					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P30S					Naziv dokumenta: **Politika upravljanja sigurnosnim incidentima**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i regulativom

Standard/regulativa	Točka/članak	Napomena
ISO/IEC 27001:2022	Točke 6.1, 6.3, 8	upravljanje incidentima, kontinuirano poboljšavanje, operativne kontrole
ISO/IEC 27002:2022	Kontrole 5.24, 5.25	otkrivanje incidenata, pripravnost, učenje iz incidenata
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	postupanje s incidentima, praćenje i prijavljivanje
GDPR EU	Članak 33	zahtjevi za prijavu povrede osobnih podataka
Direktiva EU NIS2	Članak 23	obvezna prijava kibernetičkih incidenata
Uredba EU DORA	Članak 17	upravljanje IKT incidentima
COBIT 2019	DSS02, DSS04	upravljanje zahtjevima za uslugu, incidentima i kontinuitetom

1. Svrha

1.1. Ova politika definira način na koji organizacija otkriva, prijavljuje i rješava incidente informacijske sigurnosti koji utječu na njezine digitalne sustave, podatke ili usluge.

1.2. Ova politika omogućuje organizaciji smanjenje štete, zaštitu podataka klijenata i ispunjavanje regulatornih obveza, uključujući zahtjev iz GDPR-a za prijavu povrede osobnih podataka u roku od 72 sata.

1.3. Ova politika osigurava jasno definirane odgovornosti, komunikacijske korake i aktivnosti nakon incidenta, uključujući i primjenu u malim organizacijama bez namjenskog sigurnosnog tima.

2. Područje primjene

2.1. Ova politika primjenjuje se na:

2.1.1. sve zaposlenike, ugovorne izvođače i vanjske pružatelje IT usluga

2.1.2. sve sustave i usluge kojima upravlja društvo, uključujući mrežne stranice, platforme u oblaku, mobilne uređaje, prijenosna računala i račune e-pošte

2.1.3. sve vrste incidenata, uključujući:

2.1.3.1. neovlašten pristup podacima ili sustavima

2.1.3.2. zarazu zlonamjernim softverom ili ucjenjivačkim softverom

2.1.3.3. pokušaje krađe identiteta ili socijalnog inženjeringa

2.1.3.4. prekide rada sustava zbog kibernetičkog napada ili zlouporabe

2.1.3.5. slučajno otkrivanje ili brisanje osjetljivih informacija

2.1.3.6. gubitak ili krađu poslovnih uređaja ili medija za pohranu

3. Ciljevi

3.1. Uspostaviti jasan postupak za prepoznavanje i eskalaciju sigurnosnih incidenata.

3.2. Osigurati da se incidenti prijavljuju, evidentiraju i obrađuju u unaprijed definiranim rokovima.

3.3. Omogućiti brzo ograničavanje štete, povrat podataka i obnovu usluga.

3.4. Osigurati da se pogođene strane, kao što su klijenti i regulatorna tijela, obavijeste kada je to propisano zakonom.

3.5. Spriječiti ponavljanje putem analize temeljnog uzroka, korektivnih radnji i poboljšanja politike.

3.6. Omogućiti SME organizacijama ispunjavanje zahtjeva za certifikaciju prema normi ISO 27001 i dokazivanje odgovornosti tijekom revizija.

4. Uloge i odgovornosti

4.1. glavni direktor (GM)

4.1.1. Vlasnik je ove politike i odgovoran je za osiguravanje njezine provedbe.

4.1.2. Nadzire aktivnosti odgovora na incidente i odobrava obavijesti regulatornim tijelima ili klijentima.

4.1.3. Pregledava izvješća nakon incidenta i osigurava ažuriranje politike kada je to potrebno.

4.1.4. Može delegirati koordinacijske dužnosti, ali zadržava odgovornost.

4.2. pružatelj IT podrške / administrator sustava (interni ili vanjski)

4.2.1. Otkriva i istražuje moguće sigurnosne incidente.

4.2.2. Provodi mjere ograničavanja i oporavka, primjerice onemogućavanje pristupa i povrat podataka iz sigurnosnih kopija.

4.2.3. Obavještava GM-a o svim potvrđenim ili sumnjivim incidentima u roku od jednog sata od otkrivanja.

4.2.4. Vodi evidenciju incidenata s vremenskim oznakama, procjenom utjecaja i poduzetim radnjama odgovora.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Zahtjevi za pregled i ažuriranje

9.1. Redoviti pregled

9.1.1. Ovu politiku glavni direktor (GM) mora pregledati najmanje jednom svakih 12 mjeseci kako bi se osiguralo:

9.1.1.1. usklađenost s kontrolama norme ISO/IEC 27001:2022

9.1.1.2. pravodoban odgovor na nove prijetnje, rizike i incidente

9.1.1.3. trajna usklađenost sa zakonskim i ugovornim obvezama, primjerice s GDPR-om i DORA-om

