					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P30					Naslov dokumenta: **Politika odzivanja na incidente**							
Različica: 1.0		Datum začetka veljavnosti: 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	Clause 8.1, Clause 9	Strukturirani procesi za obvladovanje tveganj in odzivanje na incidente
ISO/IEC 27002:2022	Kontrole 5.25–5.27	Vloge, poročanje, odzivanje in izboljševanje pri obravnavi incidentov
NIST SP 800-53 Rev.5	IR-1 do IR-9	Celovit življenjski cikel odzivanja na incidente
Uredba EU GDPR	Člen 33(1), 33(3)(a)–(d), 34(1), 34(2)(a)–(c)	Časovni roki za obveščanje o kršitvah, poročanje in komunikacija s posamezniki, na katere se osebni podatki nanašajo
Direktiva EU NIS2	Člen 23(1)–(4)	Obveščanje pristojnega nacionalnega organa in strukturirano poročanje
Uredba EU DORA	Člen 17(1)–(3)	Poročanje o večjih incidentih, povezanih z IKT, za finančne subjekte
COBIT 2019	DSS02, DSS04, MEA	Določa, spremlja in ocenjuje upravljanje incidentov, neprekinjeno poslovanje in vrednotenje

1. Namen

1.1 Ta politika vzpostavlja formalni okvir za prepoznavanje, prijavo, analizo, zajezitev, odzivanje, obnovitev in pregled po incidentu za incidente informacijske varnosti, ki vplivajo na organizacijo.

1.2 Zagotavlja pravočasen, usklajen in učinkovit odziv za zmanjšanje operativnih motenj, finančnih izgub, škode za ugled in regulatorne neskladnosti.

1.3 Politika podpira tudi stalno izboljševanje odpornosti organizacije na področju kibernetske varnosti z uporabo pridobljenih spoznanj ter vključevanjem ugotovitev po incidentu v upravljanje, orodja in programe usposabljanja.

2. Področje uporabe

2.1 Ta politika velja za:

2.1.1 vse osebje, vključno z zaposlenimi, pogodbenimi izvajalci, svetovalci in ponudniki storitev tretjih oseb,

2.1.2 vse informacijske sisteme, aplikacije, infrastrukturo, omrežja in podatke, ne glede na to, ali se nahajajo v lokalnem okolju, v oblaku ali v hibridnem okolju,

2.1.3 vse vrste varnostnih incidentov, vključno, vendar ne omejeno na:

2.1.3.1 nepooblaščen dostop ali povišanje privilegijev,

2.1.3.2 napade z zlonamerno programsko opremo in izsiljevalsko programsko opremo,

2.1.3.3 napade zavrnitve storitve (DoS/DDoS),

2.1.3.4 izgubo podatkov, uhajanje podatkov ali odtekanje podatkov,

2.1.3.5 notranjo neustrezno uporabo ali kršitve politike,

2.1.3.6 kršitve fizične varnosti, ki vplivajo na digitalna sredstva.

2.2 Politika zajema zaznavanje, triažo, preiskavo, eskalacijo, zajezitev, ravnanje z dokaznim gradivom, obveščanje, obnovitev in analizo temeljnega vzroka.

3. Cilji

3.1 Vzpostaviti ponovljivo in razširljivo zmožnost odzivanja na incidente, ki omogoča hitro zaznavanje, razvrščanje in omejevanje vpliva varnostnih incidentov.

3.2 Zmanjšati vpliv varnostnih dogodkov na poslovanje s strukturiranimi postopki za zajezitev, odstranitev in obnovitev sistemov.

3.3 Zagotoviti, da sta prijava incidentov in odzivanje nanje usklajena s pravnimi, regulativnimi in pogodbenimi zahtevami, zlasti glede rokov za obveščanje o kršitvah in ravnanja z dokaznim gradivom.

3.4 Podpreti preglednost in odgovornost z ustreznim beleženjem, dokumentiranjem in spremljanjem kazalnikov za vse varnostne incidente.

3.5 Spodbujati stalno izboljševanje s pregledi po incidentu, korektivnimi ukrepi in usposabljanjem deležnikov.

4. Vloge in odgovornosti

4.1 Vodja informacijske varnosti (CISO)

4.1.1 Je lastnik okvira odzivanja na incidente, zagotavlja izvajanje politike in nadzira usklajevanje obravnave incidentov na ravni celotne organizacije.

4.1.2 Deluje kot primarna kontaktna točka za regulatorje, izvršno vodstvo in zunanje pravne svetovalce med večjimi incidenti.

