

Konfidenciāls

Trūkumu analīze un rīcības plāns

SIA Paraugs

31.10.2026. · v1.0

Trūkumu analīze un rīcības plāns

Dokumenta vadība

Lauks	Vērtība
Dokumenta īpašnieks	Valdes norīkota persona / IT pakalpojumu sniedzējs
Versija	v1.0
Sagatavots	31.10.2026
Valde apstiprinājusi	—
Nākamā pārskatīšana	31.10.2027
Klase	Konfidenciāls
Izplatīšana	Valde un par informācijas drošību atbildīgā persona

Versiju vēsture

Versija	Datums	Izmaiņas	Sagatavoja	Apstiprināja
v1.0	31.10.2026	Pirmā versija	—	—
—	—	—	—	—
—	—	—	—	—

Uzņēmums: SIA Paraugs

Reģistrācijas numurs: 40000000000

Adrese: Rīga, Paraugu iela 1, LV-1001

Valsts: Latvija

Standarts: ES NIS2 direktīva un Latvijas Nacionālais kiberdrošības likums

1. Kopsavilkums

- 1.1. Gatavības novērtējums ir 22 no 100. Tas salīdzina anketā norādīto pašreizējo praksi ar informācijas drošības politikas prasībām atbilstoši mērķa standartam (ES NIS2 direktīva un Latvijas Nacionālais kiberdrošības likums).
- 1.2. Konstatēti 13 trūkumi: 2 augstas, 7 vidējas un 4 zemas prioritātes. Augstas prioritātes trūkumu novērš 30 dienu laikā, vidējas — 90 dienu laikā, zemas — 180 dienu laikā.
- 1.3. Novērtējums nav audita rezultāts un neapliecina atbilstību. Tas parāda, kur politika prasa vairāk, nekā sabiedrība dara pašlaik.

2. NIS2 piemērojamība

- 2.1. Visticamāk ārpus NIS2 tiešā tvēruma. Nozare nav NIS2 pielikumos. Politika tomēr noder klientu, iepirkumu un VDAR prasībām, un NIS2 pasākumi ir laba prakse.
- 2.2. Šis ir sākotnējs novērtējums pēc nozares, darbinieku skaita un apgrozījuma. Galīgais statuss ir atkarīgs no faktiski sniegtajiem pakalpojumiem un kompetentās iestādes vērtējuma.

3. Pašreizējais stāvoklis un politikas prasība

Joma	Pašreizējais stāvoklis	Politikas prasība	Statuss
Daudzfaktoru autentifikācija	tikai svarīgākajiem kontiem, īsziņa	Visiem kontiem, autentifikācijas lietotne	Trūkums
Paroļu pārvaldnieks	nē	Apstiprināts paroļu pārvaldnieks	Trūkums
Rezerves kopijas	reizi nedēļā	reizi dienā	Trūkums
Nošķirta kopija	nē	Vismaz viena bezsaistes vai nemainīga kopija	Trūkums
Atjaunošanas tests	netiek veiktas	reizi ceturksnī	Trūkums
Piekļuves tiesību pārskats	netiek pārskatītas	reizi ceturksnī	Trūkums
Iekārtu šifrēšana	daļa iekārtu ir šifrēta	Visas portatīvās iekārtas šifrētas	Trūkums
Drošības atjauninājumi	manuāli, bez noteikta termiņa	Automātiski; kritiskie 14 dienu laikā	Trūkums
Žurnālēšana	žurnāli netiek pārskatīti	Glabā 12 mēnešus, brīdinājumi ieslēgti	Trūkums
Piegādātāji	drošības prasības ir dažos līgumos	Drošības noteikumi katrā kritiskajā līgumā	Trūkums

Apmācības	tikai ievadapmācība	Ievadapmācība un ikgadēja apmācība	Trūkums
Incidentu plāns	nē	Apstiprināts plāns un kontakti	Trūkums
Iekārtas	tikai uzņēmuma iekārtas	Uzņēmuma iekārtas vai kontrolētas personīgās iekārtas	Atbilst

4. Rīcības plāns

4.1. Valde šo plānu apstiprina kopā ar politiku. Atbildīgā persona drīkst mainīt pasākumu secību, bet termiņus groza tikai ar valdes lēmumu.

