					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P13S					Dokumenta nosaukums: **Datu klasificēšanas un marķēšanas 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	Punkti 5.3, 8	
ISO/IEC 27002:2022	Kontroles pasākumi 5.12, 5	
NIST SP 800-53 Rev.5	AC-16, MP-3, MP-5	
ES NIS2	Pants 21(2)(a)	
ES DORA	Pants 5(8)	
COBIT 2019	BAI03.05, DSS05	
ES VDAR	Panti 5, 32	

1. Mērķis

1.1 Šī politika nosaka, kā organizācijā apstrādājamā informācija ir jāklasificē un jāmarķē, lai visā tās dzīves ciklā saglabātu tās konfidencialitāti, integritāti un pieejamību.

1.2 Tā nodrošina konsekventu datu apstrādes praksi, piešķirot informācijai atbilstošus aizsardzības līmeņus atkarībā no tās sensitivitātes, ietekmes uz uzņēmējdarbību vai normatīvajiem pienākumiem.

1.3 Klasificēšana un marķēšana palīdz mazināt sensitīvu datu nejaušas izpaušanas, neatļautas piekļuves vai neatbilstošas apstrādes risku, jo īpaši MVU vidē, kur var tikt izmantotas vienkāršākas sistēmas un mazāk formalizēti kontroles pasākumi.

1.4 Šī politika ir būtiska ISO/IEC 27001 sertifikācijai un normatīvo prasību izpildei, jo īpaši attiecībā uz datu aizsardzības tiesību aktiem, piemēram, VDAR, un kiberdrošības ietvariem, piemēram, NIS2 un DORA.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visiem organizācijas datiem neatkarīgi no to formāta vai atrašanās vietas, tostarp:

2.1.1 elektroniskiem dokumentiem, izklājlapām, e-pasta ziņojumiem, veidlapām, attēliem un skenētiem failiem;

2.1.2 fiziskiem dokumentiem, piemēram, drukātiem ierakstiem, pārskatiem, rēķiniem un piezīmēm;

2.1.3 datiem, kas tiek glabāti vai apstrādāti mākoņpakalpojumos, lokālajos serveros, noņemamos datu nesējos vai uzņēmējdarbības vajadzībām izmantotās personīgajās ierīcēs;

2.1.4 pagaidu vai pārejošiem datiem, kas rodas uzņēmējdarbības procesu laikā (piemēram, žurnāli, kešatmiņas faili, e-pasta ziņojumi).

2.2 Visiem darbiniekiem, darbuzņēmējiem, pagaidu darbiniekiem un ārējiem pakalpojumu sniedzējiem, kuriem ir piekļuve organizācijas datiem, ir jāievēro šī politika.

2.3 Tā attiecas uz visu datu dzīves ciklu — no izveides un glabāšanas līdz piekļuvei, pārsūtīšanai, arhivēšanai vai dzēšanai.

3. Mērķi

3.1 Noteikt vienkāršu un ieviešamu klasificēšanas shēmu, kuru var viegli saprast un piemērot visā organizācijā.

3.2 Noteikt prasību katram datu aktīvam piešķirt klasifikāciju atbilstoši tā sensitivitātei un to attiecīgi marķēt, lai nodrošinātu pareizu apstrādi, glabāšanu un piekļuvi.

3.3 Nodrošināt, ka datu marķēšanas prakse ir integrēta uzņēmējdarbības procesos, piemēram, personāla pieņemšanā, projektu uzsākšanā un sistēmu ieviešanā.

3.4 Samazināt datu aizsardzības pārkāpumu risku, piemērojot apstrādes kontroles pasākumus (piemēram, šifrēšanu, piekļuves ierobežošanu) atbilstoši klasifikācijas līmenim.

3.5 Nodrošināt atbilstību privātuma un informācijas drošības prasībām, pierādot, ka sensitīvi dati (piemēram, personas, finanšu vai īpašumtiesību dati) ir pienācīgi marķēti un pārvaldīti.

3.6 Noteikt pārskatatbildību par klasificēšanas lēmumiem un nodrošināt periodisku pārskatīšanu un atjaunināšanu atbilstoši mainīgajām uzņēmējdarbības un tiesiskajām vajadzībām.

