| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vnesite naziv registrirane pravne osebe | | | | | | | |
| Številka dokumenta:<br>P30S | | | | | Naslov dokumenta:<br>**Politika odzivanja na incidente** | | | | | | | |
| Različica:<br>1.0 | | Datum začetka veljavnosti:<br>01.01.2025 | | | Lastnik dokumenta: | | | | | | | |
| X | Politika | | Standard | | Postopek | | Obrazec | | Register | | Drugo | |

| **Zgodovina revizij** | | | | |
|---|---|---|---|---|
| **Številka revizije** | **Datum revizije** | **Spremembe** | **Pregledal** | **Lastnik procesa** |
| | | | | |
| | | | | |

| **Odobritve** | | | |
|---|---|---|---|
| **Ime** | **Delovno mesto** | **Datum** | **Podpis** |
| | | | |
| | | | |

Usklajenost s standardi in predpisi

| Standard/predpis | Klavzula/člen | Komentar |
|---|---|---|
| ISO/IEC 27001:2022 | Klavzule 6.1, 6.3, 8 | upravljanje incidentov, nenehno izboljševanje, operativno upravljanje |
| ISO/IEC 27002:2022 | Kontrole 5.24, 5.25 | zaznavanje incidentov, pripravljenost, učenje |
| NIST SP 800-53 Rev. 5 | IR-4, IR-5, IR-6 | obravnava in spremljanje incidentov, poročanje |
| Uredba (EU) GDPR | Člen 33 | zahteve glede prijave kršitev |
| Direktiva (EU) NIS2 | Člen 23 | obvezno poročanje o kibernetskih incidentih |
| Uredba (EU) DORA | Člen 17 | upravljanje incidentov IKT |
| COBIT 2019 | DSS02, DSS04 | upravljanje zahtevkov za storitve in incidentov ter neprekinjeno poslovanje |

**1. Namen**

1.1. Ta politika določa, kako organizacija zaznava, prijavlja in obravnava incidente informacijske varnosti, ki vplivajo na njene digitalne sisteme, podatke ali storitve.

1.2. Organizaciji omogoča zmanjšanje škode, zaščito podatkov strank in izpolnjevanje regulativnih obveznosti, kot je zahteva GDPR glede prijave kršitve v 72 urah.

1.3. Politika zagotavlja jasno opredeljene odgovornosti, komunikacijske poti in aktivnosti po incidentu, tudi v manjših organizacijah brez namenske varnostne ekipe.

**2. Področje uporabe**

**2.1. Ta politika velja za:**

2.1.1. vse zaposlene, pogodbene izvajalce in zunanje ponudnike IT-storitev,

2.1.2. vse sisteme in storitve, ki jih upravlja podjetje, vključno s spletnimi mesti, oblačnimi platformami, mobilnimi napravami, prenosnimi računalniki in e-poštnimi računi,

**2.1.3. vse vrste incidentov, vključno z:**

2.1.3.1. nepooblaščenim dostopom do podatkov ali sistemov,

2.1.3.2. okužbami z zlonamerno programsko opremo ali izsiljevalsko programsko opremo,

2.1.3.3. poskusi spletnega ribarjenja ali socialnega inženiringa,

2.1.3.4. izpadi sistemov zaradi kibernetskega napada ali neustrezne uporabe,

2.1.3.5. nenamernim razkritjem ali izbrisom občutljivih informacij,

2.1.3.6. izgubo ali krajo poslovnih naprav ali nosilcev podatkov.

**3. Cilji**

3.1. Vzpostaviti jasen postopek za prepoznavanje in eskalacijo varnostnih incidentov.

3.2. Zagotoviti, da so incidenti prijavljeni, evidentirani in obravnavani v vnaprej določenih časovnih okvirih.

3.3. Omogočiti hitro zajezitev škode, obnovitev podatkov in ponovno vzpostavitev storitev.

3.4. Zagotoviti, da so prizadete strani (npr. stranke, regulatorji) obveščene, kadar to zahteva zakonodaja.

3.5. Preprečevati ponovitve z analizo temeljnega vzroka, korektivnimi ukrepi in izboljšanjem politike.

3.6. Omogočiti SME izpolnjevanje zahtev za certificiranje po ISO/IEC 27001 in dokazovanje odgovornosti med revizijami.

**4. Vloge in odgovornosti**

**4.1. Generalni direktor (GM)**

4.1.1. Je lastnik te politike in zagotavlja njeno izvajanje.

4.1.2. Nadzoruje dejavnosti odzivanja na incidente in odobri obvestila regulatorjem ali strankam.

4.1.3. Pregleduje poročila po incidentu in zagotavlja posodobitve politike, kadar so potrebne.

4.1.4. Lahko prenese naloge koordinacije, vendar ohrani odgovornost.

**4.2. Ponudnik IT-podpore / skrbnik sistema (notranji ali zunanji)**

4.2.1. Zaznava in preiskuje morebitne varnostne incidente.

4.2.2. Izvaja ukrepe za zajezitev in obnovitev (npr. onemogoči dostop, obnovi varnostne kopije).

4.2.3. O vseh potrjenih ali sumljivih incidentih obvesti GM v 1 uri od zaznave.

4.2.4. Vodi dnevnik incidentov s časovnimi žigi, oceno vpliva in izvedenimi odzivnimi ukrepi.

[ ... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ... ]

**9. Zahteve za pregled in posodobitev**

**9.1. Redni pregled**

**9.1.1. To politiko mora Generalni direktor (GM) pregledati najmanj enkrat na 12 mesecev, da zagotovi:**

9.1.1.1. usklajenost s kontrolami ISO/IEC 27001:2022,

9.1.1.2. odzivnost na nove grožnje, tveganja in incidente,

9.1.1.3. stalno skladnost s pravnimi in pogodbenimi obveznostmi (npr. GDPR, DORA).

