**Strategie rozvoje ICT - analýza rizik zabezpečení informací, verze 2022**

# Schéma/topologie sítě

PC1



 Tiskárna 1 Tiskárna 2

**. . . . H U B**



**WIFI router**

**notebook**



# Prostředky zpracování

Aplikace (softwarové prostředky zpracování OÚ)), které organizace používá.

|  |  |
| --- | --- |
| Název aplikací pro zpracování OÚ (prostředky zpracování) | Umístění databáze/dat (např. v rámci organizace nebo u jiného subjektu) |
| Czech point | PC |
| SW Triada |  |
| MS 2014+ | PC |
| MS Office | PC |
| Dotis | PC |
| Knihovnický systém | PC |
|  |  |
|  |  |
|  |  |

# Rizika

## Analýza rizik

Analýza rizik posuzuje slabá místa u podpůrných aktiv, pomocí kterých jsou zpracovávány osobní údaje. Rizika, která jsou hodnocena jako „**nízká**“ jsou akceptována. Na rizika hodnocená jako „**Vysoká**“ jsou přijímána opatření (viz kap. 2.2) pro jejich snížení.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Hodnocená oblast | Hrozby | S agendami související podpůrná aktiva | Popis již zavedených opatření a popis  zranitelností/slabých míst v zabezpečení | Riziko | Číslo opatření |
| 1. Řízení přístupu uživatelů, cíl: zajistit oprávněný přístup k informacím a předcházet neoprávněnému přístupu k systémům a službám | | | | | |
| Přidělení/odebrání/změna uživatelských přístupů | Neoprávněný přístup | SW prostředky zpracování |  |  |  |
| Správa privilegovaných přístupových práv | Neoprávněný přístup | SW prostředky zpracování | Žádná privilegovaná práva nejsou přidělena. | - | - |
| Přezkoumání rozsahu přístupových práv | Neoprávněný přístup | SW prostředky zpracování | Nedochází k přezkoumávání rozsahu přístupových práv, práva nejsou ani pravidelně obměňována. | Nízké | 4 |
| 1. Ochrana proti malwaru, cíl: zajistit, aby informace a vybavení pro zpracování informací byly chráněny proti malwaru | | | | | |
| Opatření proti malwaru | Neoprávněný přístup | SW prostředky zpracování |  | Nízké | - |
| Aktualizace a distribuce změnových balíčků | Neoprávněný přístup | SW prostředky zpracování |  | Nízké | - |
| 1. Zálohování ochrana dat při ztrátě, cíl: ochrana dat při ztrátě a zašifrování | | | | | |
| Způsob zálohování dat | Nedostupnost služeb | HW |  |  |  |
| Řízení plánu záloh | Nedostupnost služeb | Znalosti/procesy |  |  |  |
| 1. Řízení incidentů, cíl: učit se z neočekávaných událostí, uchovávat důkazy a plnit ohlašovací povinnost | | | | | |
| Odhalení, klasifikace a evidence incidentů | Opakování stejných nežádoucích jevů | Znalosti/procesy | Incidenty nejsou evidovány. | - | - |
| Přijímání opatření | Opakování stejných nežádoucích jevů | Znalosti/procesy | Opatření nebyla dosud přijata. | - | - |
| 1. Správa bezpečnosti sítí, cíl: zajistit ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací | | | | | |
| Kontrola a nastavení Firewallu | Neoprávněný přístup | HW, SW |  |  |  |
| Bezpečnost síťového provozu a připojení | Neoprávněný přístup | HW, SW |  |  |  |
| 1. Mobilní zařízení a práce na dálku, cíl: zajistit bezpečnost při použití mobilních zařízení a pro práci na dálku | | | | | |
| Politika mobilních zařízení | Neoprávněný přístup | SW prostředky zpracování | Mobilní zařízení jsou využívána pouze místostarostou a to notebook. V notebooku nejsou žádné osobní údaje. Notebook je zabezpečen uživatelským jménem a heslem. | Nízké | - |
| Práce na dálku, vzdálený přístup | Neoprávněný přístup | SW prostředky zpracování | Vzdálený přístup není. | Nízké | - |
| 1. Správa zařízení a SW, cíl: předcházet ztrátě, poškození, krádeži, kompromitaci aktiv, přerušení činnosti organizace a zajistit integritu provozních systémů | | | | | |
| Instalace software na provozní systémy | Nedostupnost služeb | SW prostředky zpracování | Odpovědnost za provozní systém není stanovena | Vysoké | 4 |
| Umístění zařízení a jeho ochrana | Zneužití zařízení | HW |  | Nízké | - |
| Podpůrné služby (např. UPS, klimatizace…) | Nedostupnost služeb | HW | Nejsou zajištěny žádné podpůrné systémy. | - | - |
| Bezpečnost kabelových rozvodů | Nedostupnost služeb | HW | Pravidelné revize elektrických zařízení dle zákonných požadavků neprobíhají | Vysoké | 3 |
| Údržba zařízení – plán údržby | Nedostupnost služeb | HW | Neprobíhá žádná údržba zařízení, není zpracován plán údržby. | Vysoké | 4 |
| Bezpečnost zařízení mimo prostory organizace | Nedostupnost služeb | HW | Mimo prostory organizace je používán pouze notebook místostarosty. V tomto notebooku nejsou přenášeny osobní údaje. Je zajištěn uživatelským jménem a heslem a není ponechán bez dozoru. | Vysoké | 4 |
| Bezpečná likvidace, opravy, opakované použití zařízení | Neoprávněný přístup | HW | Veškerá zařízení jsou likvidována mechanicky na základě vyřazovacích protokolů. | Nízké | - |
| Uživatelská zařízení bez obsluhy (např. sdílené tiskárny) | Neoprávněný přístup | HW |  | Nízké | - |
| Řízení kapacit | Nedostupnost služeb | HW | Řízení kapacit neprobíhá | Vysoké | 4 |
| 1. Provozní postupy a odpovědnosti ICT, cíl: zajistit správný, bezpečný a kontinuální provoz vybavení pro zpracování informací | | | | | |
| Dokumentované provozní postupy a odpovědnosti ICT | Neznalost pravidel nebo jejich absence | Znalosti/procesy | Nejsou vedeny – pro obec irelevantní | - | - |
| Plán monitoringu a kontrol | Vznik nežádoucích událostí | Znalosti/procesy | Není veden – pro obec irelevantní | - | - |
| Záznamy významných změn v ICT | Neznalost pravidel nebo jejich absence | Znalosti/procesy | Nejsou vedeny – pro obec irelevantní | - | - |
| Řízení kapacit | Nedostupnost služeb | HW | Odpovědnost má starosta | - | - |
| 1. Kryptografická opatření, cíl: zajistit řádné a efektivní užívání kryptografie k ochraně důvěrnosti, autentičnosti a / nebo integrity informací | | | | | |
| Politika používání kryptografických opatření | Neoprávněný přístup | SW | Kryptografická opatření se používají u podpisových certifikátů a certifikátů pro bankovní přístup. Certifikáty jsou vydávány se souhlasem starosty na konkrétní jména uživatelů | Nízké | - |
| Správa klíčů | Neoprávněný přístup | Znalosti/procesy | Klíče k certifikátům zná pouze daný uživatel a nikde nejsou evidovány. | Nízké | - |
| 1. Bezpečné oblasti, cíl: předcházet neoprávněnému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace | | | | | |
| Zabezpečení prostor a vybavení | Neoprávněný přístup | Prostory |  | Nízké | 4 |
| Ochrana před vnějšími hrozbami a hrozbami prostředí | Nedostupnost služeb | HW | Budova je zabezpečena hromosvodem, přepěťovými zásuvkami. Jiné zabezpečení není nastaveno. | Nízké | 4 |
| 1. Bezpečnost informací ve vztazích s třetími stranami, cíl: zajistit ochranu aktiv organizace, ke kterým mají dodavatelé přístup | | | | | |
| Bezpečnostní požadavky v dohodách s dodavateli | Neoprávněný přístup | SW prostředky zpracování |  | Vysoké | 5 |
| Dodavatelský řetězec | Neoprávněný přístup | SW prostředky zpracování | Žádný dodavatelský řetězec není využíván. | Nízké | - |