4. Lomas un pienākumi

4.1 Ģenerāldirektors

4.1.1 Ir šīs politikas īpašnieks un apstiprina klasificēšanas shēmu.

4.1.2 Nodrošina pārraudzību, lai klasificēšanas pienākumi būtu deleģēti un ieviesti.

4.1.3 Pārskata un apstiprina visus izņēmumus no klasificēšanas vai marķēšanas prasībām.

4.1.4 Nodrošina, ka datu apstrādes prakse atbilst tādu tiesību aktu prasībām kā VDAR un DORA.

4.2 Informācijas īpašnieks / datu pārzinis

4.2.1 Katram jaunam datu kopumam vai informācijas aktīvam piešķir sākotnējo klasifikāciju tā izveides vai iegādes brīdī.

4.2.2 Nodrošina, ka, kur piemērojams, tiek izmantoti redzami marķējumi (piemēram, failu galvenes, kājenes, ūdenszīmes, mapju nosaukumi).

4.2.3 Periodiski pārskata klasifikāciju, lai pārliecinātos par tās atbilstību, precizitāti un nepieciešamajām izmaiņām (piemēram, pēc deklasificēšanas vai publicēšanas).

4.2.4 Sadarbojas ar IT vadītāju, lai ieviestu tehniskos aizsardzības pasākumus atbilstoši klasifikācijai (piemēram, piekļuves tiesības, šifrēšana).

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Ģenerāldirektoram un datu pārzinim šī politika jāpārskata reizi gadā, lai nodrošinātu, ka tā atspoguļo:

9.1.1 izmaiņas uzņēmējdarbībā vai datu tipos;

9.1.2 jaunas regulatīvās prasības (piemēram, datu privātuma vai finanšu uzraudzības jomā);

9.1.3 tehnoloģiju izmaiņas, kas ietekmē marķēšanas vai klasificēšanas iespējas.

9.2 Pārskatīšanā jāiekļauj klasifikācijas kategoriju, marķēšanas rīku vai prakses un informētības/apmācību satura atjaunināšana.

9.3 Politikas grozījumi jāapstiprina ģenerāldirektoram un jāpaziņo visiem darbiniekiem. Ieraksts par versiju izmaiņām jāsaglabā audita vajadzībām.

10. Saistītās politikas un sasaiste

10.1 P2S – Pārvaldības lomu un atbildības politika: nosaka pārskatatbildību par politikas īpašumtiesībām un ieviešanu.

10.2 P4S – Piekļuves kontroles politika: saskaņo sistēmu piekļuvi ar datu klasifikācijas līmeņiem.

10.3 P12S – Aktīvu pārvaldības politika: uzskaita fiziskos un digitālos aktīvus, kuros tiek glabāti klasificēti dati.

10.4 P17S – Datu aizsardzības un privātuma politika: nosaka personas datu aizsardzību, no kuriem liela daļa ir klasificēta kā Konfidenciāla.

10.5 P30S – Incidentu reaģēšanas politika: nosaka eskalācijas ceļus un reaģēšanas procedūras klasifikācijas pārkāpumu vai datu izpaušanas gadījumā.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 Punkts 5.3: nosaka prasību skaidri definēt pienākumus datu apstrādei un aizsardzībai.

11.1.2 Punkts 8.1: nosaka darbības plānošanu un kontroles pasākumus, tostarp tos, kas saistīti ar datu klasificēšanu.

11.2 ISO/IEC 27002

11.2.1 5.12. kontrole: sniedz vadlīnijas informācijas klasificēšanai, pamatojoties uz risku un regulatīvajām prasībām.

11.2.2 5.13. kontrole: nosaka praktiskos marķēšanas mehānismus un saistītos apstrādes noteikumus.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-16: nosaka prasību marķēt informāciju, lai aizsardzības pasākumi atbilstu klasifikācijai.

11.3.2 MP-3 / MP-5: sniedz vadlīnijas datu nesēju un izvades marķēšanai un kontrolei.

11.4 ES VDAR

11.4.1 Panti 5 un 32: nosaka datu minimizēšanu un integritāti, piemērojot atbilstošus klasificēšanas un apstrādes drošības pasākumus.

11.5 ES NIS2

11.5.1 Pants 21(2)(a): nosaka tehnoloģiskos kontrolpasākumus un organizatoriskās kontroles uz risku balstītai datu aizsardzībai.

11.6 ES DORA

11.6.1 Pants 5(8): nosaka prasību uzņēmumiem klasificēt datu aktīvus kā daļu no to IKT risku pārvaldības programmas.

11.7 COBIT 2019

11.7.1 BAI03.05: nosaka informācijas klasificēšanu un riskam pielāgotu aizsardzību.

11.7.2 DSS05.02: attiecas uz klasifikācijā balstītu kontroles pasākumu piemērošanu un uzraudzību.