č. j. NPÚ: NPU-362/35069/2020

**evid. číslo NPÚ: S/NPÚ-362/13/2020**

(dodatek č. 1 ke smlouvě č. S/NPÚ-362/23/2019)

**Smluvní strany**

**Národní památkový ústav,** státní příspěvková organizace

IČO 75032333, DIČ CZ75032333

se sídlem Valdštejnské náměstí 162/3, 118 01 Praha 1 – Malá Strana

zastoupený Ing. x, ředitelem územního odborného pracoviště v Josefově

bankovní spojení: x, číslo účtu: x

ID DS: x

**doručovací a kontaktní adresa:**

Národní památkový ústav, územní odborné pracoviště v Josefově, Okružní 418, 551 02 Jaroměř – Josefov

(dále jako „**Objednatel“** na straně jedné)

a

**ALPHA StylSoft, s.r.o.**

IČO 25978152, DIČ CZ25978152

se sídlem x

adresa provozovny: x

zastoupený jednatelem x

kontakt: tel.: x, mailto: [x](mailto:info@stylsoft.cz)

bankovní spojení: x, číslo účtu: x

ID datové schránky: x

**doručovací adresa:** x

(dále jako „**Zhotovitel“** na straně druhé)

uzavřely níže uvedeného dne, měsíce a roku tento

**DODATEK č. 1**

**ke smlouvě o dílo č. S/NPÚ-362/23/2019**

**komplexní správa ICT v NPÚ ÚOP v Josefově na dobu 24 měsíců**

(dále jen **„Dodatek č. 1“**)

**Článek I.**

**Úvodní ustanovení**

1. Smluvní strany uzavřely dne 17. 10. 2019 smlouvu o dílo č. S/NPÚ-362/23/2019 (ID v registru smluv 9738382), kterou byl mimo jiné sjednán způsob evidence a správy komponent informačních a komunikačních technologií, správy počítačové sítě, zálohování dat a ochrany osobních údajů (dále jen „Smlouva“).
2. Objednatel konstatuje, že je při provozu informačních a komunikačních technologií a informačních systémů povinen ode dne 18. 3. 2020 dodržovat vnitřní předpis upravující pravidla a postupy pro správu informačních technologií a informačních systémů (dále jen „Směrnice“). Zhotovitel byl s obsahem Směrnice seznámen dne 23. 3. 2020, s novelizovaným zněním Směrnice byl seznámen dne 2. 11. 2020. Objednatel se zavazuje Zhotovitele informovat o všech změnách Směrnice přijatých po uzavření tohoto Dodatku č. 1 s tím, že smluvní strany, bude-li to vzhledem ke změnám Směrnice třeba, upraví svá vzájemná práva a povinnosti ze Smlouvy dalším dodatkem. Směrnice je jako příloha č. 2 nedílnou součástí tohoto Dodatku č. 1.
3. Tímto Dodatkem č. 1 se upravuje předmět Smlouvy v návaznosti na ustanovení Směrnice, doplňují se termíny plnění nově sjednaných prací, cena nově sjednaných prací a podmínky jejich úhrady.

**Článek II.**

**Předmět Dodatku č. 1**

1. Dodatkem č. 1 se rozšiřuje Předmět Smlouvy o
   1. závazek Zhotovitele k následujícímu plnění:
      1. příprava Přístupových údajů ve formátu požadovaném Směrnicí a jejich předání Odpovědné osobě Objednatele, poté aktualizace Přístupových údajů minimálně 1x ročně nebo v případě bezpečnostního incidentu nebo v souvislosti s ukončením smluvního vztahu – viz čl. 6 Směrnice;
      2. zajištění informovanosti externích uživatelů sítě Wi-Fi o způsobu zpracování osobních údajů – viz čl. 4.5 a čl. 7.5 Směrnice, příloha č. 3 Směrnice; každoroční kontrola aktuálnosti podávaných informací a jejich dostupnosti;
      3. kontrola nastavení kamerového systému dle čl. 5.1.3.3 Směrnice a zpřístupnění informace o tomto nastavení dle čl. 5.1.3.3.2 Směrnice;
      4. zpracování dokumentace vybraných základních prvků IT a infrastruktury IT, poté průběžná aktualizace dokumentace vybraných základních prvků IT a infrastruktury IT - čl. 4.3, čl. 7.1 a čl. 7.4 Směrnice, příloha č. 1 Směrnice;
      5. revize stávajících postupů zálohování a archivace dat v kontextu s obsahem Směrnice, nastavení postupů zálohování a archivace dat dle Směrnice a jeho údržba – čl. 4.6 Směrnice, čl. 7.6, příloha č. 4 Směrnice
      6. zpracování dokumentace vybraných ostatních prvků IT a infrastruktury IT, poté průběžná aktualizace dokumentace vybraných ostatních prvků IT a infrastruktury IT - čl. 4.3, čl. 7.1 a čl. 7.4 Směrnice, příloha č. 1 Směrnice.
   2. závazek Objednatele
      1. poskytnout Zhotoviteli potřebné podklady pro plnění dle odst. 1.1,
      2. poskytnout Zhotoviteli plnou součinnost při naplňování účelu Směrnice jako celku a tohoto Dodatku č. 1.
2. Zhotovitel prohlašuje, že byl Objednatelem seznámen se skutečností, že uskutečnění jednotlivých částí plnění dle odst. 1.1 je podmíněno přidělením příslušné částky ze státního rozpočtu a rozsah plnění sjednaného v odst. 1.1 proto může být zúžen v závislosti na výši přidělené částky. Vyvstane-li nutnost zúžení tohoto sjednaného plnění, Objednatel se zavazuje o tomto Zhotovitele bezodkladně a prokazatelnou formou informovat a sjednat s ním nový rozsah plnění.

**Článek III.**

**Termíny plnění**

1. Zhotovitel se zavazuje provést plnění sjednaná v čl. 1.1 tohoto Dodatku č. 1 v termínech, jejichž specifikace je uvedená v příloze č. 1 tohoto Dodatku č. 1.
2. Objednatel se zavazuje předat Zhotoviteli podklady dle čl. II. odst. 1.2.1 Dodatku č. 1 do 5 dnů ode dne nabytí účinnosti Dodatku č. 1.

**Článek IV.**

**Cena plnění z Dodatku č. 1 a podmínky fakturace**

1. Smluvní strany se dohodly, že plnění v rozsahu Dodatku č. 1 bude fakturováno v cenové sazbě totožné se sazbou za služby poskytované Zhotovitelem dle Smlouvy na kontaktní adrese/v sídle Objednatele nebo prostřednictvím vzdálené správy ze sídla/z místa provozovny Zhotovitele, tj. v sazbě 380,- Kč bez DPH za 1 hod výkonu.
2. **Maximální rozsah prací souvisejících s plněním předmětu Dodatku č. 1 je 340 hodin.**
3. **Maximální cena plnění z Dodatku č. 1 činí bez DPH 129.200 Kč, 156.332 Kč včetně DPH** s tím, že maximální ceny pro jednotlivá dílčí plnění vymezená v čl. II. odst. 1.1.1 až 1.1.6 jsou uvedeny v příloze č. 1 tohoto Dodatku č. 1.
4. **Smluvní strany sjednaly, že celková cena Díla na základě Smlouvy ve znění tohoto Dodatku č. 1, která je uvedena v čl. IV. odst. 3 Smlouvy se mění a nově nesmí přesáhnout částku ve výši 819.200,- Kč bez DPH (991.232,- Kč včetně DPH).**
5. Práce sjednané Dodatkem č. 1 budou fakturovány odděleně od prací dle Smlouvy, tj. na samostatných daňových dokladech, vždy po převzetí řádně zhotoveného dílčího plnění specifikovaného v čl. II. odst. 1.1.1 až 1.1.6 a na základě výkazu skutečného počtu hodin potřebných pro realizaci plnění.

**Článek V.**

**Závěrečná ustanovení**

1. Dodatek č. 1 nabývá platnosti podpisem Smluvních stran a účinnosti dnem zveřejnění dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Zveřejnění Dodatku č. 1 postupem dle zákona o registru smluv zajistí Objednatel.
2. Nedílnou součástí Dodatku č. 1 je příloha č. 1 obsahující položkový rozpis, termíny a finanční rozpočet plnění dle Dodatku č. 1. a příloha č. 2 obsahující Směrnici ve znění k datu podpisu Dodatku č. 1.
3. Ostatní ustanovení Smlouvy zůstávají beze změn.
4. Dodatek č. 1 je vyhotoven v počtu 3 (slovy: tří) stejnopisů, z nichž 2 (slovy: dva) stejnopisy obdrží Objednatel a jeden stejnopis obdrží Zhotovitel.
5. Smluvní strany prohlašují, že si Dodatek č. 1 přečetly, Dodatek č. 1 je pro ně určitý, srozumitelný, s jeho obsahem souhlasí. Smluvní strany dále prohlašují, že Dodatek č. 1 uzavírají ze své vážné a svobodné vůle, nikoliv v tísni nebo za nápadně nevýhodných podmínek. Na důkaz výše uvedeného prohlášení připojují osoby oprávněné jednat za Smluvní strany své podpisy.

