					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P30S					Dokumenta nosaukums: **Incidentu reaģēšanas politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Saskaņotība ar piemērojamajiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	6.1., 6.3., 8. punkts	incidentu pārvaldība, nepārtraukta pilnveide, darbību plānošana un kontrole
ISO/IEC 27002:2022	5.24., 5.25. kontrole	incidentu atklāšana, gatavība, mācīšanās
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	incidentu apstrāde un uzraudzība, ziņošana
ES GDPR	33. pants	paziņošanas prasības personas datu aizsardzības pārkāpuma gadījumā
ES NIS2	23. pants	obligāta ziņošana par kiberdrošības incidentiem
ES DORA	17. pants	IKT incidentu pārvaldība
COBIT 2019	DSS02, DSS04	pakalpojumu un incidentu pārvaldība un darbības nepārtrauktība

1. Mērķis

1.1. Šī politika nosaka, kā organizācija atklāj informācijas drošības incidentus, ziņo par tiem un reaģē uz tiem, ja tie ietekmē tās digitālās sistēmas, datus vai pakalpojumus.

1.2. Tā nodrošina organizācijai iespēju mazināt kaitējumu, aizsargāt klientu datus un izpildīt normatīvās prasības, piemēram, GDPR noteikto 72 stundu prasību paziņošanai par personas datu aizsardzības pārkāpumu.

1.3. Politika nosaka skaidru atbildības sadalījumu, komunikācijas soļus un pēcincidenta darbības arī mazās organizācijās bez atsevišķi izveidotas drošības komandas.

2. Piemērošanas joma

2.1. Šī politika attiecas uz:

2.1.1. visiem darbiniekiem, līgumslēdzējiem un ārējiem IT pakalpojumu sniedzējiem;

2.1.2. visām uzņēmuma pārvaldītajām sistēmām un pakalpojumiem, tostarp tīmekļvietnēm, mākoņplatformām, mobilajām ierīcēm, klēpjdatoriem un e-pasta kontiem;

2.1.3. visu veidu incidentiem, tostarp:

2.1.3.1. nesankcionētu piekļuvi datiem vai sistēmām;

2.1.3.2. inficēšanos ar ļaunatūru vai izspiedējprogrammatūru;

2.1.3.3. pikšķerēšanas vai sociālās inženierijas mēģinājumiem;

2.1.3.4. sistēmu nepieejamību kiberuzbrukuma vai nepareizas lietošanas dēļ;

2.1.3.5. sensitīvas informācijas nejaušu izpaušanu vai dzēšanu;

2.1.3.6. uzņēmuma ierīču vai datu nesēju nozaudēšanu vai zādzību.

3. Mērķi

3.1. Noteikt skaidru procesu drošības incidentu identificēšanai un eskalācijai.

3.2. Nodrošināt, ka par incidentiem tiek ziņots, tie tiek reģistrēti un apstrādāti iepriekš noteiktajos termiņos.

3.3. Nodrošināt ātru ietekmes ierobežošanu, datu atjaunošanu un pakalpojumu darbības atjaunošanu.

3.4. Nodrošināt, ka skartās puses (piemēram, klienti un uzraudzības iestādes) tiek informētas, ja to pieprasa tiesību akti.

3.5. Novērst atkārtošanos, veicot pamatcēloņa analīzi, korektīvās darbības un pilnveidojot politiku.

3.6. Nodrošināt, ka SME spēj izpildīt ISO 27001 sertifikācijas prasības un audita laikā pierādīt pārskatatbildību.

4. Lomas un pienākumi

4.1. Ģenerāldirektors (GM)

4.1.1. ir šīs politikas īpašnieks un nodrošina tās ieviešanu;

4.1.2. pārrauga incidentu reaģēšanas darbības un apstiprina paziņojumus uzraudzības iestādēm vai klientiem;

4.1.3. pārskata pēcincidenta ziņojumus un nodrošina politikas atjaunināšanu, ja tas ir nepieciešams;

4.1.4. var deleģēt koordinēšanas pienākumus, saglabājot pārskatatbildību.

4.2. Ārējs IT pakalpojumu sniedzējs / sistēmu administrators (iekšējs vai ārējs)

4.2.1. atklāj un izmeklē iespējamos drošības incidentus;

4.2.2. īsteno ierobežošanas un atjaunošanas darbības (piemēram, atspējo piekļuvi, atjauno rezerves kopijas);

4.2.3. paziņo GM par visiem apstiprinātajiem vai iespējamiem incidentiem 1 stundas laikā pēc to atklāšanas;

4.2.4. uztur incidentu žurnālu ar laikspiedoliem, ietekmes novērtējumu un reaģēšanas darbībām.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1. Plānotā pārskatīšana

9.1.1. Šī politika Ģenerāldirektoram (GM) jāpārskata vismaz reizi 12 mēnešos, lai nodrošinātu:

9.1.1.1. atbilstību ISO/IEC 27001:2022 kontroles pasākumiem;

9.1.1.2. spēju reaģēt uz jauniem apdraudējumiem, riskiem un incidentiem;

9.1.1.3. nepārtrauktu atbilstību tiesiskajiem un līgumiskajiem pienākumiem (piemēram, GDPR, DORA).