Nr.	Trūkums un pasākums	Prioritāte	Termiņš	Atbildīgais	Politika	Izpildīts
1	Rezerves kopijas nav nošķirtas no pamatsistēmas (bezsaistē vai nemainīgā krātuvē). Ieviest vismaz vienu nošķirtu kopiju (3-2-1 princips), ko nevar izdzēst vai šifrēt ar ikdienas piekļuves datiem.	Augsta	30.11.2026	Valdes norīkota persona / IT pakalpojumu sniedzējs	11. sadaļa	___
2	Atjaunošana no rezerves kopijas nekad nav pārbaudīta. Veikt pirmo atjaunošanas testu un rezultātu ierakstīt atjaunošanas testa protokolā.	Augsta	30.11.2026	Valdes norīkota persona / IT pakalpojumu sniedzējs	10. un 11. sadaļa	___
3	Daudzfaktoru autentifikācija ir tikai svarīgākajiem kontiem. Paplašināt daudzfaktoru autentifikāciju uz visiem lietotāju un pakalpojumu kontiem; izņēmumus fiksēt valdes lēmumā.	Vidēja	29.01.2027	Valdes norīkota persona / IT pakalpojumu sniedzējs	4. sadaļa	___
4	Rezerves kopijas veido retāk, nekā prasa izvēlētais standarts. Palielināt rezerves kopiju biežumu līdz politikā noteiktajam intervālam.	Vidēja	29.01.2027	Valdes norīkota persona / IT pakalpojumu sniedzējs	10. sadaļa	___

5	Piekļuves tiesības netiek pārskatītas. Veikt pirmo piekļuves tiesību pārskatu un atcelt liekās tiesības; turpmāk to darīt politikā noteiktajā biežumā.	Vidēja	29.01.2027	Valdes norīkota persona / IT pakalpojumu sniedzējs	4. sadaļa	___
6	Šifrēta ir tikai daļa iekārtu. Ieslēgt pilna diska šifrēšanu atlikušajām iekārtām un to fiksēt aktīvu reģistrā.	Vidēja	29.01.2027	Valdes norīkota persona / IT pakalpojumu sniedzējs	8. sadaļa	___
7	Atjauninājumus uzstāda manuāli bez noteikta termiņa. Ieslēgt automātiskos atjauninājumus, kur tas ir pieejams, un noteikt uzstādīšanas termiņus.	Vidēja	29.01.2027	Valdes norīkota persona / IT pakalpojumu sniedzējs	9. sadaļa	___
8	Drošības žurnāli netiek glabāti un pārskatīti. Ieslēgt audita žurnālus mākoņpakalpojumos un serveros, noteikt glabāšanas termiņu un brīdinājumus par aizdomīgu pieteikšanos.	Vidēja	29.01.2027	Valdes norīkota persona / IT pakalpojumu sniedzējs	9. sadaļa	___
9	Nav noteikts kiberincidentu reaģēšanas un ziņošanas plāns. Apstiprināt darbības nepārtrauktības plānu, iepazīstināt krīzes komandu un aizpildīt ārkārtas kontaktus.	Vidēja	29.01.2027	Valdes norīkota persona / IT pakalpojumu sniedzējs	11. un 14. sadaļa	___
10	Otrais faktors ir īsziņa vai e-pasts, kas ir vieglāk pārtverams. Pāriet uz autentifikācijas lietotni vai drošības atslēgu visiem kontiem.	Zema	29.04.2027	Valdes norīkota persona / IT pakalpojumu sniedzējs	4. sadaļa	___
11	Paroļu pārvaldnieks netiek izmantots. Ieviest valdes apstiprinātu paroļu pārvaldnieku un kopīgās piekļuves datus pārvietot uz to.	Zema	29.04.2027	Valdes norīkota persona / IT pakalpojumu sniedzējs	4. un 8. sadaļa	___
12	Drošības prasības ir tikai dažos piegādātāju līgumos. Papildināt atlikušos kritisko piegādātāju līgumus ar drošības prasībām.	Zema	29.04.2027	Valdes norīkota persona / IT pakalpojumu sniedzējs	12. sadaļa	___

13	Notiek tikai ievadapmācība. Ieviest ikgadēju atkārtotu apmācību, tostarp par pikšķerēšanu.	Zema	29.04.2027	Valdes norīkota persona / IT pakalpojumu sniedzējs	13. sadaļa	_____
----	--	------	------------	--	------------	-------

5. Uzraudzība

5.1. Valde plāna izpildi pārbauda vismaz reizi ceturksnī un rezultātu fiksē.

5.2. Termiņa pagarinājumu fiksē rakstveidā, norādot iemeslu un pagaidu pasākumu.

5.3. Kad visi pasākumi izpildīti, atbildīgā persona novērtējumu atkārtoti un atjauno riska reģistru.