V Josefově, dne 23. 11. 2020 V Jaroměři, dne 23. 11. 2020

…….................................................... ………...................................................

x x

ředitel NPÚ ÚOP v Josefově za Zhotovitele

za Objednatele

Příloha:

1. Položkový rozpis a finanční rozpočet plnění dle Dodatku č. 1

2. Směrnice o správě informačních technologií ve znění k datu podpisu Dodatku č. 1

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Příloha č. 1 k Dodatku č. 1 ke smlouvě č. S/NPÚ-362/23/2019 - položkový rozpis a finanční rozpočet plnění dle Dodatku č. 1** | |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| **číslo položky plnění dle Dodatku č. 1** | **položka plnění dle Dodatku č. 1** | **odkaz na vnitřní předpis a navazující dokumenty** | **termín plnění** | **hodinová sazba v Kč bez DPH** | **maximální počet hodin výkonu CELKEM** | **CELKOVÁ maximální cena PLNĚNÍ DLE Dodatku č. 1 v Kč bez DPH** | **CELKOVÁ maximální cena PLNĚNÍ DLE Dodatku č. 1 v Kč včetně DPH** | **rozpis výkonů v letech 2020 - 2021** |
| 1 | příprava Přístupových údajů ve formátu požadovaném Směrnicí a jejich předání Odpovědné osobě Objednatele, poté aktualizace Přístupových údajů minimálně 1x ročně nebo v případě bezpečnostního incidentu nebo v souvislosti s ukončením smluvního vztahu | čl. 6.Směrnice | **30. 11. 2020**, poté minimálně 1x ročně vždy do **30.11. běžného roku,** kdykoliv při bezpečnostním incidentu a  při ukončení smluvního vztahu | 380,00 | **20** | **7 600,00** | **9 196,00** |
| 2 | zajištění informovanosti externích uživatelů sítě Wi-Fi o způsobu zpracování osobních údajů a pravidelná 1-roční kontrola aktuálnosti informací a jejich dostupnosti | čl. 4.5 a čl. 7.5 Směrnice, příloha č. 3 Směrnice | **30.11.2020,** poté kontrola 1x ročně spolu s kontrolou a aktualizací dokumentce ICT, tj. k 28. 2. běžného roku | 380,00 | **0** | **0,00** | **0,00** |
| 3 | kontrola nastavení kamerového systému dle čl. 5.1.3.3 Směrnice a zpřístupnění informace o tomto nastavení dle čl. 5.1.3.3.2 Směrnice | čl. 5.1.3.3 Směrnice | **30.11.2020**, poté kontrola 1x ročně spolu s kontrolou a aktualizací dokumentce ICT, tj. k 28. 2. běžného roku | 380,00 | **0** | **0,00** | **0,00** |
| 4 | zpracování dokumentace vybraných ZÁKLADNÍCH(\*) prvků IT a infrastruktury IT,  poté průběžná aktualizace dokumentace vybraných ZÁKLADNÍCH prvků IT a infrastruktury IT | čl. 4.3, čl. 7.1 a čl. 7.4 Směrnice, příloha č. 1 Směrnice | **18. 3. 2021**, poté aktualizace k 28. 2. běžného roku | 380,00 | **180** | **68 400,00** | **82 764,00** |
| 5 | revize stávajících postupů zálohování a archivace dat v kontextu s obsahem Směrnice, nastavení postupů zálohování a archivace dat dle Směrnice a jeho údržba | čl. 4.6 a 7.6 Směrnice, příloha č. 4 Směrnice | **18.3.2021** | 380,00 | **60** | **22 800,00** | **27 588,00** |
| 6 | zpracování dokumentace vybraných OSTATNÍCH(\*\*) prvků IT a infrastruktury IT,  poté průběžná aktualizace dokumentace vybraných OSTATNÍCH prvků IT a infrastruktury IT | čl. 4.3, čl. 7.1 a čl. 7.4 Směrnice, příloha č. 1 Směrnice | **18. 9. 2021**, poté aktualizace k 28. 2. běžného roku | 380,00 | **80** | **30 400,00** | **36 784,00** |
|  |  |  |  |  | **340** | **129 200,00** | **156 332,00** |
| (\*) | základní prvky ICT jsou v příloze č. 1 Směrnice zvýrazněny šedým podbarvením textu | | |  |  |  |  |  |
| (\*\*) | ostatní prvky ICT jsou v příloze č. 1 Směrnice uvedeny bez zvýraznění textu | | |  |  |  |  |  |

pokračování tabulky

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **maximální cena plnění v r. 2020** | |  | **maximální cena plnění v r. 2021 bez DPH** | |
| **rozpis výkonů v letech 2020 - 2021** | **maximální rozsah plnění v r. 2020 (počet hodin výkonu)** | **bez DPH** | **včetně DPH** | **maximální rozsah plnění v r. 2021 (počet hodin výkonu)** | **bez DPH** | **včetně DPH** |
| **20** | 7 600,00 | 9 196,00 | **0** | 0,00 | 0,00 |
| **0** | 0,00 | 0,00 | **0** | 0,00 | 0,00 |
| **0** | 0,00 | 0,00 | **0** | 0,00 | 0,00 |
| **80** | 30 400,00 | 36 784,00 | **100** | 38 000,00 | 45 980,00 |
| **30** | 11 400,00 | 13 794,00 | **30** | 11 400,00 | 13 794,00 |
| **0** | 0,00 | 0,00 | **80** | 30 400,00 | 36 784,00 |
| **130** | **49 400,00** | **59 774,00** | **210** | **79 800,00** | **96 558,00** |

**Příloha č. 1 k Dodatku č. 1 ke smlouvě č. S/NPÚ-362/23/2019 –** Směrnice o správě informačních technologií ve znění k datu podpisu Dodatku č. 1

SMĚRNICE NÁRODNÍHO PAMÁTKOVÉHO ÚSTAVU

|  |  |  |  |
| --- | --- | --- | --- |
| **Druh vnitřního předpisu:** | **Směrnice GŘ č. XXII/2020/NPÚ** | **Číslo jednací** | **NPU-310/82165/2020** |
| **Název:** | **o správě informačních technologií** | | |
| **Vydává:** | generální ředitelka | | |
| **Platí pro:** | NPÚ | | |
| **Účinnost od:** | dnem podpisu | | |
| **Účinnost:** | na dobu neurčitou | | |
| **Provádí vnitřní předpis:** | - | | |
| **Ruší vnitřní předpis:** | Směrnice GŘ č. XXIX/2019/NPÚ o správě informačních technologií (čj. NPU-310/98383/2019) | | |
| **Odpovědný útvar:** | sekce prvního náměstka GŘ, odbor informatiky | | |
| **Zpracovatel:** | Ing. Petr Volfík | | |
| **Anotace:** | Tato směrnice stanovuje pravidla a postupy pro správu informačních technologií a informačních systémů v NPÚ. Aktualizovaná verze upravuje termíny plnění některých úkolů. | | |
| **Počet a specifikace příloh:** | 1. Pokyny k vedení dokumentace ICT 2. Bezpečnostní standardy pro informační systémy 3. Informace o zpracování osobních údajů pro Wi-Fi síť 4. Pravidla a doporučení pro zálohování 5. Vzor dokumentace k aktivním prvkům | | |

**Obsah vnitřního předpisu:**

[1 Účel vnitřního předpisu, úvodní ustanovení 2](#_Toc31360713)

[2 Rozsah platnosti 2](#_Toc31360714)

[3 Použité zkratky a vymezení pojmů 2](#_Toc31360715)

[4 Pravidla pro správu Počítačové sítě a Prostředků IT 4](#_Toc31360716)

[5 Bezpečnostní standardy pro zabezpečení Serveroven 6](#_Toc31360717)

[6 Pravidla pro Přístupové údaje ke správě Infrastruktury IT a jejich předávání 7](#_Toc31360718)

[7 Přechodná a závěrečná ustanovení 9](#_Toc31360719)

Účel vnitřního předpisu, úvodní ustanovení

## Účelem této směrnice je stanovit pravidla pro správu informačních technologií a informačních systémů v Národním památkovém ústavu (dále jen „NPÚ). Cílem je stanovit postupy pro správu technických prostředků výpočetní techniky i programového vybavení.

Rozsah platnosti

## Směrnice je závazná pro interní i externí správce IT NPÚ.

## Osoba oprávněná uzavřít smlouvu na služby IT, kterých se dotýká tato směrnice, je povinna zajistit, aby postupy a zásady stanovené touto směrnicí byly smluvně závazné i pro externí správce IT.

Použité zkratky a vymezení pojmů

## Seznam zkratek

### SW – software, programové vybavení pro výpočetní techniku

### HW – hardware, technické prostředky výpočetní techniky

### ICT – informační a komunikační technologie

### IT – informační technologie, soubor HW a SW

### OS – operační systém, základní programové vybavení počítače (např. Windows 10)

### IS – informační systém, uživatelský SW řešící základní agendu firmy

### PC – osobní počítač

### SLA - Service Level Agreement, dohoda o úrovni poskytovaných služeb

### PZTS – poplachové zabezpečovací a tísňové systémy

### MBOU - manažer bezpečnosti osobních údajů[[1]](#footnote-1)

## Definice pojmů pro účely této směrnice

### **Pojmem IT** se pro účely této směrnice rozumí veškeré hardwarové, softwarové a další technické prostředky výpočetní a telekomunikační techniky používané v prostorách budov všech pracovišť NPÚ nebo připojené (i vzdáleně) do počítačové sítě NPÚ.

### **Počítačová síť** zahrnuje veškeré Počítače, servery, tiskárny a další hardwarová zařízení používaná v prostorách budov všech pracovišť NPÚ a připojená k Počítačové síti, instalovaný software na těchto Počítačích, serverech a dalších zařízeních, a veškeré pasivní (kabeláž, rozvaděče, zásuvky apod.) a aktivní (switche, routery, access pointy apod.) prvky zajišťující provoz Počítačové sítě a její připojení do Internetu (firewally apod.).

### **Počítač** je osobní počítač (PC), notebook či obdobné zařízení (např. tablet, PDA, včetně počítače nepřipojeného k Počítačové síti), využívaný pro běžnou práci Uživatelů, přístup a zpracování dat NPÚ.

### **Prostředek IT** je Počítač, Mobilní telefon nebo jiné zařízení určené pro elektronickou komunikaci a zpracování dat pro NPÚ.

### **Sdílený dis**k je prostor na serveru, sdíleném diskovém úložišti v rámci počítačové sítě nebo cloudové diskové úložiště, které slouží pro ukládání a sdílení dokumentů NPÚ.

### **Firemní email** – osobní e-mailová adresa přidělená zaměstnanci a případně též externím pracovníkům, pokud se smluvně podílejí na činnosti NPÚ, v systému elektronické pošty NPÚ v souladu se směrnicí o užívání elektronické pošty[[2]](#footnote-2).

### **Technická zařízení zajišťující provoz počítačové sítě** jsou zařízení a prostředky umožňující propojit počítače a servery a připojit celou počítačovou síť do počítačové sítě a k Internetu (aktivní prvky, router, HW firewall, access point, wifi router atd.).

### **Uživatel j**e každá osoba, která používá jakýkoliv Prostředek IT, má zpravidla přiřazeno Uživatelské ID, přístupové heslo, přístupová práva a Firemní email.

### **Uživatelská aplikace** je SW nebo IS, který řeší podporu konkrétní činnosti nebo okruhu činností Uživatelů.

### **Systém** zahrnuje operační systémy na serverech a klientských zařízeních, informační systémy a sdílené aplikace, ve kterých lze definovat uživatelské přístupy.

### **Infrastruktura IT** zahrnuje Počítačovou síť, Technická zařízení a používané Systémy v NPÚ, případně část této infrastruktury.

### **Serverovna** je prostor, který podléhá režimu povinného zamykání a kde jsou umístěna některá Technická zařízení: zpravidla samostatná místnost nebo rack.

### **Přístupové údaje** zahrnují uživatelské jméno a heslo, pomocí kterého je možné se přihlásit s nejvyšším oprávněním pro správu části infrastruktury, tj. zpravidla s úrovní oprávnění Administrátora.

