nebo smazání údajů, atd.). Při monitoringu je důraz kladen hlavně na kontrolu při provádění kritických nebo nestandardních transakcí. Relevantní informace jsou průběžně zpracovávány a uchovávány pro potřeby zpětného šetření. Podrobně jsou také monitorovány činnosti spojené s internetovou komunikací (navštívené web stránky, odeslané/přijaté emaily – nekontroluje se obsah zprávy, ale čas odeslání/příjmu zprávy, kdo, komu). Rovněž jsou monitorovány aktivity Dodavatele v síti. Útvar IT sleduje přihlášení, změny konfigurace a nestandardní chování aktivních prvků sítě.

D.8 Ošetření výjimek

Ve výjimečných případech je možno vyhlásit výjimku z dodržování pravidel stanovených tímto metodickým pokynem. Udělení výjimek ze stanovených pravidel se provádí na základě požadavku zaslaného Řediteli, Informační technologie, který má právo výjimku udělit.

E Související dokumentace

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.

F Závěrečná a přechodná ustanovení

Tento metodický pokyn nabývá účinnosti dnem jeho vydání.

P Přílohy

Bez příloh.