Informācija no Satiksmes ministrijas

2021. gada 13. decembra iekšējiem noteikumiem Nr. 01-02/37

“Starptautiskās kravu loģistikas un ostu informācijas sistēmas drošības politika”

**Starptautiskās kravu loģistikas un ostu informācijas sistēmas (turpmāk – SKLOIS vai Sistēma) drošības politika**

**I SKLOIS drošības principi**

1. SKLOIS tiek ievēroti šādi drošības principi:

1.1. SKLOIS lietotājiem piekļuves tiesības piešķir atbilstoši SKLOIS lietotāju lomām un tiesību apjomiem, kas noteikti normatīvajos aktos.

1.2. SKLOIS lietotāji, kuriem ir reģistrēta piekļuve SKLOIS tiešo darba pienākumu veikšanai vai līgumsaistību izpildei, ievēro ar SKLOIS darbību saistītos iekšējos un ārējos normatīvos aktus un nekavējoties ziņo VSIA “Latvijas Jūras administrācija” par identificētajiem drošības incidentiem, kā arī sniedz visu nepieciešamo atbalstu to izmeklēšanā.

1.3. Pienākumu ievērot ar SKLOIS drošību saistītās prasības ietver SKLOIS lietošanas līgumos un SKLOIS lietošanas noteikumos.

1.4. Ja tehnisko resursu uzturēšana uz līguma pamata tiek nodota ārpakalpojuma sniedzēja datu centram, ārpakalpojuma sniedzējs nekļūst par turētāju. VSIA “Latvijas Jūras administrācija” regulāri seko līdzi un pārliecinās, ka ārpakalpojuma sniedzējs pilda SKLOIS noteiktās pieejamības un drošības prasības, kas noteiktas līgumā ar ārpakalpojuma sniedzēju.

1.5. SKLOIS lietotāju konti:

1.5.1. lietotāji, kas veic SKLOIS administrēšanas darbu, izmanto tam īpašus lietotāju kontus (turpmāk – Sistēmas administratora konts), kas netiek izmantoti ikdienas darbību veikšanai;

1.5.2. katrs lietotāja konts ir saistīts ar konkrētu fizisko personu;

1.5.3. ar Sistēmas administratora kontu piekļūt Sistēmai iespējams tikai ar daudzfaktoru autentifikāciju vai izmantojot iekārtas, kas atrodas VSIA “Latvijas Jūras administrācija” kontrolētās telpās;

1.5.4. ja Sistēmā tiek izmantoti konti, kas nav piesaistāmi konkrētai fiziskai personai, (turpmāk – sistēmkonts), tad Sistēmā jābūt iestrādātiem kontroles mehānismiem, kas novērš iespēju reģistrētiem lietotājiem izmantot sistēmkontu;

1.5.5. SKLOIS lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju, lai sistēmas lietotājs pašrocīgi vai ar sistēmas atbalsta personāla palīdzību atrisinātu kļūdu.

1.6. SKLOIS lietotāju paroles:

1.6.1. Sistēmas piekļuve katram lietotājam ir aizsargāta ar divpakāpju autentifikāciju: lietotāja vārds un parole fiksētai un reģistrētai lietotāja IP adresei, un lietotāja vārds, parole un kodu karte brīvi izvēlētai IP adresei;

1.6.2. Sistēmas lietotāju paroļu garums nav mazāks par 9 (deviņiem) simboliem un satur vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un citu simbolu;

1.6.3. katram Sistēmas lietotājam parole ir obligāti jāmaina pēc ne vairāk kā 90 (deviņdesmit) dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā;

1.6.4. Sistēmas lietotāja parole jāizvēlas tā, lai tā nesakristu ne ar vienu no piecām iepriekšējām šī lietotāja parolēm;

1.6.5. 5 (piecas) secīgas reizes nepareizi ievadot Sistēmas lietotāja konta paroli, šis konts (izņemot Sistēmas administratora kontu) nekavējoties tiek bloķēts;

1.6.6. Sistēmas lietotāja paroles aizliegts glabāt un transportēt nešifrētā veidā, t.sk. lietotāja autentifikācijas procesa ietvaros;

1.6.7. Sistēmas lietotāja parole ievadīšanas brīdī netiek pilnībā attēlota lietotājam;

1.6.8. Sistēmas lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir vienreiz lietojama un derīga ne ilgāk kā 72 stundas pēc tās nosūtīšanas;

1.6.9. Sistēmā nav funkcionalitātes, kas atļauj Sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;

1.6.10. iekārtām, t.sk. infrastruktūras iekārtām, kas nodrošina sistēmas funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītas) paroles.