### **Uživatelské ID** je jednoznačný identifikátor (uživatelské jméno, login) přidělený Uživateli pro přihlášení do operačního systému Windows, ke sdíleným prostředkům serverů a do Systémů.

### **Správce počítačové sítě** je pověřená osoba, která zajišťuje dle touto směrnicí stanovených pravidel i jiných souvisejících předpisů funkčnost Infrastruktury IT, přidělování a správu Prostředků IT, instalaci a funkčnost software, správu Sdílených disků, správu Uživatelů a jejich přístupových údajů a další související činnosti. Správce počítačové sítě je zajišťován zaměstnancem NPÚ, příp. formou outsourcingu externí společností, která smluvně zajišťuje správu IT.

### **Externí správce počítačové sítě** je osoba pověřená smluvním partnerem pro správu Infrastruktury IT. Rozsah odpovědnosti a popis činností je definován ve smluvním vztahu mezi NPÚ a smluvním partnerem.

### **Správce uživatelské aplikace** je pověřená osoba, která zajišťuje správu konkrétní Uživatelské aplikace, přidělování přístupových práv Uživatelům do této aplikace a řešení chyb a požadavků souvisejících s touto aplikací.[[3]](#footnote-3)

### **Správce IT** je souhrnné označení pro Správce počítačové sítě a Správce uživatelské aplikace.

### **IT manažer** je osoba, která dohlíží na celkový chod a bezpečnost IT, a řídí tým Správců IT[[4]](#footnote-4).

### **Odpovědná osoba** je osoba určená za NPÚ k převzetí Přístupových údajů, odpovídá za jejich bezpečné uložení a účastní se ověřování platnosti předaných přístupových údajů. Pro následující pracoviště jsou stanoveny tyto odpovědné osoby:

### Generální ředitelství NPÚ: vedoucí odboru informatiky

### ÚPS nebo ÚOP: ředitel pracoviště.

### **Obálka** označuje obálku, ve které jsou Přístupové údaje.

### **Zálohováním** se rozumí vytvoření dočasné kopie zdrojových dat za účelem uchování pro potřeby obnovy nebo návratu k původní verzi.

### **Archivace dat** je proces, který slouží k dlouhodobému uchování dat, která již většinou nejsou aktivně využívána tak, aby byla uchována bez poškození, pro případnou obnovu.

### **Životní cyklus serveru** se rozlišuje pro každý samostatný server. Začíná záměrem pořídit server a končí jeho vyřazením. Server může mít vazbu na OS serveru.

### **Životní cyklus produktu/aplikace** se rozlišuje pro každý samostatný produkt. Ten začíná vydáním produktu v dané verzi a končí, když už produkt není podporován a je vyřazen.

### **Bezpečnost informací** – posouzení ochrany informací ze tří základních hledisek:

### Dostupnost – zda jsou informace dostupné v případě potřeby.

### Důvěrnost – zda mají k informacím přístup pouze oprávněné osoby.

### Integrita – zda nejsou informace měněny nebo mazány neautorizovaným způsobem.

### **Riziko** – potenciální možnost, že konkrétní hrozba využije zranitelnost Aktiva a způsobí tak jeho ztrátu nebo zničení.

### **Aktivum** – cokoliv, co má pro NPÚ hodnotu (servery, software, databáze, data, dokumenty).

### **Hrozba** – potenciální příčina nežádoucího incidentu, který může ohrozit Aktiva.

### **Bezpečnostní incident** – událost, která způsobuje narušení dostupnosti, důvěrnosti nebo integrity Aktiv, případně se jedná o kombinaci uvedených narušení.

### **Zranitelnost** – slabé místo Aktiva, které může být využito Hrozbou.

### **Šifrování** je proces, kterým se nezabezpečená elektronická data převádí za pomoci kryptografie na data šifrovaná. Šifrovaná data jsou čitelná pouze pro majitele dešifrovacího klíče (hesla). Šifrování dat slouží k jejich ochraně proti nežádoucímu přístupu jiné osoby a využívá se jak pro ukládání dat, tak pro jejich přenos.

Pravidla pro správu Počítačové sítě a Prostředků IT

## **Základní činnosti a povinnosti Správce IT**

### Správce IT zajišťuje všechny činnosti, které mu přísluší na základě Směrnice o užívání informačních technologií[[5]](#footnote-5), tj. zejména

#### Správu Infrastruktury IT,

#### Přidělování a správu Prostředků IT včetně veškerého příslušenství,

#### Instalaci a aktualizaci OS, SW a Uživatelských aplikací na Prostředky IT,

#### Správu Sdílených disků,

#### Správu Uživatelů a jejich přístupových údajů,

#### Správu Firemních emailů,

#### Správu Uživatelských aplikací,

#### Kontrolu dodržování předepsaných pravidel používání Počítačové sítě a Prostředků IT ze strany Uživatelů,

#### Technickou podporu Uživatelů a řešení hlášených problémů a bezpečnostních incidentů.

### Správce IT dále zajišťuje nákup a evidenci HW a SW v souladu s ostatními interními předpisy NPÚ.

### Správce IT na územním pracovišti NPÚ se řídí pokyny IT manažera GnŘ NPÚ.

## **Obecná pravidla pro zajištění bezpečnosti Infrastruktury IT**

### Správce IT nesmí vyvíjet takovou činnost, která by poškozovala Infrastrukturu IT, nebo která by ostatním uživatelům škodila nebo bránila v řádném využívání IT.

### Správce IT je povinen chránit Infrastrukturu IT před zneužitím, odcizením nebo poškozením nepovolanými osobami nebo jiným nežádoucím způsobem.

### Správce IT zavádí nezbytná bezpečnostní opatření pro zamezení poškození a proti neoprávněným zásahům do Infrastruktury IT.

### Správce IT zajišťuje pravidelnou aktualizaci a obměnu Infrastruktury IT v rámci Životního cyklu jednotlivých zařízení a aplikací s ohledem na zajištění její maximální bezpečnosti (včasnou výměnu zařízení s končící podporou ze strany výrobce, aktualizaci nebo upgrade OS a SW s končící podporou ze strany dodavatele apod.).

## **Dokumentace ICT**

### Správce IT vede v aktuální podobě dokumentaci ICT dle Přílohy č. 1 této směrnice.

## **Dokumentace informačních systémů/aplikací**

### Správce IT vede v aktuální podobě dokumentaci všech provozovaných informačních systémů/aplikací dle Přílohy č. 2 této směrnice.

## **Informovanost uživatelů o zpracování osobních údajů**

### Pokud je na daném pracovišti provozována veřejně dostupná Wi-Fi síť, zajistí Správce IT vhodným způsobem informovanost uživatelů o zpracování osobních údajů pro Wi-Fi síť, v rozsahu dle Přílohy č. 3 této směrnice. Vhodnou informovanost lze zajistit například umístěním informace společně s přístupovými údaji například u vstupu do místnosti nebo na přihlašovací obrazovce k Wi-Fi síti apod.

### Struktura informací stanovená v Příloze č. 3 je závazná. Obsah informací je nutné upravit dle skutečného stavu konkrétní Wi-Fi sítě (např. rozsah využívaných informací pro provoz Wi-Fi sítě, délka uložení/zpracování těchto informací apod.).

### V případě potřeby si vyžádá součinnost odpovědné osoby za účelem zajištění informovanosti uživatelů.

### Aktuálnost informace a její dostupnost uživatelům je kontrolována 1x ročně společně s kontrolou a aktualizací dokumentace ICT dle Přílohy č. 1 směrnice.

## **Zálohování**

### Správce IT zajišťuje zálohování dat podle pravidel a doporučení uvedených v Příloze č. 4 této směrnice.

Bezpečnostní standardy pro zabezpečení Serveroven

## **Obecné pokyny k zabezpečení Serveroven**

### Technická zařízení by měla být vždy umístěna v uzamykatelném prostoru, tj. v Serverovně nebo v racku.

### Prostor, kde jsou technická zařízení umístěna, by měl být mimo prostory s povoleným vstupem veřejnosti.

### Zabezpečení přístupu do Serverovny musí splňovat minimálně jeden (1) ze tří (3) požadavků na fyzické zabezpečení Serverovny:

#### Zabezpečení vstupních dveří zámkovou vložkou s bezpečnostní třídou 4.

##### Předané klíče, které umožňují vstup do Serverovny včetně generálního klíče, jsou evidovány písemně nebo elektronicky.

##### Klíče jsou předávány na základě předávacích protokolů.

#### Elektronické zabezpečení vstupu, které umožňuje otevřít vstupní dveře od Serverovny pomocí kódového zámku, magnetické karty nebo čipu.

##### Elektronický systém zaznamenává vstupy do Serverovny s uchováváním záznamů min. 12 měsíců.

##### Samostatná bezpečnostní zóna napojená na PZTS zajišťující zabezpečení prostor a spuštění alarmu v případě narušení bezpečnostní zóny s hlášením na velín ostrahy nebo správu objektu, PCO Policie ČR, městské policie nebo bezpečnostní agentury.

#### Kamerový systém[[6]](#footnote-6), který zaznamenává vstup do Serverovny a pohyb a práci osob v Serverovně.

##### Pokud je Serverovna vybavena konzolí pro ovládání serverů nebo jiných Technických zařízení, nesmí kamera zabírat prostor, kde jsou přes klávesnici zadávaná hesla, tak aby nebylo možné vizuálně zjistit zadávané heslo přes klávesnici.

##### Informace k nastavení kamerového systému musí být vyvěšena na vnitřní straně vstupních dveří nebo na jiném viditelném místě uvnitř Serverovny.

## **Fyzické zabezpečení přístupu do Serverovny**

### Fyzický přístup je omezován pro zajištění ochrany na úrovni objektů a v rámci objektů.

### Fyzický přístup do místností:

#### Místnost, která podléhá režimu povinného zamykání, musí být v případě, že se v ní nenacházejí žádné osoby, uzamčena.

#### Samostatně se smějí v těchto místnostech pohybovat pouze pověřené osoby, ostatní osoby se v takové místnosti mohou vyskytovat pouze v přítomnosti pověřené osoby.

### Omezení fyzického přístupu je řešeno k zamezení neoprávněnému vstupu.

#### Osoby s povoleným vstupem jsou vedeny v evidenci dostupné u Odpovědné osoby.

#### Pokud přístup vyžaduje osoba, která není uvedena na seznamu s povoleným vstupem, musí její vstup do Serverovny schválit Odpovědná osoba nebo její zástupce v době nepřítomnosti (dovolená, dlouhodobá nepřítomnost, služební cesta atp.).

#### Neoprávněný vstup do Serverovny by měl být zaznamenán jako narušení fyzické bezpečnosti:

* + kamerovým systémem,
  + elektronickou docházkou,
  + nebo pomocí PZTS.

