| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vložte název registrované právnické osoby | | | | | | | |
| Číslo dokumentu:<br>P22S | | | | | Název dokumentu:<br>**Politika protokolování a monitorování** | | | | | | | |
| Verze:<br>1.0 | | Datum účinnosti:<br>01.01.2025 | | | Vlastník dokumentu: | | | | | | | |
| X | Politika | | Standard | | Postup | | Formulář | | Registr | | Jiné | |

| **Historie revizí** | | | | |
|---|---|---|---|---|
| **Číslo revize** | **Datum revize** | **Změny** | **Přezkoumal** | **Vlastník procesu** |
| | | | | |
| | | | | |

| **Schválení** | | | |
|---|---|---|---|
| **Jméno** | **Funkce** | **Datum** | **Podpis** |
| | | | |
| | | | |

V souladu s normami a právními předpisy

| Norma / právní předpis | Kapitola / článek | Komentář |
|---|---|---|
| ISO/IEC 27001:2022 | Kapitola 8 | Provozní opatření včetně protokolování |
| ISO/IEC 27002:2022 | Opatření 8.15, 8.16, 8.17 | Protokolování událostí, ochrana logů a monitorování |
| NIST SP 800-53 Rev.5 | AU-2 až AU-12, SI-4 | Obsah a přezkum auditních logů, uchovávání, detekce anomálií a upozorňování |
| GDPR | Články 5 odst. 1 písm. f), 32, 33 | Důvěrnost a integrita dat, technická opatření a oznamování porušení zabezpečení |
| směrnice NIS2 | Články 21 odst. 2 písm. d), 23 | Mechanismy protokolování pro detekci anomálií a hlášení incidentů do 24 hodin |
| nařízení DORA | Články 10, 15 | Digitální provozní odolnost, monitorování a protokolování poskytovatelů služeb |
| COBIT 2019 | DSS01.03, DSS05.02 | Dohledatelnost činností a ochrana prostřednictvím protokolování a monitorování |

## 1. Účel

1.1 Tato politika stanoví povinná opatření pro protokolování a monitorování za účelem zajištění bezpečnosti, odpovědnosti a provozní integrity IT systémů organizace.

1.2 Vymezuje typy událostí, které musí být protokolovány, způsob ukládání logů, způsob jejich přezkumu a odpovědnosti zaměstnanců a poskytovatelů služeb.

1.3 Protokolování a monitorování podporují detekci hrozeb, soulad s právními a regulatorními požadavky, reakci na incidenty a forenzní analýzu.

1.4 Tato politika umožňuje organizaci plnit požadavky na provozní opatření podle ISO/IEC 27001 a podporuje průběžnou připravenost na audit, důvěru zákazníků a soulad s GDPR, směrnicí NIS2 a nařízením DORA.

## 2. Rozsah

**2.1 Tato politika se vztahuje na všechny systémy a uživatele v rámci organizace, včetně:**

2.1.1 pracovních stanic, notebooků, serverů, firewallů, přepínačů, směrovačů a bezdrátových přístupových bodů

2.1.2 cloudových služeb používaných pro provozní činnosti organizace (např. e-mail, ukládání souborů, zálohování, nástroje pro spolupráci)

2.1.3 funkcí protokolování v antivirovém softwaru, aplikacích, operačních systémech a síťových prvcích

2.1.4 všech zaměstnanců, smluvních pracovníků a poskytovatelů řízených služeb (MSP), kteří systémy používají nebo spravují

2.1.5 jakéhokoli místa, kde jsou používány firemní IT systémy, včetně prostředí práce na dálku, hybridního režimu nebo využívání soukromých zařízení (BYOD)

2.2 Tato politika se rovněž vztahuje na logy vytvářené službami třetích stran, pokud má organizace administrativní přístup nebo smluvní práva na audit.

**3. Cíle**

3.1 Zajistit protokolování systémových aktivit, včetně autentizace, změn konfigurace, přístupu k citlivým datům a bezpečnostních upozornění.

3.2 Udržovat bezpečné a přesné logy pro detekci porušení politiky, systémových chyb nebo neoprávněných činností.

3.3 Umožnit rychlý přezkum logů během incidentů, vyšetřování a auditů.

3.4 Podporovat synchronizaci času za účelem zajištění integrity a korelace logových dat.

3.5 Chránit logy před manipulací, ztrátou nebo předčasným smazáním.

3.6 Plnit právní a regulatorní povinnosti týkající se odpovědnosti za systémové činnosti, dohledatelnosti a reakce na porušení zabezpečení.

