**IEKŠĒJIE NOTEIKUMI**

Rīgā

|  |  |  |  |
| --- | --- | --- | --- |
| Datums skatāms laika zīmogā |  | Nr. | 18- |

**Valsts kases informācijas sistēmas**

**“Centralizēta grāmatvedības un personāla lietvedības IS”**

**drošības politika**

Izdoti saskaņā ar

Valsts pārvaldes iekārtas likuma

72. panta pirmās daļas 2. punktu

Ministru kabineta 2024. gada 22. oktobra noteikumu Nr. 653 “Kārtība, kādā Valsts kase sniedz pakalpojumus valsts pārvaldes vienotā pakalpojumu centra ietvaros, un kārtība un apjoms, kādā valsts budžeta iestādes un budžeta nefinansētas iestādes kārto grāmatvedības uzskaiti Valsts kasē valsts pārvaldes vienotā pakalpojumu centra ietvaros” 36. punktu

1. **Vispārīgie jautājumi**
2. Valsts kases informācijas sistēmas “Centralizēta grāmatvedības un personāla lietvedības IS” (turpmāk - sistēma) drošības politika (turpmāk - politika) nosaka prasības sistēmas informācijas tehnoloģiju videi ar mērķi maksimāli nodrošināt aizsardzību pret ārējiem un iekšējiem apdraudējumiem.
3. Politika ir izstrādāta, lai nodrošinātu Nacionālās kiberdrošības likumā noteikto prasību ievērošanu un normatīvo aktu prasības informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām jomā (turpmāk - drošības noteikumi), kā arī 2024. gada 22. oktobra Ministru kabineta noteikumos Nr. 653 “Kārtība, kādā Valsts kase sniedz pakalpojumus valsts pārvaldes vienotā pakalpojumu centra ietvaros, un kārtība un apjoms, kādā valsts budžeta iestādes un budžeta nefinansētas iestādes kārto grāmatvedības uzskaiti Valsts kasē valsts pārvaldes vienotā pakalpojumu centra ietvaros” (turpmāk - VPC noteikumi) noteikto.

