Technická opatření ICT

Cílem dokumentu je definovat strategii ICT v organizaci tzn. popsat stávající stav a navrhnout rozvojové programy pro další období.

Obsah

[1 Soupis použitých SW 1](#_Toc500751064)

[2 Strategie a nastavení ICT systémů 2](#_Toc500751065)

[2.1 Způsob řízení přístupu uživatelů 2](#_Toc500751066)

[2.2 Zálohování informací 2](#_Toc500751067)

[2.3 Opatření proti malwaru 2](#_Toc500751068)

[2.4 Práce na dálku 2](#_Toc500751069)

[2.5 Firewall 2](#_Toc500751070)

[2.6 Politika mobilních zařízení 2](#_Toc500751071)

[2.7 Řízení kapacit 2](#_Toc500751072)

[2.8 Bezpečná likvidace nebo opakované použití zařízení 3](#_Toc500751073)

[2.9 Umístění zařízení a jeho ochrana 3](#_Toc500751074)

[2.10 Podpůrné služby 3](#_Toc500751075)

[2.11 Údržba zařízení 3](#_Toc500751076)

[2.12 Používání privilegovaných programových nástrojů 3](#_Toc500751077)

[2.13 Zabezpečení zařízení mimo prostory organizace 3](#_Toc500751078)

[2.14 Řízení změn a událostí 4](#_Toc500751079)

[2.15 Monitorování, měření a hodnocení 4](#_Toc500751080)

[2.16 Vývoj informačních systémů 4](#_Toc500751081)

[2.17 Incidenty a události 4](#_Toc500751082)

[2.18 Kryptografie/šifrování 4](#_Toc500751083)

[2.19 Dokumentované provozní postupy 4](#_Toc500751084)

[2.20 Pravidla pro uživatele 4](#_Toc500751085)

[3 Rozvoj ICT systémů 5](#_Toc500751086)

[4 Kontinuita provozu 5](#_Toc500751087)

# Soupis použitých SW

Uveďte všechny aplikace, které organizace používá,jejich umístění a rozsahu logování.

|  |  |  |
| --- | --- | --- |
| Název aplikace pro zpracování OÚ | Umístění databáze (např. v rámci organizace nebo jiného subjektu) | Rozsah logování (jaké informace o činnosti uživatele aplikace zaznamenává) |
| MS Office |  |  |
| Helios Fenix |  |  |
| MS 2014 + |  |  |
| Dotis |  |  |

# Strategie a nastavení ICT systémů

## Způsob řízení přístupu uživatelů

Definujte politiku řízení přístupu uživatelů (včetně výhradních přístupů „admin“ u serverů a pracovních stanic) k ICT systémům (síť/systém, aplikace, cloud, adresáře/složky, vzdálený přístup, atp.). Včetně řízení změn a rušení přístupů.

Popis stávajícího stavu:

Server není používán, k pracovním stanicím je jednotný přístup pro všechny uživatele. Stejně řešen je i přístup k aplikacím. Cloud a vzdálený přístup není řešen.

Návrhy na zlepšení, plánovaná opatření:

Vytvoření přístupu pro jednotlivé uživatele.

## Zálohování informací

Probíhá zálohování dat podle schváleného Plánu záloh?

Popis stávajícího stavu:

Zálohy probíhají na pevný disk

Návrhy na zlepšení, plánovaná opatření:

Zálohování na zabezpečené úložiště (cloud).

## Opatření proti malwaru

Jaká jsou opatření proti škodlivým programům, jak probíhá jejich údržba/aktualizace a jak jsou distribuovány na koncová zařízení.

Popis stávajícího stavu:

Pomocí antivirového programu, aktualizace probíhají automaticky.

Návrhy na zlepšení, plánovaná opatření:

## Práce na dálku

Popište technickézpůsoby vzdáleného přístupu do sítě (např. VPN, FTP atp.).

Popis stávajícího stavu:

Vzdálených přístupů do sítě se nevyužívá.

Návrhy na zlepšení, plánovaná opatření:

## Firewall

Popište, kdo a jakým způsobem nastavuje, monitoruje a ověřuje funkčnost firewallů.

Popis stávajícího stavu:

Využíván firewall, který je součástí antivirového programu. Monitoring a ověření funkčnosti neprobíhá.

Návrhy na zlepšení, plánovaná opatření:

Pořízení a nastavení hardwarového firewallu z něhož budou pořizovány pravidelné reporty, bude pravidelně aktualizován a bude kontrolována jeho funkčnost

## Politika mobilních zařízení

Popište stávající politiku použití mobilních zařízení (např. zda a které typy zařízení se připojují do sítě a za jakým účelem – internet, pošta atp.)

Popis stávajícího stavu:

Mobilní zařízení připojující se do sítě nejsou používány.

Návrhy na zlepšení, plánovaná opatření:

## Řízení kapacit

Zodpovídáte za hlídání kapacit systémů (např. prostor na disku, výkon procesoru, vytíženost sítě), a jak řešíte jejich nedostatek.

Popis stávajícího stavu:

Kapacita disků, výkony procesorů ani vytíženost sítě není hlídána. Nedostatek prostoru disků se řeší navýšením kapacity nákupem nových disků.

Návrhy na zlepšení, plánovaná opatření:

Monitoring výkonu procesorů, kontrola vytíženosti sítě.

## Bezpečná likvidace nebo opakované použití zařízení

Popište způsob likvidace paměťových médií a způsob předávání zařízení do oprav/jinému subjektu.

Popis stávajícího stavu:

Paměťová média typu CD,DVD a flashdisky se likvidují vyhozením do komunálního odpadu. Zařízení předávána do opravy jinému subjektu probíhají na základě předávacích protokolů.