**4. Role a odpovědnosti**

**4.1 Generální ředitel (GM)**

4.1.1 schvaluje tuto politiku a zajišťuje její zavedení napříč všemi podnikovými systémy

4.1.2 přezkoumává upozornění s vysokou závažností a závažná zjištění auditů oznámená IT funkcí nebo funkcí ochrany soukromí

4.1.3 schvaluje výjimky v případech, kdy protokolování nebo uchovávání nelze technicky vynutit

**4.2 Poskytovatel IT podpory / interní IT funkce**

4.2.1 zavádí a konfiguruje protokolování pro operační systémy, síťová zařízení, antivirové nástroje a klíčové aplikace

4.2.2 zajišťuje, aby byly logy uchovávány, zálohovány a chráněny proti změnám

4.2.3 provádí přezkum logů podle stanoveného harmonogramu a vyšetřuje podezřelé nebo neoprávněné činnosti

4.2.4 udržuje systémy upozorňování, které identifikují anomální chování nebo indikátory kompromitace

[ ... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ... ]

**9. Požadavky na přezkoumávání a aktualizaci**

**9.1 Roční přezkum**

9.1.1 Tato politika musí být nejméně jednou ročně přezkoumána generálním ředitelem za podpory poskytovatele IT podpory a koordinátora ochrany soukromí.

**9.2 Spouštěče přezkumu**

**9.2.1 Neplánované přezkumy musí být provedeny v reakci na:**

9.2.1.1 zjištění související s logy z interních nebo externích auditů

9.2.1.2 bezpečnostní incidenty, při nichž logy chyběly, byly poškozené nebo byly nedostatečné

9.2.1.3 významné změny IT infrastruktury (např. migrace na cloudové platformy pro protokolování)

9.2.1.4 aktualizace právních nebo regulatorních povinností (např. GDPR, směrnice NIS2, nařízení DORA)

**9.3 Řízení verzí**

9.3.1 Všechny změny této politiky musí být zaznamenány s číslem verze, datem a shrnutím změn.

9.3.2 Předchozí verze musí být archivovány a uchovávány nejméně 3 roky.

9.3.3 Aktualizované politiky musí být oznámeny dotčeným zainteresovaným stranám, zejména těm se systémovým přístupem.

## 10. Související politiky a vazby

### 10.1 Tato politika přímo podporuje a je podporována následujícími SME politikami informační bezpečnosti:

10.1.1 P17S – Politika ochrany dat a soukromí: zajišťuje, aby logová data obsahující osobní údaje byla spravována s ohledem na integritu, uchovávání a ochranu přístupu v souladu s požadavky GDPR.

10.1.2 P21S – Politika bezpečnosti sítí: poskytuje základ pro zachycování logů souvisejících s firewally, bezdrátovým přístupem, VPN a monitorováním segmentace.

10.1.3 P24S – Politika bezpečného vývoje: zajišťuje, aby aplikační logy (např. pro pokusy o přihlášení, chyby a výjimky) byly zahrnuty do návrhu softwaru a jeho provozu.

10.1.4 P30S – Politika reakce na incidenty: spoléhá na přesná a úplná logová data při detekci, analýze a reakci na události informační bezpečnosti.

10.1.5 P23S – Politika synchronizace času: zajišťuje konzistentní a dohledatelná časová razítka napříč všemi systémy, aby bylo možné logy korelovat během vyšetřování.

## 11. Referenční normy a rámce

### 11.1 ISO/IEC 27001

11.1.1 Kapitola 8 – Vyžaduje zavedení provozních opatření ke zmírnění rizik informační bezpečnosti, včetně protokolování.

### 11.2 ISO/IEC 27002

11.2.1 Opatření 8.15 – Vyžaduje protokolování událostí na podporu detekce anomálií a odpovědnosti.

11.2.2 Opatření 8.16 – Vyžaduje ochranu logů před manipulací a neoprávněným přístupem.

11.2.3 Opatření 8.17 – Vyžaduje monitorování systémů z hlediska neobvyklé činnosti a potvrzení účinnosti monitorovacích opatření.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 až AU-12 – Pokrývají obsah auditních logů, jejich přezkum, uchovávání a automatizované upozorňování.

11.3.2 SI-4 – Vyžaduje detekci systémových anomálií a hlášení podezřelých událostí.

### 11.4 GDPR

11.4.1 Článek 5 odst. 1 písm. f) – Vyžaduje integritu a důvěrnost osobních údajů, což zahrnuje i protokolování přístupu.

11.4.2 Článek 32 – Ukládá technická a organizační opatření k zajištění bezpečnosti, včetně protokolování a monitorování.

11.4.3 Článek 33 – Vyžaduje včasné oznámení porušení zabezpečení, podpořené logy umožňujícími analýzu kořenové příčiny.

### 11.5 směrnice NIS2

11.5.1 Článek 21 odst. 2 písm. d) – Vyžaduje mechanismy protokolování, které detekují anomálie a poskytují podporu při vyšetřování incidentů.

11.5.2 Článek 23 – Ukládá hlášení incidentů do 24 hodin, což závisí na přesných a včasných logových datech.

### 11.6 nařízení DORA

11.6.1 Článek 10 – Vyžaduje digitální provozní odolnost, včetně dohledatelnosti incidentů souvisejících s ICT prostřednictvím protokolování.

11.6.2 Článek 15 – Ukládá monitorování poskytovatelů služeb, včetně přístupu k logům a práv na jejich přezkum.

**11.7 COBIT 2019**

11.7.1 DSS01.03 – Vyžaduje dohledatelnost systémové aktivity prostřednictvím protokolování a monitorování.

11.7.2 DSS05.02 – Řeší protokolování jako klíčové opatření při ochraně proti malwaru a jiné neoprávněné činnosti.