## **Vybavení Serverovny**

### Uzamykatelný rack (povinné vybavení, jestliže místnost samotná není uzamykatelná).

### Hasicí přístroj typu CO2 by měl být umístěn max. do 5 metrů od vstupu do Serverovny.

### Serverovna by měla být vybavena monitorováním teploty a zasíláním notifikací při překročené teplotní hranici.

### Serverovna by měla mít zajištěné dostatečné větrání pro zamezení vysokých teplot.

### Serverovna by měla mít dva (2) nezávislé okruhy napájení.

### Jističe pro Serverovnu by měly být v Serverovně nebo by měly být dostatečně zabezpečeny – min. zámkem[[7]](#footnote-7).

### Nejdůležitější technická zařízení by měla být napojena na náhradní záložní zdroj.

Pravidla pro Přístupové údaje ke správě Infrastruktury IT a jejich předávání

## **Pravidla pro hesla a Přístupové údaje**

### Každý Správce IT má vytvořeno své jedinečné ID pro správu Infrastruktury IT nebo její části. Sdílené účty nejsou používány, pokud to OS nebo IS umožňuje.

### Externí správci IT se zavazují, že vytvořené heslo pro správu Infrastruktury IT nepoužijí pro jiné účely a u jiných smluvních partnerů.

### Správci IT nesmí používat stejné heslo pro registraci k soukromým nebo firemním účelům, například pro přístup k jiným službám dostupným přes internet.

### Předávání hesel a Přístupových údajů není povoleno přes žádný veřejný elektronický systém, například internet, email, mobilní aplikace, SMS, telefonní hovor.

### Správce IT nesmí komukoli sdělit své Přístupové údaje.

### Správce IT nesmí předávat žádná hesla pro správu Infrastruktury IT NPÚ při jakékoli situaci jiným zaměstnancům včetně jiných Správců IT nebo zastupujícím osobám v době dovolené.

### Správce IT nesmí mít hesla zapsána na viditelných místech.

### Správce IT musí respektovat svá přístupová práva k Infrastruktuře IT a nesmí se pokoušet o neoprávněné získání přístupových práv nebo přístupových údajů k jiným částem Infrastruktury IT, pokud k nim nemá přiděleno oprávnění.

### Správce IT je povinen dodržovat politiku tvorby bezpečných hesel a jejich periodické obnovy min. 1x za rok. V případě, kdy není možné dodržet politiku tvorby bezpečných hesel, zapíše výjimku do dokumentace ICT. Hesla musí splňovat následující pravidla:

#### délka hesla nejméně 12 znaků

#### heslo musí splňovat požadavek na komplexitu (musí obsahovat nejméně 3 z následujících 4 množin znaků):

* + velká písmena (A až Z),
  + malá písmena (a až z),
  + čísla (0 až 9),
  + ne-alfanumerické znaky (např. !, $, #, %),

#### heslo nesmí být tvořeno na základě jména a příjmení, přihlašovacího jména, e-mailu nebo obdobným jednoduše odvoditelným způsobem,

#### nesmí být použito heslo, které je obsaženo v dostupných databázích uniklých hesel[[8]](#footnote-8)

#### nelze použít minimálně 8 posledních používaných hesel, aby nebylo možné se přihlašovat pod stejným heslem několikrát po sobě. Pokud systém umožňuje takové nastavení, blokuje použití 8 posledních hesel.

## **Postup pro předávání Přístupových údajů ke správě Infrastruktury IT**

### Platné Přístupové údaje jsou předávány v tištěné podobě v zalepené Obálce.

### Přístupové údaje předává Správce IT nebo jím pověřená osoba Odpovědné osobě při osobním setkání, tj. není povoleno využívat služeb přepravních a kurýrních společností pro předání Obálky.

### Tištěné Přístupové údaje jsou vkládány:

#### do bezpečnostní obálky nebo

#### mezi další dva (2) listy A4 přehnuté do Obálky o velikosti A5; listy A4, mezi které jsou vkládány Přístupové údaje, by neměly být prázdné, ale měly by být potisknuty jiným textem, který neobsahuje Chráněné nebo Utajované informace dle klasifikace informací[[9]](#footnote-9).

### Na Obálce musí být uvedeny následující informace: jméno, příjmení a podpis předávající a přebírající osoby, datum předání.

### Odpovědná osoba je povinná uložit Obálku bezpečně tak, aby nemohlo dojít k odcizení Obálky, nejlépe do trezoru v uzamykatelné místnosti.

## **Aktualizace a změna Přístupových údajů ke správě Infrastruktury IT**

### Předání nových Přístupových údajů probíhá jedenkrát (1x) za rok.

### Před změnou Přístupových údajů je za účasti Správce IT a Odpovědné osoby otevřena původní Obálka a je ověřena funkčnost původních Přístupových údajů.

### Následně Správce IT provede změnu Přístupových údajů a připraví Obálku s novými Přístupovými údaji, které předá Odpovědné osobě NPÚ.

### Původní Obálka je za účasti Odpovědné osoby a Správce IT skartována.

### Odpovědná osoba má právo mimo plánovaný termín otevření Obálky vyzvat Správce IT k ověření správnosti zadaných Přístupových údajů a otevření Obálky za účasti Správce IT.

### V případě, kdy byla rozlepena Obálka bez přítomnosti Správce IT, je Správce IT zbaven odpovědnosti za bezpečnost dat Infrastruktury IT do doby, než na základě výzvy Odpovědné osoby provede změnu Přístupových údajů a jejich předání.

### V případě, kdy má Správce IT nebo Odpovědná osoba podezření na vyzrazení Přístupových údajů nebo dojde k odcizení Obálky, má Správce IT povinnost neprodleně Přístupové údaje změnit, informovat pověřence pro ochranu osobních údajů a manažera bezpečnosti osobních údajů (MBOU) max. do 12 hodin od zjištění incidentu a zabezpečit potencionální hrozby vhodnými bezpečnostními opatřeními, které konzultují s MBOU.

### V případě plánovaného ukončené smluvního vztahu mezi NPÚ a smluvním partnerem je externí Správce IT povinen naplánovat předání Přístupových údajů před ukončením smluvního vztahu.

Přechodná a závěrečná ustanovení

## Dokumentace dle bodu 4.3 (příloha č. 1)této směrnice bude pro GnŘ, ÚOP a centrály ÚPS zpracována v termínech uvedených v příloze č. 1 této směrnice.

## Dokumentace dle bodu 4.4 (příloha č. 2) této směrnice bude pro GnŘ, ÚOP a centrály ÚPS zpracována do 18. 3. 2021.

## Dokumentace dle bodů 4.3 a 4.4 této směrnice bude pro SPO zpracována do 18. 3. 2022.

## Aktuální verzi dokumentace dle bodů 4.3 a 4.4 této směrnice v elektronické podobě předají Správci IT ÚOP a ÚPS každoročně vždy k 28. 2. IT manažerovi GnŘ.

## Informovanost uživatelů o zpracování osobních údajů dle bodu 4.5 této směrnice bude zajištěna do 3 měsíců od data nabytí účinnosti této směrnice.

## Procesy zálohování dle bodu č. 4.6 této směrnice budou na GnŘ, ÚOP a centrálách ÚPS nastaveny do 18. 3. 2021.

## Zabezpečení Serveroven dle čl. 5 této směrnice bude na všech pracovištích NPÚ zajištěno do 18. 3. 2022.

Ing. arch Naděžda Goryczková

generální ředitelka

**Příloha č. 1 Směrnice GŘ č. XXIX/2019/NPÚ o správě informačních technologií**

**POKYNY K VEDENÍ DOKUMENTACE ICT**

## Pro každou spravovanou lokalitu vede Správce IT dokumentaci ICT v elektronické podobě, v následující doporučené struktuře. Dokumentace je primárně vedena v jednotném evidenčním IS definovaném odborem informatiky GnŘ NPÚ v rozsahu, který tento IS umožňuje, nad rámec tohoto rozsahu pak v samostatných souborech ve formátech MS Office. Přístup do tohoto IS[[10]](#footnote-10) bude zřízen Správcům IT jednotlivých pracovišť do 14 dnů od data nabytí účinnosti této směrnice, v případě změny na pozici Správce IT do 14 dnů od nahlášení této změny Odpovědnou osobou daného pracoviště NPÚ. Detailní specifikace jednotlivých zařízení lze nahradit uložením konfiguračních souborů nebo výpisů z management rozhraní či jiných nástrojů, pokud jsou z nich tyto údaje zjistitelné. Dokumentace je aktualizována min. 1x ročně, nebo vždy při pořízení nového nebo výměně daného zařízení, nebo změny v konfiguraci ovlivňující zabezpečení Počítačové sítě.

## *Části dokumentace vyznačené šedým podbarvením budou vypracovány do 18. 3. 2021. Ostatní části budou vypracovány do 18. 9. 2021.*

1. Název lokality (pracoviště NPÚ)

## Popis prostředí

### Popis IT prostředí – základních technických prostředků. Popis prostředí by měl obsahovat shrnutí základních prvků Infrastruktury IT tak, aby dal ucelený přehled o prostředí IT.

## Serverová infrastruktura

### Seznam fyzických serverů, případně fyzických hostů – s uvedením pro každý server

* Název fyzického serveru
* IP adresa
* Výrobce
* Model
* S/N; ServiceTag
* RAID (typ RAID, počet HDD)
* Hotspare
* Partition (popis, celková velikost v GB)
* CPU
* RAM
* RMM, iDrac, iLO
* Záruka
* Operační systém
* Popis využití (zpravidla role serveru a názvy informačních systémů nebo sdílených SW)
* Popis zda a jaká data jsou sdílena ze serveru
* Umístění
* Zapojení do UPS

### Seznam virtuálních serverů – s uvedením pro každý server

* Název virtuálního serveru
* IP adresa
* Datastore/RAID (typ RAID)
* Partition (popis, celková velikost v GB)
* vCPU
* RAM
* Operační systém
* Virtualizační platforma / hypervisor
* Popis využití
* Popis zda a jaká data jsou sdílena ze serveru
* Nastavení UPS ve virtualizaci

### Externí diskové pole

* Název diskového pole
* IP adresa
* Výrobce
* Model
* S/N; ServiceTag
* RAID (typ RAID, počet HDD)
* Hotspare
* Partition (popis, celková velikost v GB)
* Záruka
* Popis využití
* Popis zda a jaká data jsou sdílena ze serveru
* Umístění
* Zapojení do UPS

### Terminálový server

* Pokud je využíván terminálový server, je zpřístupněn z internetu?
* Na jakém portu je terminálový server zpřístupněn?
* Jaká technologie je použita pro terminálové připojení?
* Operační systém serveru?
* Jaký SW pro terminálové připojení je využíváno?
* Seznam uživatelů s povoleným vzdáleným přístupem?
* Jaká zabezpečení jsou aplikována?
* Blokování IP adresy po několika po sobě jsoucích neúspěšných pokusech
* Dvoufázové ověřování
* Single Sign On server

### Aktivní prvky

#### Dokumentace síťové infrastruktury

##### Evidence nastavení síťové infrastruktury je nutná nejen za účelem uchování těchto informací, ale také pro případ analýzy a řešení nastalých problémů, či kontrole bezpečnosti a topologie dané sítě.