1.7. Izsekojamība:

1.7.1. tiek nodrošināta Sistēmas (gan servisa, gan operētājsistēmas) auditācijas pierakstu veidošana (ietverot sistēmas auditācijas datus – autentifikācijas datus un tīkla plūsmas auditācijas datus, domēna vārdu sistēmas (DNS) servera pierakstus, ielaušanās atklāšanas sistēmu (IDS) pierakstus, operētājsistēmas autentifikācijas pierakstus) un to uzglabāšana pastāvīgi;

1.7.2. Sistēmas auditācijas pierakstu kopijas uzglabā atsevišķi no Sistēmas. Sistēmas auditācijas pierakstos ietver informāciju par pieslēgšanos vai atslēgšanos no sistēmas, datu atlasi, kā arī konta izveidi, grozīšanu vai dzēšanu. Auditācijas pierakstos fiksē aprakstu, kā arī informāciju par darbības iniciatoru – identifikatoru, pieslēguma metadatus;

1.7.3. jebkura piekļuve Sistēmai ir izsekojama līdz konkrētam Sistēmas lietotāja kontam vai interneta protokola (IP) adresei;

1.7.4. auditācijas pieraksti tiek veikti, norādot pareizu (sinhronizētu) pulksteņa laiku – ierakstā norādītais laiks sakrīt ar faktiskā notikuma pašreizējo vietējo laiku GMT+2;

1.7.5. Sistēmas auditācijas pierakstiem tiek veikta satura plānveida uzraudzība un analīze, lai konstatētu drošības incidentus.

1.8. Atjauninājumi:

1.8.1. VSIA “Latvijas Jūras administrācija” sadarbībā ar Drošības pārvaldnieku veic pieejamo programmatūras atjauninājumu izvērtēšanu un nepieciešamības gadījumā – testēšanu;

1.8.2. Sistēmai nodrošina visus pieejamos un nepieciešamos programmatūras atjauninājumus.

1.9. Sistēmas aizsardzības pasākumi:

1.9.1. Sistēmas funkcionalitāte ir izpildāma ar minimāli iespējamo tiesību kopu;

1.9.2. VSIA “Latvijas Jūras administrācija” nodrošina SKLOIS esošo datu rezerves kopiju veidošanu un atjaunošanu;

1.9.3. visās Satiksmes ministrijas un VSIA “Latvijas Jūras administrācija” valdījumā esošajās galalietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos Sistēmai, jābūt iekļautai pretvīrusu funkcionalitātei;

1.9.4. fiziski piekļūt Sistēmas tehniskiem resursiem atļauts vienīgi VSIA “Latvijas Jūras administrācija” un Satiksmes ministrijas atbildīgajiem darbiniekiem vai citām līgumos noteiktām pilnvarotām personām;

1.9.5. plūsma starp Sistēmu un tās lietotājiem, kā arī starp Sistēmu un citām sistēmām tiek kontrolēta, izmantojot ugunsmūra risinājumu;

1.9.6. veicot Sistēmas izstrādi vai izmaiņas, kā arī testēšanu, nav pieļaujams radīt apdraudējumu Sistēmā glabāto datu integritātei, tādēļ šādiem nolūkiem tiek izmantota Sistēmas testa vide;

1.9.7. Sistēmā ir atslēdzami tie pakalpojumi *(Network Services)*, kuri netiek izmantoti Sistēmas darbības nodrošināšanai;

1.9.8. Sistēmu izmitina ārpakalpojumu sniedzēja nodrošinātos resursos Eiropas Savienības vai Eiropas Ekonomikas zonas valstu teritorijā un Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī reģistrēta ārpakalpojumu sniedzēja datu centrā.

**II SKLOIS drošības risku (pieejamības, integritātes un konfidencialitātes risku) pieņemamais līmenis**

2. Sistēmas darbības atjaunošanu pēc drošības incidenta veic saskaņā ar Sistēmas darbības atjaunošanas plānu.

3. Uz Sistēmu ir attiecināmi šādi drošības pieņemamie riski:

3.1. pakalpojuma neplānots pārtraukums Sistēmas paredzētajā darba laikā var būt ne lielāks par četrām stundām mēnesī (summāri);

3.2. atsevišķu Sistēmā glabāto datu integritātes apdraudējums, kas ir radījis risku valsts un pašvaldību institūcijas pamatfunkciju nodrošināšanai, bet nerada sekas Sistēmas lietotāju darbībai;

3.3. Sistēmā apstrādāto fiziskas personas datu vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūde rada kaitējumu valsts un pašvaldību institūcijas, citu institūciju vai Latvijas Republikas reputācijai, bet nerada smagākas sekas.

4. Sistēmas nepārtrauktas darbības laiks:

4.1. Sistēmai ir jābūt pieejamai 24/7 režīmā. Sistēmas kopējā pieejamība gada laikā ir 99,6 %;

4.2. Sistēmas darbība pēc drošības incidenta, kura rezultātā ir iestājies darbības pārtraukums, jāatjauno ne vēlāk kā 12 stundu laikā pēc darbības pārtraukuma.