3. Politika ir saistoša visiem sistēmas lietotājiem un uzturētājiem.

1. **Raksturojums un analīze drošības jomā**
   1. Sistēma ir izveidota, pielāgojot Visma Horizon resursu vadības un grāmatvedības programmu centralizēta finanšu grāmatvedības uzskaites pakalpojuma un personāla lietvedības informācijas sistēmas pakalpojuma sniegšanai valsts budžeta iestādēm un budžeta nefinansētām iestādēm (turpmāk - iestādes).
   2. Sistēma sastāv no vairākām savstarpēji saistītām komponentēm – galvenās datubāzes, Horizon lietojumprogrammas, pašapkalpošanās portāla,  integrāciju programmsaskarnes un  Excel spraudņa.
   3. Sistēma ir standarta programmatūra, kuras esošā funkcionalitāte, funkcionalitātes izmaiņas un problēmu risināšana atkarīga no tās ražotāja.
   4. Visas iestādes izmanto kopēju sistēmu, kurā katras iestādes dati ir pilnībā nodalīti no citu iestāžu datiem, neņemot vērā valsts pārvaldes hierarhisko struktūru.
   5. Visi iestādes darbinieki ir sistēmas pašapkalpošanās portāla lietotāji (turpmāk - lietotāji), bet atsevišķi iestādes darbinieki izmanto sistēmu finanšu vadības, personāla lietvedības funkciju nodrošināšanai un iestādes pašapkalpošanās portāla lietotāju pārvaldībai.
   6. Pēc nepieciešamības iestādēm ir pieejamas programmsaskarnes sistēmu integrācijām un Excel spraudnis datu analītikai.
   7. Sistēmas ekspluatācijā netiek izmantoti mākoņdatošanas pakalpojumi ārpus Latvijas. Sistēmas darbībai publiskā interneta pieejamība nav nepieciešama.
   8. Lietotājiem sistēma pieejama, izmantojot vienoto valsts interneta plūsmu apmaiņas punktu.
   9. Sistēmas administrēšanu, konfigurēšanu, jauninājumu ieviešanu, problēmu risināšanu, lietotāju atbalstu un drošības uzraudzību nodrošina Valsts kase atbilstoši iekšējiem normatīviem aktiem, ievērojot VPC Noteikumu un drošības noteikumu prasības.
   10. Saskaņā ar drošības noteikumiem sistēmai ir novērtētas drošības klases un piešķirta drošības kategorija - paaugstinātas drošības sistēma.
2. **Drošības pārvaldības organizācijas principi**
   1. Valsts kase pārzina sistēmas tehnoloģisko resursu, nodrošinot tā pieejamību, lietojamību, pielāgojamību, savietojamību un drošību, atbild par informācijas drošības prasību noteikšanu un ievērošanu savā infrastruktūrā saskaņā ar drošības noteikumiem.
   2. Iestāde nodrošina saviem lietotājiem un integrācijām tehnoloģiskos resursus sistēmas piekļuvei~~,~~ un atbild par informācijas drošības prasību ievērošanu savā infrastruktūrā saskaņā ar drošības noteikumiem un sistēmas drošības politiku.
3. **Sistēmas aizsardzības pasākumi**
   1. Sistēma izvietota divos administratīvi un fiziski nodalītos datu centros Latvijas teritorijā ar iespēju operatīvi mainīt aktīvo centru.
   2. Sistēma pieejama izmantojot divus neatkarīgus interneta pakalpojumu sniedzējus ar iespēju operatīvi mainīt aktīvo pakalpojumu sniedzēju.
   3. Interneta domēnu vārdu ārējiem pieprasījumiem sistēma izmanot Cert.lv DNS ugunsmūri.
   4. Piekļūt iekārtām, kas nodrošina sistēmas darbību, atļauts tikai pilnvarotām personām.
   5. Sistēmas komponentes izmanto Valsts kases kopējo virtualizācijas un ugunsmūra risinājumu.
   6. Katra sistēmas komponente ir nodalīta savā datu tīkla segmentā, atļaujot tikai nepieciešamos datu savienojumus.
   7. Katras iestādes dati sistēmā atrodas savā, no citām iestādēm nodalītā datubāzē, kuras izvietotas vienā vai vairākos datubāžu serveros.
   8. Papildus sistēmas pamata darbības videi tiek uzturētas vēl divas tehniski nodalītas, bet loģiski identiskas sistēmas vides – demonstrācijas vide un pārbaudes vide.
   9. Sistēmas demonstrācijas vide dod iespēju iestādēm izmēģināt sistēmas funkcionalitāti un  pārbaudīt integrācijas programmsaskarņu darbību, tai skaitā pirms jaunu versiju uzstādīšanas.
   10. Sistēmas demonstrācijas vides dati tiek regulāri atjaunoti no pamata darbības vides un pieejami iestādēm ar tām pašām pieejas tiesībām kā pamata darbības videi.
   11. Sistēmas pārbaudes vide dod iespēju Valsts kasei pārbaudīt jaunākās sistēmas versijas un izmeklēt kļūdas.