##### Za účelem zpětného ověření přístupů a činností je doporučeno využít centrální logovací systém, a tedy i zařízení, která tato data umí předávat.

##### Schéma sítě musí vystihnout nejen to, co a kam je zapojeno, ale také jaké prostupy jsou mezi danými zařízeními / sítěmi povoleny apod. Za tímto účelem musí dokumentace obsahovat schéma fyzického zapojení (L1/L2) a schéma logického zapojení (L3). Schéma je doporučeno uchovávat v editovatelné podobě za účelem aktualizace realizovaných změn.

#### Dokumentace k aktivním prvkům

##### Všechny aktivní prvky musí být evidovány v dokumentaci, pro případ nahrazení zařízení je nutné provádět zálohy konfigurací.

##### Vzor pro zpracování dokumentace aktivních prvků je uveden v Příloze č. 5[[11]](#footnote-11) této směrnice.

#### Všeobecná evidence u všech zařízení

* název (dle interního značení)
* umístění (kde je zařízení fyzicky umístěno)
* typ zařízení, PN a SN (co je to za zařízení, výrobce, modelové označení, sériové číslo)
* stručný popis (poznámka o tom k čemu je zařízení využito)
* verze FW, příp. OS (verze firmware zařízení vč. verze operačního systému, pokud je systém odlišný)
* evidence přístupových údajů (samotné přístupy pro administraci uchovány zabezpečeně)
* odkud je administrace zpřístupněna (odkud je možné se do zařízení připojit a odkud nikoli)
* jak je administrace zabezpečena (informace o tom, že je nutné autorizovat uživatele jménem a heslem, 2FA apod., pokud má zařízení povoleno více metod přístupu ke konfiguraci, je nutné evidovat pro každou zvlášť, jako je např. SSH a serial)
* kdo zodpovídá za dané zařízení (kdo ho má pod správou)
* zálohování (kdy / jak často a kam jsou ukládány zálohy konfigurace daného zařízení)
* kam zařízení reportuje chyby
* dohled (jakým systémem je zařízení dohledováno)
* připojení napájení (je zařízení připojeno do UPS, redundantní napájení)
* redundance (je zařízení v HA, příp. je k dispozici náhradní kus)
* záruka (je zařízení pod platnou zárukou, do kdy)
* evidence základní konfigurace typické pro dané zařízení

#### Dokumentace nastavení jednotlivých prvků

##### Každé zařízení má několik hlavních parametrů, které je nutné zaevidovat, příklad je uveden na těch nejčastěji použitých níže.

##### Router

* adresace
  + IP adresy WANů vč. informací pro nastavení rout
  + IP adresy LANů vč. informací pro natavení lokálních síti, tj. konfigurace DHCP, DNS apod.
* VPN Tunely
  + Typ tunelu (Site-to-Site nebo Remote Access)
  + Metody zabezpečení (spojení, přenosu apod.)
  + Pro koho je tunel určen
  + Co a jak je v tunelu povoleno (odkud, kdy, kdo a kam)
* Definice povolených komunikací
  + odkud
  + kdy
  + kdo
  + kam na routeru
  + kam finálně
  + pokud je, tak také za jakou adresu je zdrojová komunikace maskovaná
* Omezování šířky pásma
* Zabezpečení zařízení proti útokům
  + Prvky a kroky podniknuté pro eliminaci útoků (DDoS, SYN Flood, Brute Force, aj.)
  + Stáří nasazeného systému

##### Switch

* Adresace
  + VLAN interface vč. informací pro nastavení komunikace
* Zapojení portů
  + informace o tom, kam jsou dané porty switche fyzicky propojeny
* VLANy
  + informace o tom, jaké VLANy jsou na jakých portech aplikovány a jak

##### Wi-Fi

* Adresace a sítě
  + Vysílané sítě/VLANy a jejich SSID
  + IP adresy, pokud jsou v daných VLAN
  + Prostupy daných VLAN (detailní evidence, pokud nejsou v routeru)
* SSID
  + Evidence, na jakých AP jsou vysílány, jaké Wi-Fi sítě/VLANy
* Zabezpečení
  + Zabezpečení jednotlivých vysílaných sítí
* Fyzické zabezpečení
  + Fyzické umístění HW
  + Evidence, zda je Wi-Fi síť dostupná mimo cílené prostory

#### Prostupy do sítě

##### Za účelem zajištění bezpečnosti sítě je třeba evidovat prostupy z internetu. Ty mohou být řešeny nejčastěji např. pomocí VPN serverů, aplikacemi jako je VNC, LogMeIn, TeamViewer apod. Správce by měl všechna tato využívaná řešení evidovat a zajistit blokaci, či eliminaci jejich zneužití. Nasazení těchto řešení formou klientských aplikací by mělo být řešeno již v rámci politik na serverech a stanicích, jejich samotný provoz pak může být v některých případech blokován / monitorován na routeru.

## Docházkový elektronický systém

* Název SW docházkového elektronického systému
* Napojení na PZTS
* Umístění, kde jsou uložená data
* Servisní organizaci uveďte do kapitoly 1.14 Kontaktní osoby
* Vzdálený přístup pro správu: ano/ne
* Jak je vzdálený přístup zabezpečen
* Popis komunikace mezi čtečkou a serverem
* Popis dalšího nastavení

## Kamerové systémy[[12]](#footnote-12)

### Počet kamer

* Výrobce
* Délka uchovávání záznamů
* Umístění záznamového zařízení
* Fyzické zabezpečení záznamového zařízení

## Záložní zdroje UPS

* Název
* IP
* Datum poslední výměny baterií
* Záruka
* Seznam zařízení napojených na záložní zdroj

## Zálohování

### Zálohování dat ze serverů

* Popis, jakým SW jsou data zálohována, uveďte všechny metody zálohování (Cobian Backup, Volume Shadow Copy, Veeam, Acronis atp.)
* Uveďte, jaká data jsou zálohovaná (typicky celý operační systém; partition - uveďte jaké, vybraná data - uveďte jaké)
* Kam jsou zálohy uloženy (primární případně sekundární úložiště)
* Metodika zálohování (plná záloha, přírůstková, rozdílová, jiná popište jaká)
* Interval zálohování (denní, týdenní, jiný uveďte jaký)
* Dochází k automatickému promazávání starších záloh?
* Jak dlouho jsou zálohy uchovávány?
* V jakém intervalu jsou zálohy kontrolovány?
* Jsou zasílány notifikace emailem o provedení úspěšného/neúspěšného zálohování?
* Je prováděno testování obnovy dat ze zálohy?
* Jsou zálohy archivovány?
* Kde jsou archivy uloženy?
* Uveďte, jak se liší zabezpečení archivů od zabezpečení záloh?
* V jakém intervalu je prováděno testování obnovy dat ze zálohy?
* Jsou zálohy zabezpečeny šifrováním nebo je šifrované diskové úložiště?
* Osoby oprávněné přistupovat k zálohám uveďte do kapitoly 1.14 Kontaktní osoby
* Osoby oprávněné obnovovat data ze záloh uveďte do kapitoly 1.14 Kontaktní osoby
* Co bývá nejčastější příčinou neprovedení zálohy?

### Zálohy mobilních telefonů

* Popište, jak je řešeno zálohování mobilních telefonů, pokud není řešeno individuálně uživateli, kteří byli proškoleni dle směrnice pro uživatele IT[[13]](#footnote-13).

### Zálohování koncových klientů

#### Pokud jsou zálohována data z koncových zařízení, uveďte obdobně jako v kapitole 1.6.1, jak je zálohování řešeno.

### Geografické zálohování

##### Pokud je využíváno geografické zálohování, popište:

* Kam jsou data přenášena
* Jak je zabezpečen přenos dat
* Seznam poskytovatelů služby uveďte do kapitoly 1.14 Kontaktní osoby

## Lokálně používané aplikace a informační systémy

### Seznam aplikací určených pro sdílenou práci uživatelů nebo pro účely evidence, instalovaných a provozovaných pouze lokálně na daném pracovišti. V seznamu není nutné uvádět centrální systémy jako je například Colosseum, VEMA, intranet atp.

## Domény

### Seznam aktivně využívaných interních i veřejných domén, včetně uvedení účelu, pro který jsou využívány (kromě domén webových prezentací a centrálních IS evidovaných na Intranetu NPÚ v aplikaci „Weby NPÚ, sociální sítě“ <https://intranet.npu.cz/sprava-webovych-domen>)

## Internet

### Poskytovatel Internetu (ISP)

#### Kontakt na podporu uveďte do kapitoly 1.14 Kontaktní osoby

### Primární linka:

* kapacita linky: X Mbps / X Mbps
* technologie: optika / mikrovlnné připojení / VDSL / ADSL / jiné (uveďte jaké)
* agregace
* počet vnějších IP adres
* vnější IP adresy:
* monitoring výpadku od ISP:
* jiný monitoring výpadku:
* smluvní úvazek: délka, datum do kdy je úvazek sjednán

### Záložní linka:

* kapacita linky: X Mbps / X Mbps
* technologie: optika / mikrovlnné připojení / VDSL / ADSL / jiné (uveďte jaké)
* agregace
* počet vnějších IP adres
* vnější IP adresy:
* monitoring výpadku od ISP:
* jiný monitoring výpadku:
* smluvní úvazek: délka, datum do kdy je úvazek sjednán

## Telefonní ústředna

* Telefonní ústředna: analogová/digitální
* Výrobce:
* Model:
* GSM karty/moduly:
* Servisní organizaci uveďte do kapitoly 1.14 Kontaktní osoby
* Vzdálený přístup pro správy: ano/ne
* Jak je vzdálený přístup zabezpečen:
* Nahrávání hovorů/záznamník: ano/ne
* Popis nastavení (přepady, aj.):

### 

## Síťové a multifunkční tiskárny

* Název (výrobce, model)
* S/N
* Typ připojení (LAN, USB, Wi-Fi)
* Umístění
* Multifunkční tiskárna: ano/ne
* Podpora funkce odloženého tisku: ano/ne
* Nastavená funkce odloženého tisku: ano/ne
* Podpora a nastavení skenování do složky: ano/ne
* Nastavená funkce skenování do složky: ano/ne
* Podpora funkce zasílání skenů emailem: ano/ne
* Nastavená funkce zasílání skenů emailem: ano/ne
* Podporuje tiskárna vytvoření adresáře osob: ano/ne