**9.2. Sprožilni dogodki**

**9.2.1. Politiko je treba pregledati in posodobiti tudi po:**

9.2.1.1. vsakem incidentu z visoko stopnjo resnosti ali regulativnem obvestilu,

9.2.1.2. uvedbi nove IT-infrastrukture ali spremembah sistemov,

9.2.1.3. spremembah pravnih zahtev v zvezi z varnostnimi kršitvami.

**9.3. Dokumentiranje pregleda in razdeljevanje**

9.3.1. Vsi pregledi in spremembe morajo biti dokumentirani v evidenci sprememb politike.

9.3.2. Posodobljene različice morajo biti razdeljene vsem zaposlenim, dobaviteljem in ponudnikom IT-podpore, ki sodelujejo pri varnosti ali delovanju sistemov.

9.3.3. Dokazila o ozaveščenosti zaposlenih (npr. zapiski sestankov ali e-poštne potrditve) morajo biti hranjena zaradi pripravljenosti na revizijo.

**10. Povezane politike in povezave**

**10.1. To politiko je treba uporabljati usklajeno z naslednjimi politikami SME:**

10.1.1. P1S – Politika informacijske varnosti: določa splošna pričakovanja glede ohranjanja zaupnosti, celovitosti in razpoložljivosti med delovanjem, vključno z obravnavo incidentov.

10.1.2. P2S – Politika vlog in odgovornosti upravljanja: vzpostavlja strukture pooblastil in odgovornosti za zaznavanje, poročanje in eskalacijo incidentov.

10.1.3. P4S – Politika nadzora dostopa: omogoča takojšen preklic pravic dostopa med ukrepi odzivanja na incidente.

10.1.4. P8S – Politika ozaveščanja in usposabljanja za informacijsko varnost: zagotavlja, da lahko vsi zaposleni učinkovito prepoznajo in prijavijo varnostne incidente.

10.1.5. P17S – Politika varstva podatkov in zasebnosti: usmerja pravne postopke prijave kršitev po GDPR in podpira regulativno skladnost med incidenti.

10.1.6. P22S – Politika beleženja in spremljanja: zagotavlja potrebna orodja in preglednost za zaznavanje, analizo in presojo varnostnih dogodkov.

10.1.7. P31S – Politika zbiranja dokazov in forenzike: podpira preiskavo in pravno zagovornost ukrepov, povezanih z incidenti, z usmerjanjem pravilnega ravnanja z dokazi.

10.2. Te politike skupaj vzpostavljajo operativni okvir SME za zaznavanje incidentov informacijske varnosti, odzivanje nanje in obnovitev po njih.

## 11. Referenčni standardi in okviri

### 11.1. ISO/IEC 27001

11.1.1. Klavzula 6.1 – zahteva načrtovanje obravnave tveganj, vključno s pripravo na incidente.

11.1.2. Klavzula 6.3 – podpira nenehno izboljševanje na podlagi izkušenj, pridobljenih iz varnostnih dogodkov.

11.1.3. Klavzula 8.1 – poudarja operativno upravljanje za obravnavo incidentov in motenj.

### 11.2. ISO/IEC 27002

11.2.1. Kontrola 5.24 – zahteva strukturiran pristop k poročanju, presoji in odzivanju na incidente informacijske varnosti.

11.2.2. Kontrola 5.25 – osredotoča se na učenje iz incidentov za izboljšanje prihodnje pripravljenosti in odpornosti sistemov.

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

11.3.1. IR-4 – določa postopke obravnave incidentov, vključno z zajezitvijo in obnovitvijo.

11.3.2. IR-5 – vzpostavlja zahteve za spremljanje in analizo incidentov.

11.3.3. IR-6 – predpisuje protokole za zunanje in notranje poročanje o incidentih.

### 11.4. Uredba (EU) GDPR

11.4.1. Člen 33 – zahteva prijavo kršitev varnosti osebnih podatkov regulatorjem v 72 urah skupaj s podrobnostmi o obsegu in ukrepih za ublažitev.

### 11.5. Direktiva (EU) NIS2 (2022/2555)

11.5.1. Člen 23 – zahteva, da bistveni in pomembni subjekti pomembne incidente prijavijo pristojnim organom z uporabo standardiziranih oblik poročanja.

### 11.6. Uredba (EU) DORA (2022/2554)

11.6.1. Člen 17 – zahteva, da finančni subjekti razvrščajo, prijavljajo in spremljajo incidente in motnje, povezane s sistemi IKT.

### 11.7. COBIT 2019

11.7.1. DSS02 – Upravljanje zahtevkov za storitve in incidentov: usmerja učinkovito obravnavo operativnih in varnostnih incidentov v skladu s cilji upravljanja.

11.7.2. DSS04 – Upravljanje neprekinjenega poslovanja: povezuje odzivanje na incidente s širšimi strategijami neprekinjenega poslovanja in obnovitve.