9.2. Događaji koji pokreću pregled

9.2.1. Politika se također mora pregledati i ažurirati nakon:

9.2.1.1. svakog incidenta visoke ozbiljnosti ili regulatorne obavijesti

9.2.1.2. uvođenja nove IT infrastrukture ili promjena sustava

9.2.1.3. izmjena zakonskih zahtjeva koji se odnose na sigurnosne povrede

9.3. Dokumentiranje pregleda i distribucija

9.3.1. Svi pregledi i promjene moraju se dokumentirati u zapisniku promjena politike.

9.3.2. Ažurirane verzije moraju se distribuirati svim zaposlenicima, dobavljačima i pružateljima IT usluga uključenima u sigurnost ili rad sustava.

9.3.3. Dokazi o upoznatosti osoblja, primjerice zapisnici sa sastanaka ili potvrde e-poštom, moraju se čuvati radi spremnosti za reviziju.

10. Povezane politike i poveznice

10.1. Ova politika mora se primjenjivati usklađeno sa sljedećim SME politikama:

10.1.1. P1S – Politika informacijske sigurnosti: utvrđuje opća očekivanja za održavanje povjerljivosti, cjelovitosti i dostupnosti tijekom poslovanja, uključujući postupanje s incidentima.

10.1.2. P2S – Politika uloga i odgovornosti u upravljanju: uspostavlja strukture ovlasti i odgovornosti za otkrivanje, prijavljivanje i eskalaciju incidenata.

10.1.3. P4S – Politika kontrole pristupa: omogućuje trenutačno ukidanje prava pristupa tijekom aktivnosti odgovora na incidente.

10.1.4. P8S – Politika podizanja svijesti i osposobljavanja o informacijskoj sigurnosti: osigurava da svi zaposlenici mogu učinkovito prepoznati i prijaviti sigurnosne incidente.

10.1.5. P17S – Politika zaštite podataka i privatnosti: uređuje zakonske postupke prijave povrede prema GDPR-u i podupire usklađenost s regulatornim zahtjevima tijekom incidenata.

10.1.6. P22S – Politika zapisivanja događaja i praćenja: osigurava potrebne alate i vidljivost za otkrivanje, analizu i reviziju sigurnosnih događaja.

10.1.7. P31S – Politika prikupljanja dokaza i forenzike: podupire istragu i dokazivost radnji povezanih s incidentima pravilnim postupanjem s dokazima.

10.2. Ove politike zajedno uspostavljaju operativni okvir SME organizacije za otkrivanje, odgovor i oporavak od incidenata informacijske sigurnosti.

11. Referentni standardi i okviri

11.1. ISO/IEC 27001

11.1.1. Točka 6.1 – Zahtijeva planiranje obrade rizika, uključujući pripremu za incidente.

11.1.2. Točka 6.3 – Podupire kontinuirano poboljšavanje kroz naučene lekcije iz sigurnosnih događaja.

11.1.3. Točka 8.1 – Naglašava operativne kontrole radi upravljanja incidentima i prekidima.

11.2. ISO/IEC 27002

11.2.1. Kontrola 5.24 – Zahtijeva strukturirani pristup prijavljivanju, procjeni i odgovoru na incidente informacijske sigurnosti.

11.2.2. Kontrola 5.25 – Usmjerena je na učenje iz incidenata radi poboljšanja buduće pripravnosti i otpornosti sustava.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – Definira postupke rješavanja incidenata, uključujući ograničavanje i oporavak.

11.3.2. IR-5 – Uspostavlja zahtjeve za praćenje i analizu incidenata.

11.3.3. IR-6 – Propisuje protokole za vanjsko i unutarnje prijavljivanje incidenata.

11.4. GDPR EU

11.4.1. Članak 33 – Zahtijeva prijavu povreda osobnih podataka regulatornim tijelima u roku od 72 sata, uz pojedinosti o opsegu i mjerama ublažavanja.

11.5. Direktiva EU NIS2 (2022/2555)

11.5.1. Članak 23 – Zahtijeva od ključnih i važnih subjekata prijavu značajnih incidenata nadležnim tijelima uporabom standardiziranih obrazaca za prijavu.

11.6. Uredba EU DORA (2022/2554)

11.6.1. Članak 17 – Zahtijeva da financijski subjekti klasificiraju, prijavljuju i prate incidente i prekide povezane s IKT-om.

11.7. COBIT 2019

11.7.1. DSS02 – Upravljanje zahtjevima za uslugu i incidentima: usmjerava učinkovito postupanje s operativnim i sigurnosnim incidentima u skladu s ciljevima upravljanja.

11.7.2. DSS04 – Upravljanje kontinuitetom: povezuje odgovor na incidente sa širim strategijama kontinuiteta i oporavka.