### Seznam osob oprávněných provádět správu tiskáren uveďte do kapitoly 1.14 Kontaktní osoby

## Licence

### Licencovaný SW

#### Seznam licencovaného SW v rámci pracoviště

* Název SW
* Počet zakoupených licencí
* Počet využívaných licencí
* Seznam PC/uživatelů, ke kterým je licence přiřazena

## Bezpečnost

### Tento bod popisuje oblasti bezpečnosti, které nejsou zmíněny v rámci ostatních oblastí

#### Zabezpečovací ústředna/y (PZTS), které nesouvisí s ochranou památek, typicky na pracovišti ÚPS, ÚOP (tj. nepodléhá Utajovaným informacím):

* Výrobce:
* Model:
* Počet bezpečnostních zón:
* Nákres bezpečnostních zón:
* Informace k nastavení automatického zakódování/odkódování:
* Další konfigurace:
* Seznam osob oprávněných odkódovat objekt:
* Uveďte, zda každý oprávněný uživatel má přidělen vlastní kód nebo je využíván jeden kód sdílený více uživateli:
* Uveďte datum poslední změny kódů k PZTS:
* Napojení na PCO:
* Název bezpečnostní agentury:
* Seznam osob, které jsou oprávněny kontaktovat PCO:
* Je PZTS napojena na elektronický docházkový systém:
* Je povolena vzdálená správa PZTS:
* Jak je zabezpečeno/omezeno vzdálené připojení pro správu PZTS:

##### Seznam správců PZTS uveďte do kapitoly 1.14 Kontaktní osoby

### Zabezpečení Serverovny – Kamery

* Pro monitoring pohybu osob v prostorech Serverovny je/není využíván kamerový systém.
* Záznamy z kamerového systému jsou ukládány (uveďte kam):
* Délka uchovávání záznamů
* Úložiště pro uchovávání záznamů je/není šifrované
* Odesílají se fotografie pohybujících se osob emailem
* Je možný přístup ke kamerovému systému přes mobilní aplikaci nebo Internet?
* Je povolen přístup ke kamerovému systému přes mobilní aplikaci nebo Internet?

#### Seznam správců kamerového systému uveďte do kapitoly 1.14 Kontaktní osoby

### Zabezpečení Serverovny – PZTS

* Má Serverovna vlastní zónu PZTS: ano/ne
* Napojení PZTS Serverovny je na stejnou zabezpečovací ústřednu uvedenou v 1.13.1.1: ano/ne
* Pokud je PZTS Serverovny napojenou na jinou zabezpečovací ústřednu, uveďte informace dle kapitoly 1.13.1.1

### Zabezpečení aktivních prvků

#### Popište umístění nebo přiložte nákres rozmístění aktivních prvků a uveďte, jak je omezen fyzický přístup k aktivním prvkům.

### Vzdálené přístupy pro správu

#### Popište použité procesy a technologie pro vzdálené připojení.

### Bezpečnostní rizika a návrhy na jejich snížení

#### Uveďte oblasti, jaké považujete za rizikové z hlediska bezpečnosti IT (fyzického přístupu i elektronického přístupu) a jaké opatření navrhujete pro snížení uvedených rizik.

## Kontaktní osoby

### Seznam osob oprávněných provádět správu. U každé osoby uveďte oblasti, které je oprávněna spravovat. Pro každou z níže definovaných oblastí musí být určen správce.

* Interní zaměstnanec / Název externí společnosti
* Jméno, Příjmení
* Telefonický kontakt
* Email
* Webové stránky
* Systém pro zadávání požadavků: uveďte jaký systém/proces je využíván pro zadávání požadavků na odstranění zjištěných neshod nebo jiných požadavků
* Oblasti s povolenou správou

#### Seznam oblastí:

* Celková správa ICT
* Serverová infrastruktura
* Konkrétní servery
* Externí diskové pole
* Firewall/Router
* Aktivní prvky
* Wi-Fi
* Záložní zdroj UPS
* Telefonní ústředna
* Zabezpečovací ústředna (PZTS)
* Docházkový elektronický systém
* Kamerové systémy
* Klientské zařízení
* Internet
* Základní uživatelský SW (OS, Office, Zoner, antivir apod.)
* IS (jednotlivé odborné a specializované aplikace)

**Příloha č. 2 Směrnice GŘ č. XXIX/2019/NPÚ o správě informačních technologií**

**BEZPEČNOSTNÍ STANDARDY PRO INFORMAČNÍ SYSTÉMY**

## Pro každý provozovaný informační systém/aplikaci vede Správce IT dokumentaci v následující doporučené struktuře:

1. Název informačního systému/aplikace

## Umožňuje informační systém/aplikace napojení na Active Directory/LDAP Objednatele?

### Ano / pokračujte na otázku č.2

### Ne

#### Umožňuje informační systém/aplikace nastavit automatickou změnu hesla v definovaném intervalu?

#### Umožňuje informační systém/aplikace vyžadovat požadavky na složitost hesla?

#### Umožňuje informační systém/aplikace zadat požadavek na změnu hesla, např. při zakládání účtu?

#### Umožňuje systém zadat uživatelovi prázdné heslo, tj. nezadat žádné heslo?

#### Dojde k blokování uživatelského účtu, po několika po sobě jdoucích neúspěšných pokusech o přihlášení?

## Umožňuje informační systém/aplikace automatické odhlášení uživatele při nečinnosti?

## Kde jsou uložena data

### na zařízení Objednatele

### na zařízení Dodavatele

### v hostingu v rámci cloudové služby, na HW cloudového poskytovatele (subdodavatel Objednatele)

### v hostingu v rámci cloudové služby, na HW cloudového poskytovatele (subdodavatel Dodavatele)

#### uveďte název cloudového poskytovatele/datacentra: …………………………………………………….

### v hostingu v rámci cloudové služby, na HW Objednatele

### v hostingu v rámci cloudové služby, na HW Objednatele Dodavatele

#### uveďte název cloudového poskytovatele/datacentra: …………………………………………………….

## Servery, na kterých je informační systém provozován, jsou:

### Dedikovány pouze pro Objednatele

#### Ano

#### Ne

### Jsou využívány Dodavatelem i pro jiné klienty

#### Ano

#### Ne

## Je úložiště dat/databáze zabezpečeno šifrováním?

### Ano

#### Šifrování je nasazeno v rámci diskového pole (hardwarové šifrování)

#### Šifrování je nasazeno v rámci hypervisoru na diskovém poli

#### Šifrování je nasazeno v rámci celého operačního systému (např. BitLocker)

#### Šifrování je nasazeno v rámci vybraných dat/databáze

#### Ani jedna z uvedených možností, popište Vaše jiné řešení ………………………………………….

### Ne

## Jaký typ RAID je na diskovém poli nasazen: ……………………………………………………………….

### Má Raidové pole vyhrazený hotspare?

#### Ano

#### Ne

### Napište kolik disků z Raidového pole může vykázat chybu, aniž by došlo k poškození dat: ……...

### Je diskové pole zapojeno v HA?

#### Ano

#### Ne

## Informační systém je provozován v rámci:

### Windows aplikace

#### Ano

#### Ne

### Webového serveru

#### Ano

#### Ne

### Linux serveru

#### Ano

#### Ne

## Jsou servery zapojeny v HA?

### Ano

### Ne

## Informační systém má uložena data v rámci Databázového serveru

### Ano

#### Napište název databázového serveru a jeho verzi (včetně případných aktualizací a servis packů): ……………………………………………………………………………

#### Je databázový server na jiném serveru, než je aplikační nebo webový server?

##### Ano

###### Dodejte schéma propojení jednotlivých serverů

##### Ne

### Ne

## Jaké operační systémy podporuje informační systém

### Linux

### MacOS

### Windows

## Jak je řešeno napojení klientů na informační systém

### Windows klient (aplikace)

#### Ano

#### Ne

### Webové rozhraní

#### Ano

#### Ne

### Mobilní aplikace

#### Ano

##### Je komunikace mezi klientem a serverem zabezpečena šifrováním?

###### Ano

###### Ne

##### Jaká oprávnění vyžaduje povolit mobilní aplikace povinně? …………….......................... ………………………….......................................................................................................

##### Jaká oprávnění vyžaduje povolit mobilní aplikace nepovinně? ……………...................... …………………………......................................................................................................

##### Jaké operační systémy mobilní aplikace podporuje?

###### Android

###### iOS

###### Windows Mobile

#### Ne

## Jak je řešeno zálohování informačního systému

### Jsou zálohovány celé servery včetně konfiguraci, instalací a dat?

#### Ano

#### Ne

### Jsou zálohovány data/databáze?

#### Ano

#### Ne

### Jaký je interval vytváření záloh?

#### Hodinový

##### Zapište interval počtu hodin

#### Denní

##### Ano

##### Ne

#### Týdenní

##### Ano

##### Ne

#### Měsíční

##### Ano

##### Ne

#### Roční

##### Ano

##### Ne

#### Jiný, zapište jaký: …………………………………………………….

### Jsou zálohy šifrovány

#### Ano

#### Ne

### Jak dlouho jsou uchovávány logy o provedených zálohách a obnovách serverů/dat/databází, napište garantovaný interval: ………………………………………………………

### Dochází k testování integrity vytvořených záloh?

#### Ano

##### V jakém intervalu jsou prováděny obnovy záloh

###### Měsíční

Ano

Ne

###### Kvartální

Ano

Ne

###### Roční

Ano

Ne

###### Jiné, uveďte interval: ………………………………………………………

#### Ne

### Uveďte seznam osob, které mají oprávnění pro vytváření záloh: …………………………………..

### Uveďte seznam osob, které mají oprávnění provádět obnovu: ……………………………………..

## Je prováděna archivace dat?

### Ano

#### V jakém intervalu? ……………………………………………………………………………………...

### Ne

## Umožňuje aplikace definovat uživatelské role (soubor uživatelských oprávnění, který se přiděluje jednotlivým uživatelům)?