Návrhy na zlepšení, plánovaná opatření:

Likvidace CD, DVD pomocí skartovacích zařízení. Flashdisky a ostatní zařízení které není možno skartovat na skartovacích strojích zlikvidovat tak, aby nebylo možné jejich přečtení. Zařízení předávána do opravy jiným subjektům je-li to možné předávat do opravy bez citlivých dat.

## Umístění zařízení a jeho ochrana

Definujte,kdo je odpovědný za umístění ICT zařízení a prvků sítě, včetně datových kabelových rozvodů.

Popis stávajícího stavu:

Za umístění je odpovědný starosta a místostarosta.

Návrhy na zlepšení, plánovaná opatření:

Pořízení elektronického zabezpečovacího systému prostor obecního úřadu.

## Podpůrné služby

Podpůrná zařízení jsou zařízenípotřebná pro zabezpečení provozu důležitých procesů a zařízení. Jedná se například o záložní zdroje, klimatizaci, nouzové vypínače apod. Definujte, v jakém rozsahu se o něstaráte (zajištění revizí atp.).

Popis stávajícího stavu:

Záložní zdroje, klimatizace atd. nejsou používány.

Návrhy na zlepšení, plánovaná opatření:

Je zapotřebí pořízení záložních zdrojů k PC.

## Údržba zařízení

Popište jaké údržby a v jakém rozsahu provádíte.

Popis stávajícího stavu:

Provádí se pravidelné revize elektrozařízení.

Návrhy na zlepšení, plánovaná opatření:

## Používání privilegovaných programových nástrojů

Popište, které nástroje (SW) pro správu a monitorování sítě používáte a v jakém rozsahu.

Popis stávajícího stavu:

Nepoužívají se.

Návrhy na zlepšení, plánovaná opatření:

Pořízení firewallu. Monitoring sítě pravidelnými reporty z firewallu.

## Zabezpečení zařízení mimo prostory organizace

Popište zařízení, která jsou umístěna mimo budovy organizace (např. satelit, cloud atp.).

Popis stávajícího stavu:

Není využíváno zařízení umístěných mimo budovy organizace.

Návrhy na zlepšení, plánovaná opatření:

## Řízení změn a událostí

Zapište, kam provádíte záznamy o důležitých změnách a událostech v síti, o instalacích SW atp. (např. Administrátorský/Provozní deník).

Popis stávajícího stavu:

Záznamy se neprovádějí.

Návrhy na zlepšení, plánovaná opatření:

Vedení záznamů v provozním deníku.

## Monitorování, měření a hodnocení

Je k dispozici Plán monitoringu (např. stav aktivních prvků sítě, neoprávněný přístup) a kontrol (např. obnovitelnost záloh, aktuálnost virové databáze)- co, kdo, kdy, proč, jak…,?

Popis stávajícího stavu:

Není k dispozici.

Návrhy na zlepšení, plánovaná opatření:

## Vývoj informačních systémů

Popište, v jakém rozsahu a pro které systémy probíhá.

Popis stávajícího stavu:

Vývoj neprobíhá.

Návrhy na zlepšení, plánovaná opatření:

## Incidenty a události

Popište, jak a kde evidujete bezpečnostní incidenty, zda je definováno, co je bezpečnostní incident.

Popis stávajícího stavu:

Není evidováno ani definováno.

Návrhy na zlepšení, plánovaná opatření:

Evidovat incidenty a definovat bezpečnostní incidenty

## Kryptografie/šifrování

Popište, jaké nástroje se používají pro šifrování dat (např. VPN atp.).

Popis stávajícího stavu:

Nepoužívají se

Návrhy na zlepšení, plánovaná opatření:

## Dokumentované provozní postupy

Je k dispozici nákres sítě – topologie s vyznačením oddělení sítí a důležitými prvky sítě? Zaznamenávají se důležitá systémová nastavení, popisy aplikačních procesů, procedur, datových struktur, autorizačních procesů, řešení redundance (seznam prvků vysoké dostupnosti) apod.

Napište, zda vedete seznam systémové dokumentace, která obsahuje účel, popis a osobu odpovědnou za vedení dokumentace v aktuální podobě, místo uložení, způsob zabezpečení.

Popis stávajícího stavu:

Není k dispozici

Návrhy na zlepšení, plánovaná opatření:

## Pravidla pro uživatele

Jsou definována a proškolována pravidla pro chování uživatelů ICT?

Popis stávajícího stavu:

Nejsou definována a proškolována.

Návrhy na zlepšení, plánovaná opatření:

Definovat pravidla a pravidelně proškolovat uživatele ICT.

# Rozvoj ICT systémů

Popište, kde vidíte slabá místa v provozu a zabezpečení dat a která opatření doporučujete zavést.

1. Slabá místa jsou v zabezpečení sítě. Data nejsou zabezpečena a šifrována.

Je důležité zabezpečit síť, pravidelně zálohovat a šifrovat data.

# Zabezpečení kontinuity provozu

Je pro situace, kdy síťová infrastruktura zkolabovala, nejde elektřina, hacker zašifroval data, definován čas a způsob obnovy provozu sítě?

Popis stávajícího stavu:

Není definován čas a způsob obnovy.

Návrhy na zlepšení, plánovaná opatření:

V případě výpadku elektřiny by bylo dobré pořídit záložní zdroj k PC, v případě hackerského útoku mít zálohu dat, aby byla možná obnova. Tuto zálohu je potřeba mít uloženo mimo PC, které jsou využívány k práci (externí disk, cloud atd.) Definovat způsob a čas obnovy.