4.2 Koordinator odzivanja na incidente

4.2.1 Usklajuje medfunkcijske odzivne ekipe, upravlja poteke dela ter spremlja stanje zajezitve in obnovitve.

4.2.2 Sproži in vodi preglede po incidentu (PIR) ter zagotavlja, da so korektivni ukrepi evidentirani in izvedeni.

[... 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 Ta politika mora biti pregledana najmanj enkrat letno in po potrebi revidirana, da se vključijo:

9.1.1 spremembe v okolju groženj, vrstah incidentov ali vektorjih napadov,

9.1.2 spoznanja iz večjih incidentov, skorajšnjih incidentov ali regulativnih ugotovitev,

9.1.3 posodobitve veljavnih zakonov in predpisov (npr. GDPR, DORA, NIS2),

9.1.4 povratne informacije iz vaj odzivanja na incidente in pregledov po incidentu.

9.2 Vodja informacijske varnosti je odgovoren za začetek in usklajevanje postopka pregleda v posvetovanju z:

9.2.1.1 pravnim svetovalcem in DPO,

9.2.1.2 SOC in operativnimi ekipami IT,

9.2.1.3 ekipami za neprekinjeno poslovanje in upravljanje tveganj,

9.2.1.4 izvršnim vodstvom.

9.3 Spremembe politike morajo biti:

9.3.1 dokumentirane v repozitoriju z upravljanjem različic,

9.3.2 sporočene vsem prizadetim ekipam in vključene v usposabljanja za ozaveščanje,

9.3.3 potrjene z namiznimi ali praktičnimi vajami odzivanja na incidente v treh mesecih po odobritvi.

9.4 Nujne posodobitve, sprožene zaradi nastajajočih groženj, revizijskih ugotovitev ali na novo izdanih pravnih obveznosti, morajo biti uveljavljene takoj in zabeležene v evidenci sprememb politike.

10. Povezane politike in povezave

10.1 To politiko podpirajo in so z njo povezane naslednje organizacijske politike:

10.1.1 P1 – Politika informacijske varnosti: določa krovno zahtevo za delovanje na podlagi tveganj in pripravljenost na incidente.

10.1.2 P5 – Politika upravljanja sprememb: zagotavlja, da dejavnosti zajezitve in obnovitve, ki vključujejo infrastrukturo ali storitve, sledijo formalnim postopkom.

10.1.3 P13 – Politika klasifikacije in označevanja podatkov: podpira razvrščanje resnosti incidentov na podlagi občutljivosti podatkov.

10.1.4 P15 – Politika varnostnega kopiranja in obnove: omogoča obnovitev po napadih z izsiljevalsko programsko opremo ali drugih uničujočih napadih z zagotovljeno celovitostjo.

10.1.5 P18 – Politika kriptografskih kontrol: določa šifrirne ukrepe, ki zmanjšujejo vpliv incidentov in tveganja izpostavljenosti podatkov.

10.1.6 P22 – Politika beleženja in spremljanja: zagotavlja osnovno vidnost dogodkov, opozarjanje in hrambo dnevniških zapisov, potrebne za učinkovito zaznavanje in forenzično preiskavo.

10.1.7 P29 – Politika testnih podatkov in testnega okolja: zagotavlja, da se incidenti, ki vplivajo na neprodukcijske sisteme, obravnavajo strukturirano in varno.

10.1.8 P33 – Politika spremljanja presoje in skladnosti: s strukturiranimi presojami in preverjanji skladnosti potrjuje pripravljenost na incidente in učinkovitost odzivanja.

11. Referenčni standardi in okviri

11.1 ISO/IEC 27001: Klavzula 8.1 – operativno načrtovanje in nadzor: strukturirani procesi za obvladovanje tveganj in načrtovanje odzivanja na incidente.

11.2 ISO/IEC 27002:2022 – Kontrole 5.25–5.27: odgovornosti za upravljanje incidentov, poročanje, odzivanje, komunikacijo in izboljševanje.

11.3 NIST SP 800-53 Rev.5: IR-1 do IR-9, AU-6, PL-2: celovite zahteve za življenjski cikel odzivanja na incidente, revizijo in varnostno načrtovanje.

11.4 Uredba EU GDPR: Člen 33/34: obveznosti poročanja nadzornim organom in zahteve glede obveščanja posameznikov, na katere se osebni podatki nanašajo (z določenimi izjemami).

11.5 Direktiva EU NIS2 (2022/2555): Člen 23: obvezno nacionalno poročanje z vmesnimi in končnimi obveznostmi poročanja.

11.6 Uredba EU DORA (2022/2554): Člen 17: zahteve za poročanje finančnih institucij pristojnim organom o incidentih IKT.

11.7 COBIT 2019: DSS02, DSS04, MEA01: upravljanje storitvenih incidentov in neprekinjenega poslovanja ter spremljanje uspešnosti in skladnosti.