### Ano

### Ne

## Uveďte kolik osob má přístup s oprávněním administrátora k datům na úrovni operačního systému/databázového serveru: ……………………………………………………………………………

## Uveďte kolik osob má přístup s oprávněním administrátora k datům na úrovni souborového systému/ systému/databáze informačního systému: ………………………………………………………………

## Má Dodavatel povoleno nebo zakázáno využívat služeb Subdodavatelů pro správu/opravu informačního systému?

### Ano

### Ne

## Je povoleno vzdálené připojení pro správu informačního systému?

### Ano

### Ne

## Je připojení klientů/uživatelů šifrováno

### Ano

### Ne

## Je vzdálené připojení zabezpečeno šifrováním

### Ano

#### Uveďte jakým……………………………………………………………………………………………….

### Ne

## Je vzdálené připojení zabezpečeno dvoufázovým ověřováním

### Ano

### Ne

## Je připojení zabezpečeno pomocí Single Sign On serveru?

### Ano

### Ne

## Je vzdálené připojení pro administraci informačního systému omezeno z definovaných statických IP adres?

### Ano

### Ne

## Používá každý správce Dodavatele vlastní účet pro správu informačního systému/aplikace?

### Ano

### Ne

## V rámci zaznamenávání změn v informačním systému, včetně konkrétního času dané činnosti a uživatele, který akci provádí, jsou evidované:

### Vytvoření nové položky?

#### Ano

#### Ne

### Změna již vytvoření položky/hodnoty (editace)?

#### Ano

#### Ne

### Zaznamenání původní hodnoty před provedenou změnou?

#### Ano

#### Ne

### Vymazání záznamu/položky/hodnoty?

#### Ano

#### Ne

### Zobrazení/náhled/otevření záznamu?

#### Ano

#### Ne

## Logování

### Logy jsou uchovávány:

#### Na stejném serveru jako aplikace

##### Ano

##### Ne

###### Název a popis úložiště: ………………………………………………………………………………………………

### Jaká je garantovaná délka uchovávání logů? ………………………………………………………………

### Je úložiště logů zabezpečeno šifrováním?

#### Ano

#### Ne

## Jsou požadavky na opravu/úpravu informačního systému/aplikace evidovány písemně?

### Ano

#### Přes Helpdesk/ServiceDesk/Ticketovací systém

##### Ano

##### Ne

#### Emailem

##### Ano

##### Ne

### Ne

## Jsou požadavky na opravu/úpravu informačního systému/aplikace evidovány pomocí nahrávaných telefonických hovorů?

### Ano

### Ne

## Pokud je informační systém dostupný přes webové rozhraní:

### Je přístup zabezpečen SSL certifikátem (přes https)?

#### Ano

##### Uveďte úroveň šifrování (SSL 2.0, SSL 3.0, TLS 1.1, TLS 1.2, jiná, uveďte jaká): …………………………………………………………….

#### Ne

## Dochází k opakovaným bezpečnostním testům databázového/webového serveru informačního systému?

### Ano

#### Uveďte interval prováděných testů: ………………………………………………………………….

### Ne

## Dochází k opakovaným bezpečnostním testům zdrojových kódů informačního systému?

### Ano

#### Uveďte interval prováděných testů: ………………………………………………………………….

### Ne

## Je informační systém/aplikace dostupný z internetu?

### Ano

### Ne

## Je dostupná dokumentace se sepsanými požadavky na zajištění dostupnosti systému?

### Ano

### Ne

## Jsou vyhotoveny DRP (Disaster Recovery Plans) pro výpadky informačního systému?

### Ano

### Ne

## Je rozdělení odpovědnosti v rámci správy informačního systému popsáno ve smlouvě nebo jiném dokumentu?

### Ano

### Ne

## Jsou v informačním systému ukládány citlivé osobní údaje (údaje zvláštní kategorie podle definice v GDPR)?

### Ano

### Ne

## Jsou v informačním systému evidovány osobní údaje, které vyžadují souhlas Subjektu údajů (fyzické osoby)?

### Ano

#### Umožňuje informační systém evidenci souhlasů Subjektů údajů

##### Ano

##### Ne

#### Umožňuje informační systém evidenci odvolání souhlasů Subjektů údajů

##### Ano

##### Ne

#### Umožňuje informační systém nastavení Omezení zpracování?

##### Ano

##### Ne

#### Umožňuje informační systém nastavení skartace osobních údajů

##### Ano

###### Umožňuje informační systém definovat pravidla pro nastavení skartace včetně definování lhůty pro jejich vymazání?

Ano

Ne

##### Ne

### Ne

## Umožňuje informační systém exportování osobních údajů Subjektu údajů (konkrétní fyzické osoby) ve strukturovaném formátu?

### Ano

#### Uveďte podporované formáty: …………………………………………………………………………….

### Ne

## Umožňuje informační systém výpis osobních údajů Subjektu údajů (jaké osobní údaje v informační systému jsou o Subjektu údajů uchovávány, např. jméno, příjmení)

### Ano

### Ne

## Umožňuje informační systém zasílání emailů?

### Ano

### Ne

## Umožňuje informační systém zasílání newsletterů?

### Ano

### Ne

## Uveďte počet uživatelů, kteří mají přístup do informačního systému: ………………………………….

## Uveďte přibližný počet Subjektu údajů, kteří jsou zpracovávány v informačním systému: …….

**Příloha č. 3 Směrnice GŘ č. XXIX/2019/NPÚ o správě informačních technologií**

**INFORMACE O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PRO WI-FI SÍŤ**

Pokud je na daném pracovišti provozována veřejně dostupná Wi-Fi síť, zajistí Správce IT vhodným způsobem informovanost uživatelů o zpracování osobních údajů pro Wi-Fi síť, v tomto rozsahu:

**I. Správce osobních údajů / Správce Wi-Fi** **sítě**

Národní památkový ústav, státní příspěvková organizace, se sídlem Valdštejnské nám. 162/3, PSČ 118 01 Praha 1 – Malá Strana, IČ: 75032333.

**II. Účely a právní důvod zpracování osobních údajů**

Osobní údaje zpracováváme v rámci oprávněného zájmu za účelem provozování a monitoringu Wi-Fi sítě určené pro návštěvníky.

**III. Kategorie osobních údajů**

Osobní údaje zpracováváme v rozsahu: přidělená IP adresa, MAC adresa zařízení, log provozních údajů datové komunikace, datum a čas připojení na Wi-Fi síť, datum a čas odpojení z Wi-Fi sítě, log navštívených IP adres, log navštívených URL adres.

**IV. Příjemci osobních údajů**

Osobní údaje získané v rámci připojení na Wi-Fi síť nejsou dále předávány, pokud si je nevyžádá Policie ČR případně dalším orgánům činných v trestním řízení.

**V. Doba uložení osobních údajů**

Doba zpracování: 3 měsíce.  
Doplňkové informace lze zjistit u Správce Wi-Fi sítě.

**VI. Práva subjektů údajů a povinnosti správce**

1. **Právo na přístup ke svým osobním údajům.** Máte právo získat následující informace:

* účely zpracování,
* kategorie dotčených osobních údajů,
* příjemci nebo kategorie příjemců, kterým osobní údaje byly nebo budou zpřístupněny,
* plánovaná doba, po kterou budou osobní údaje uloženy,
* veškeré dostupné informace o zdroji osobních údajů, pokud nejsou získány od subjektu údajů,

1. **Právo na opravu**. Oznámíte-li nám, že požadujete opravu svých osobních údajů, máme povinnost se vaší žádostí zabývat.

1. **Právo na výmaz** představuje jinými slovy naši povinnost zlikvidovat vaše osobní údaje, pokud je splněna alespoň jedna podmínka:

* osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány,
* vznesete námitku proti zpracování a neexistují žádné převažující oprávněné důvody pro zpracování,
* osobní údaje byly zpracovány protiprávně,
* osobní údaje musí být vymazány ke splnění právní povinnosti,
* uplynula lhůta zpracování osobních údajů.

Právo na výmaz není absolutní právo, které by vám dávalo možnost žádat kdykoli a za jakékoli situace o vymazání osobních údajů. Nelze např. v rámci tohoto práva žádat likvidaci všech osobních údajů, jelikož se na nás vztahují povinnosti o dalším uchování některých osobních údajů.

1. **Právo na omezení zpracování osobních údajů,** pokud:

* popíráte přesnost osobních údajů, a to na dobu potřebnou k tomu, abychom mohli přesnost osobních údajů ověřit,
* zpracování je protiprávní a vy odmítáte výmaz osobních údajů a žádáte místo toho o omezení jejich použití,
* vaše osobní údaje již nepotřebujeme pro účely zpracování, ale vy je požaduje pro určení, výkon nebo obhajobu právních nároků,

1. **Právo vznést námitku** proti zpracování osobních údajů.
2. **Právo podat stížnost u dozorového úřadu**,pokud se domníváte, že zpracováním vašich osobních údajů je porušeno GDPR.

K uplatnění práv v oblasti osobních údajů se na nás můžete obracet prostřednictvím e-mailové adresy [poverenec@npu.cz](mailto:poverenec@npu.cz).

**Příloha č. 4 Směrnice GŘ č. XXIX/2019/NPÚ o správě informačních technologií**

**Pravidla a doporučení pro zálohování**

Plánování a implementace procesu zálohování dat na jednotlivých pracovištích NPÚ probíhá v následujících krocích:

1. Definování seznamu zálohovaných dat

## Konfigurace aktivních prvků

### Managovatelné switche

### Routery

### Firewally

## Konfigurace serverů

### Local Security Policy

### Konfigurace IIS

### Konfigurace DHCP

### Používané skripty

## Sdílená významná data ze serverů nebo zařízení NAS

## Data z počítačů

## Certifikáty

1. Rozdělení zálohovaných dat podle kategorií

## Kritická data

### data nezbytná k zajištění základního fungování NPÚ, plnění zákonných povinností apod. Jejich nedostupnost by způsobila zásadní potíže v činnosti jednotlivých pracovišť, data nejsou jiným způsobem nebo jen velmi obtížně nahraditelná

### v zásadě se jedná o data uchovávaná v centrálních IS NPÚ (WAM S/3, VEMA, ESS, Památkový katalog a další), jejichž zálohování zajišťuje GnŘ

## Významná data

### data důležitá k zajištění běžných činností a služeb NPÚ, převážně trvalé nebo dlouhodobé hodnoty, např. výsledky odborné nebo vědeckovýzkumné činnosti NPÚ, výstupy digitalizace apod.

## Ostatní data

### data pracovní, podkladová, převážně krátkodobého charakteru, jejichž případná ztráta nevede k finančním nebo provozním ztrátám, dají se vytvořit znovu nebo nahradit jinými.