9.2. Pārskatīšanas ierosinātāji

9.2.1. Politika jāpārskata un jāatjaunina arī pēc:

9.2.1.1. jebkura augstas smaguma pakāpes incidenta vai paziņošanas uzraudzības iestādei;

9.2.1.2. jaunas IT infrastruktūras ieviešanas vai sistēmu izmaiņām;

9.2.1.3. grozījumiem tiesību aktos, kas attiecas uz drošības pārkāpumiem.

9.3. Pārskatīšanas dokumentēšana un izplatīšana

9.3.1. Visas pārskatīšanas un izmaiņas jādokumentē politikas izmaiņu žurnālā.

9.3.2. Atjauninātās versijas jāizplata visiem darbiniekiem, piegādātājiem un IT pakalpojumu sniedzējiem, kas iesaistīti drošībā vai sistēmu darbībā.

9.3.3. Personāla informētības pierādījumi (piemēram, sanāksmju piezīmes vai e-pasta apstiprinājumi) jāsaglabā, lai nodrošinātu gatavību auditam.

10. Saistītās politikas un sasaiste

10.1. Šī politika jāpiemēro kopā ar šādām SME politikām:

10.1.1. P1S – Informācijas drošības politika: nosaka vispārējās prasības konfidencialitātes, integritātes un pieejamības uzturēšanai darbības laikā, tostarp incidentu apstrādē.

10.1.2. P2S – Pārvaldības lomu un atbildības politika: nosaka pilnvaru un pārskatatbildības struktūru incidentu atklāšanai, ziņošanai un eskalācijai.

10.1.3. P4S – Piekļuves kontroles politika: nodrošina tūlītēju piekļuves tiesību atsaukšanu incidentu reaģēšanas laikā.

10.1.4. P8S – Informācijas drošības informētības un apmācību politika: nodrošina, ka visi darbinieki spēj efektīvi identificēt drošības incidentus un ziņot par tiem.

10.1.5. P17S – Datu aizsardzības un privātuma politika: nosaka tiesiskās paziņošanas procedūras pārkāpumu gadījumā saskaņā ar GDPR un atbalsta regulatīvo atbilstību incidentu laikā.

10.1.6. P22S – Žurnālfiksēšanas un uzraudzības politika: nodrošina nepieciešamos rīkus un pārskatāmību drošības notikumu atklāšanai, analīzei un auditēšanai.

10.1.7. P31S – Pierādījumu iegūšanas un datorforensikas politika: atbalsta ar incidentiem saistīto darbību izmeklēšanu un juridisko pamatojumu, nosakot pareizu rīcību ar pierādījumiem.

10.2. Šīs politikas kopā veido SME darbības ietvaru informācijas drošības incidentu atklāšanai, reaģēšanai uz tiem un atjaunošanai pēc tiem.

11. Atsauces standarti un ietvari

11.1. ISO/IEC 27001

11.1.1. 6.1. punkts – nosaka riska apstrādes plānošanu, tostarp gatavību incidentiem.

11.1.2. 6.3. punkts – atbalsta nepārtrauktu pilnveidi, izmantojot no drošības notikumiem gūtās atziņas.

11.1.3. 8.1. punkts – uzsver darbības kontroles pasākumu nozīmi incidentu un traucējumu pārvaldībā.

11.2. ISO/IEC 27002

11.2.1. 5.24. kontrole – nosaka strukturētu pieeju ziņošanai par informācijas drošības incidentiem, to izvērtēšanai un reaģēšanai uz tiem.

11.2.2. 5.25. kontrole – vērsta uz mācīšanos no incidentiem, lai uzlabotu turpmāko gatavību un sistēmu noturību.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – definē incidentu apstrādes procedūras, tostarp ierobežošanu un atjaunošanu.

11.3.2. IR-5 – nosaka prasības incidentu uzraudzībai un analīzei.

11.3.3. IR-6 – nosaka obligātus ārējās un iekšējās ziņošanas par incidentiem protokolus.

11.4. ES GDPR

11.4.1. 33. pants – nosaka pienākumu 72 stundu laikā ziņot uzraudzības iestādēm par personas datu aizsardzības pārkāpumiem, norādot apjomu un mazināšanas pasākumus.

11.5. ES NIS2 direktīva (2022/2555)

11.5.1. 23. pants – nosaka būtisku un svarīgu subjektu pienākumu ziņot kompetentajām iestādēm par būtiskiem incidentiem, izmantojot standartizētus ziņošanas formātus.

11.6. ES DORA regula (2022/2554)

11.6.1. 17. pants – nosaka pienākumu finanšu iestādēm klasificēt, ziņot un izsekot ar IKT saistītus incidentus un traucējumus.

11.7. COBIT 2019

11.7.1. DSS02 – Pakalpojumu pieprasījumu un incidentu pārvaldība: sniedz vadlīnijas efektīvai darbības un drošības incidentu apstrādei atbilstoši pārvaldības mērķiem.

11.7.2. DSS04 – Nepārtrauktības pārvaldība: sasaista incidentu reaģēšanu ar plašākām nepārtrauktības un atjaunošanas stratēģijām.