## Plán opatření (plán zvládání rizik) na rizika, která jsou hodnocena jako „vysoká“

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Číslo  opatření | Popis opatření pro snížení rizika (plán nebo úkol) | Odpovídá | Plánovaný termín | Předpokládané náklady v Kč | Poznámka | Dokončeno dne |
| 1 | Zajistit pravidelnou obměnu přístupů (hesel) | Starosta | Průběžně | 0,- |  |  |
| 2 | Zavést pravidelnou revizi elektrických zařízení. | Starosta | Průběžně | 5 000,- |  |  |
| 3 | S každým dodavatelem podepisovat mlčenlivost | starosta | Průběžně | 0,- |  |  |
| 4 |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

# Plán přístupových práv uživatelů

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Rozsah přístupů | Název pracovního místa | | | | | | | | | | | | | |
| Popis přístupového práva  (X = přístup) | starosta | místostarosta | účetní | knihovnice |  |  |  |  |  |  |  |  |  |  |
| Přístup k síti |  | x | x |  |  |  |  |  |  |  |  |  |  |  |
| PC 1 |  | x | x |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Tiskárna 1 | x | x | X |  |  |  |  |  |  |  |  |  |  |  |
| Tiskárna 2 | x | x | X |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| notebook |  | X |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

# Plán záloh

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Popis zálohy (co) | Postup zálohování/archivace (jak) | Četnost (kdy) | Místo uložení zálohy (kde) | Způsob kontroly obnovitelnosti | Poznámka |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# Záznam o schválení dokumentu

Dokument schválil dne 01.05.2023 Ing. Miloš Veselý, starosta