1. Stanovení velikosti zálohovaných dat
2. Stanovení zálohovacího SW a metodiky
3. Doporučení k zálohování podle kategorií zálohovaných dat

## Kritická data

### Ukládání záloh do dvou geograficky oddělených lokalit

## Významná data

### Redundantní ukládání dat (RAID)

### Pravidelně kontrolovat integritu dat

### Uložiště záloh není umístěno na stejném fyzickém úložišti jako jsou zálohovaná data

## Ostatní data

### Pravidelně kontrolovat integritu dat

### Uložiště záloh není umístěno na stejném disku jako jsou zálohovaná data

1. Stanovení cílového bodu obnovy – maximální časové okno ztráty dat – stanovení intervalu vytváření záloh

## Kritická data a databáze důležitých IS – minimálně 1x denně, příp. i vícekrát za den, interval je stanoven podle konkrétního IS

## Významná data – minimálně 1x týdně

## Ostatní data – alespoň 1x měsíčně (výběr těchto dat určených k zálohování)

1. Stanovení času obnovy – stanovení požadovaného času pro obnovu

## Obnova je závislá na důležitosti dat, IS a zvolené zálohovací metodě.

1. Stanovení požadavků na velikost úložiště

## Doporučený prostor pro ukládání záloh je závislý na požadavku pro uchovávání záloh - min. 3x velikost zálohovaných dat

1. Stanovení doby uchovávání záloh – stanovení intervalu, jak dlouho mají být zálohy dostupné

## Stanovení doby je závislé na důležitosti dat, IS a zvolené zálohovací metodě – doporučené typické nastavení

### Kritická data a databáze důležitých IS - denní přírůstkové zálohy 7 dní; 4x týdenní zálohy; 6x měsíční zálohy

### Významná data - 4x týdenní přírůstkové zálohy; 6x měsíční zálohy

### Ostatní data – 4x týdenní přírůstkové zálohy; 3x měsíční zálohy

1. Stanovení požadavků na dostupnosti systémů – stanovení maximální délky výpadku služby – délku jednorázového výpadku a délku celkového ročního výpadku pro každou službu/IS

## Výpadky by měly zohledňovat uzavřené SLA, respektive uzavřené SLA by měly zohledňovat požadavky NPÚ

## Kategorizace délky jednorázového výpadku služby:

|  |  |
| --- | --- |
| Kritický | Do 4 hodin |
| Důležitý | Do 24 hodin (1 den) |
| Běžný | Do 72 hodin (3 dny) |
| Zanedbatelný | Do 168 hodin (7 dní) |

## Kategorizace délky ročního výpadku služby:

|  |  |
| --- | --- |
| Kritický | Do 2 dnů |
| Důležitý | Do 7 dnů |
| Běžný | Do 14 dnů |
| Zanedbatelný | Do 30 dnů |

1. Zabezpečení záloh nebo úložiště

## Omezení přístupu pro oprávněné osoby

## Omezení přístupu z povolených IP adres / VLAN

## Zabezpečení dat nebo úložiště šifrováním

## Fyzické zabezpečení zařízení

1. Konfigurace uchovávání logů o provedených zálohách a obnově dat

## Definování délky uchovávání dat

1. Stanovení oprávnění pro provádění záloh a obnovy dat
2. Nastavení monitorování průběhu a výsledku zálohování a zasílání alertů
3. Stanovení obsahu a intervalu provádění kontrol

## 1x měsíčně při nastavení zasílání upozornění o neprovedené záloze

## Při zaslání upozornění o neprovedené záloze

## 1x týdně bez nastavení monitorování provedených záloh

## Kontroly zahrnují

### Kontrolu integrity zálohovaných dat

### Kontrolu hardware a diskového úložiště

### Test obnovy vybraných dat ze zálohy

1. Stanovení seznamu elektronických dat k archivaci

## Stanovení obsahu archivovaných dat

## Stanovení archivační doby

## Stanovení intervalu pro ověření konzistence archivovaných dat.

**Příloha č. 5 Směrnice GŘ č. XXIX/2019/NPÚ o správě informačních technologií**

**VZOR DOKUMENTACE K AKTIVNÍM PRVKŮM**

1. Příklad dokumentace k aktivním prvkům

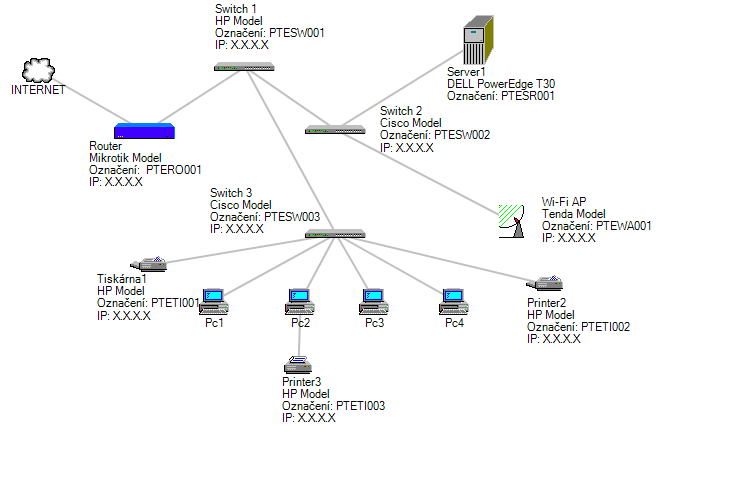
## Seznam aktivních prvků

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Typ zařízení** | **Označení zařízení** | **Název zařízení (Výrobce Model)** | **IP adresa** | **Umístění** | **Připojená zařízení** | **Popis** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Typ zařízení** | **Označení zařízení** | **Správce zařízení** | **Administrace** | **Zabezpečení administrace** | **Odpovědná osoba** | **Zálohování** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Typ zařízení** | **Označení zařízení** | **Notifikace** | **Monitoring** | **Napojení na záložní zdroj** | **Záruka** | **Logy** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## Schéma sítě



## Router / Firewall

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Označení zařízení** | **Název zařízení (Výrobce Model)** | **Veřejná IP (WAN)** | **DNS** | **Access list** | **Adresa sítě (LAN)** | **Maska** | **DHCP / Rozsah** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

### VPN Tunely

|  |  |  |  |
| --- | --- | --- | --- |
| **Typ tunelu** | **Metody zabezpečení** | **Pro koho je tunel určen** | **Povolená komunikační pravidla** |
|  |  |  |  |
|  |  |  |  |

### Definice Security Zone

### Pokud jsou využívané VLANy, uveďte, jaké Security Zone jsou využívané.

|  |  |  |  |
| --- | --- | --- | --- |
| **NÁZEV ZONY** | **VLAN** | **SUBNET** | **INTERFACE** |
|  |  |  |  |
|  |  |  |  |

### Definice povolených komunikací

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **FROM** | **TO** | **NÁZEV POLICY** | **SOURCE ADDRESS** | **DESTINATION ADDRESS** | **APPLICATION** | **ACTION** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### Uveďte, zda je používané omezování šířky pásma a pokud je využívané, jaké je jeho nastavení.

### Bezpečnostní funkce proti kybernetickým útokům

### Uveďte bezpečnostní opatření proti eliminaci útoků na routeru/firewallu (DDoS, SYN Flood, Brute Force, aj.)

### Uveďte stáří nasazeného systému

## Switche

### Pro managovatelné switche uveďte, jaké porty jsou zařazeny, do jakých VLAN.

### Pro jednotlivé porty uveďte, jaké konkrétní zařízení je, v jakém portu zapojeno.

## Wi-Fi

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Označení** | **Zařízení** | **Umístění** | **Frekvence** | **SSID** | **Zabezpečení** | **Adresa sítě** | **Maska** | **Veřejná**  **(ano/ne)** |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Označení** | **Zařízení** | **Rozsah** | **VLAN** | **Poznámka** |
|  |  |  |  |  |
|  |  |  |  |  |

### Pro Wi-Fi sítě zpřístupněné veřejnosti uveďte způsob informování uživatelů o zprac. os. údajů dle bodu 4.5 této směrnice (vývěska, logovací stránka apod.).

## Prostupy do sítě

### Uveďte, jaké další prostupy do vnitřní sítě jsou povoleny (VNC, LogMeIn, TeamViewer apod.)

### Uveďte, zda připojení vyžaduje povolení uživatele.

Potvrzení o seznámení se s vnitřním předpisem

|  |  |  |  |
| --- | --- | --- | --- |
| **Druh vnitřního předpisu:** | **Směrnice GŘ č. XXII/2020/NPÚ** | **Číslo jednací** | **NPU-310/82165/2020** |
| **Název:** | **o správě informačních technologií** | | |

Podpisem potvrzuji, že jsem byl seznámen s výše uvedeným vnitřním předpisem formou ústní prezentace a obsahu vnitřního předpisu rozumím.

|  |  |  |
| --- | --- | --- |
| **Jméno a příjmení** | **Datum** | **Podpis** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. Bude zajištěno centrálně z úrovně GnŘ NPÚ externím dodavatelem formou konzultačních služeb. [↑](#footnote-ref-1)
2. V době vydání této směrnice se jedná o směrnici GŘ č. X/2018/NPÚ - užívání elektronické pošty [↑](#footnote-ref-2)
3. Tato pozice je zpravidla zřizována pouze na GnŘ NPÚ pro jednotlivé centrální informační systémy [↑](#footnote-ref-3)
4. Tato pozice je zpravidla zřizována pouze na GNŘ NPÚ, aktuálně jde o vedoucího odboru informatiky [↑](#footnote-ref-4)
5. Směrnice GŘ č. XXXII/2019/NPÚ [↑](#footnote-ref-5)
6. Další požadavky na kamerové systémy stanovuje vnitřní směrnice. Ke dni vydání této směrnice jde o směrnici GŘ č. XX/2018/NPÚ. [↑](#footnote-ref-6)
7. Bez ohledu na to, zda lze přerušit dodávku el. proudu nezamčeným jističem, např. hlavní jistič apod. [↑](#footnote-ref-7)
8. mezi nejznámější služby pro ověření kompromitovaných hesel patří stránka https://haveibeenpwned.com/Passwords [↑](#footnote-ref-8)
9. Viz Směrnice o užívání informačních technologií č. XXXII/2019/NPÚ [↑](#footnote-ref-9)
10. IS je dostupný v rámci VPN NPÚ na adrese http://192.168.210.50/index.php [↑](#footnote-ref-10)
11. V kratším termínu stanoveném pro tento bod postačují informace uvedené v příloze č. 5 v rozsahu bodů 1. 1, 1.2 a 1. 6. [↑](#footnote-ref-11)
12. Podrobnosti ke zpracování povinné dokumentace k provozu kamerového systému jsou uvedeny ve Směrnici GŘ č. XX/2018/NPÚ o ochraně osobních údajů a provozování kamerových systémů, bod 15. Jako součást dokumentace ICT postačuje konkrétní odkaz na příslušnou zpracovanou dokumentaci k provozu kamerových systémů (kdo ji zpracoval a datum zpracování). [↑](#footnote-ref-12)
13. Směrnice č. XXXII/2019/NPÚ o užívání informačních technologií [↑](#footnote-ref-13)