   12. Sistēmas pārbaudes vide satur jauktus izlases iestāžu pamata darbības vides datus un pieejama Valsts kases darbiniekiem un piegādātajiem izpētei un problēmu risināšanai.
   13. Jebkuru Sistēmas jauninājumu vai konfigurācijas izmaiņu Valsts kase sākumā uzstāda sistēmas pārbaudes vidē, pēc tam nodrošina iestādēm iespēju pārbaudei demonstrācijas vidē un tikai pēc tam tiek uzstāda pamata darbības vidē.
   14. Lietotājiem piekļuvei sistēmai jāizmanto ierobežotu kopu (<https://www.nic.lv/lix>) publiskā interneta adrešu apgabalu.
   15. Lietotājiem, kuriem nepieciešams pieslēgties sistēmai no cita publiskā interneta adrešu apgabala, jāizmanto iestādes nodrošināts VPN slēgums ar tīkla ceļu uz sistēmu, kurš atrodas kādā no atļautiem adrešu apgabaliem.
   16. Sistēmas pašapkalpošanās portāla piekļuvei lietotajam jālieto kāds no aktuālajiem un regulāri atjaunotiem interneta pārlūkiem izmantojot standarta TCP portu 443 (HTTPS).
   17. Horizon lietojumprogrammas izmantošanai iestādei papildus jānodrošina piekļuve, izmantojot  TCP portu 1551 Valsts kases publiskā interneta adrešu apgabalā 91.245.194.0/24.
   18. Galvenā datubāze ir aizsargāta izmantojot dinamisku ugunsmūra risinājumu, kurš atļauj Horizon lietojumprogrammas piekļuvi tīkla līmenī tikai pēc sekmīgas lietotāja autentifikācijas.
   19. Katrs Sistēmas (t.sk. Pašapkalpošanās portāla) lietotāja konts ir saistīts ar konkrētu fizisku personu - identificētu, izmantojot kvalificētu elektroniskās identifikācijas līdzekli.
   20. Katrai sistēmas integrācijai tiek izmantots izdalīts sistēmas konts, kurš nav identificējams kā fiziska persona.
   21. Sistēmas Horizon lietojumprogrammas lietotāju un integrāciju programmsaskarnes sistēmas kontu pārvaldību nodrošina Valsts kase.
   22. Sistēmas pašapkalpošanās portāla lietotāju pārvaldību, izmantojot Sistēmas iespējas, nodrošina iestāde.
   23. Valsts kase nosaka un uztur sistēmas lietotāju lomas tā, lai tās funkcionalitāte ir izpildāma ar minimāli iespējamo tiesību kopu.
   24. Visas sistēmas komponenšu operētājsistēmas ir aizsargātas piemērojot CIS Benchmarks Level 1 (https://www.cisecurity.org/cis-benchmarks) rekomendācijas.
   25. Sistēmas operētājsistēmu publiskā interneta piekļuve ir ierobežota, atļaujot tikai komponenšu ražotāju norādītos datu savienojumus.
   26. Sistēmas uzstādīšanu, apkopi un ikdienas uzraudzību nodrošina Valsts kases administratori, izmantojot piegādātāju sagatavotas instrukcijas.
   27. Piegādātāju piekļuve sistēmai ir pieļaujama tikai tehniskas avārijas un būtisku problēmu risināšanas gadījumos.
   28. Jebkura piekļuve sistēmai un pašapkalpošanās portālam ir izsekojama līdz interneta protokola adresei.
   29. Valsts kase sistēmas auditācijas pierakstus veido un uzglabā vismaz 18 (astoņpadsmit) mēnešus pēc ieraksta izdarīšanas.
   30. Auditācijas pieraksti tiek veidoti, nodrošinot, ka ierakstā norādītais laiks sakrīt ar Valsts kases kopējās tehniskās infrastruktūras precīzā laika serveri.
   31. Valsts kase nodrošina sistēmas auditācijas pierakstu satura uzraudzību un analīzi.
   32. Operētājsistēmas pakalpojumi, kas netiek izmantoti sistēmas darbības nodrošināšanai, ir atspējoti.
   33. Sistēmas darbībai atļauti tikai tie tīkla savienojumi, kas nepieciešami.
   34. Datu plūsma starp sistēmu un tās lietotājiem, kā arī starp sistēmas komponentēm un citām sistēmām tiek šifrēta un uzraudzīta.
   35. Sistēmas lietotājiem ir pienākums ziņot Valsts kasei par identificētajiem informācijas drošības riskiem un notikumiem.
4. **Drošības risku pieņemamais līmenis**
   1. Valsts kase veic sistēmas tehnoloģiskā resursa risku novērtējumu un mazināšanu saskaņā ar Valsts kases Risku vadības politiku, ievērojot drošības noteikumu prasības.
   2. Atbilstoši drošības noteikumu prasībām Valsts kase nodrošina regulārus sistēmas ārējos ielaušanās testus.

1. **Noslēguma jautājums**
   1. Politiku pārskata drošības noteikumos paredzētajos gadījumos.

|  |  |  |
| --- | --- | --- |
| Pārvaldnieks | (paraksts\*) | K.Āboliņš |

\*Dokuments ir parakstīts ar drošu elektronisko parakstu

Vāvere 29550237

Lauris.Vavere@kase.gov.lv