SASKAŅOTS
Profesionālās izglītības un nodarbinātības
trīspusējās sadarbības apakšpadomes
2022. gada 8. jūnija sēdē, protokols Nr. 3

INFORMĀCIJAS SISTĒMU DROŠĪBAS SPECIĀLISTS
PROFESIONĀLĀS KVALIFIKĀCIJAS PRASĪBAS

1. Specializācijas vai saistītās profesijas nosaukums, kvalifikācijas līmenis	
Informācijas sistēmu drošības speciālists	*Ceturtais* profesionālās kvalifikācijas līmenis (4.PKL) (atbilst *piektajam* Latvijas kvalifikāciju ietvarstruktūras līmenim (5.LKI))
2. Profesijas nosaukums	
Specializācija piesaistīta profesijai 2522 01 „Datorsistēmu un datortīklu administrators" – 4.PKL. Profesijai 2522 01 „Datorsistēmu un datortīklu administrators" aktualizēts standarts.	

3. Darba uzdevumu veikšanai nepieciešamās prasmes un attieksmes, zināšanas un PROFESIONĀLĀS kompetences					
Nr. p.k.	**Uzdevumi**	**Prasmes un attieksmes**	**Zināšanas**	**Kompetences (kvalifikācijas līmenis)**	
3.1.	Novērot ar informācijas sistēmu drošību saistītās tehnoloģiju attīstības tendences	Izmantot zināšanas par jaunām nākotnes tehnoloģijām un izpratni par biznesu, lai paredzētu un formulētu nākotnē izmantojamos risinājumus. Sniegt vadībai ieteikumus un padomus, lai nodrošinātu atbalstu stratēģisku lēmumu pieņemšanā	*Priekšstata līmenī* Nākotnes tehnoloģijas un to atbilstošs pielietojums. *Izpratnes līmenī* Atbilstošie informācijas avoti (žurnāli, konferences un pasākumi, informatīvie biļeteni, vadošie speciālisti, tiešsaistes forumi u.t.t.) *Lietošanas līmenī* Diskusiju noteikumi tiešsaistes kopienās.	Spēja identificēt labākos risinājumu piegādātājus un pakalpojumu sniedzējus, novērtēt, pamatot un ieteikt iemērotāko.	*5.LKI*
3.2.	Izveidot informācijas drošības zināšanu bāzi.	Izstrādāt un veidot vispārēju funkcionālu specifikāciju un saskarnes. Pielietot iepriekšējās zināšanas par drošas infrastruktūras metodoloģiju Pielietot iepriekšējās zināšanas par drošas infrastruktūras metodoloģiju.	*Priekšstata līmenī* Drošu datu centru, serveru, krātuvju un tīklu izstrādes pamati. *Izpratnes līmenī* Mobilās tehnoloģijas. Apdraudējumu modelēšanas paņēmieni. *Lietošanas līmenī* Prasību modelēšanas un vajadzību analīzes paņēmieni. Risinājumu izstrādes metodes un to pamatojumi (prototipēšana, spējās metodes, reversā inženierija u.t.t.)	Spēja novērtēt prototipu izmantošanu, lai veicinātu savākto un noformēto prasību validēšanu. Spēja identificēt klientus, lietotājus un ieinteresētās puses un veidot ar tiem sistemātisku un biežu komunikāciju.	*5.LKI*

3.3.	Sniegt priekšlikumus jaunu tehnoloģiju integrēšanā.	Sistemātiski rīkoties, lai identificētu programmatūras un aparatūras specifikāciju saderību. Dokumentēt visas instalēšanas laikā veiktās darbības un reģistrēt novirzes un koriģējošās darbības. Ievērot atbilstošos drošības standartus un izmaiņu kontroles procedūras, lai saglabātu sistēmas funkcionalitātes un uzticamības integritāti.	*Priekšstata līmenī* Novecojušas, esošas un jaunas aparatūras komponentes un infrastruktūru moduļi. *Izpratnes līmenī* Sistēmas integrēšanas ietekme uz esošo organizāciju. Paņēmieni saskarnes veidošanai starp moduļiem, sistēmām un komponentēm. *Lietošanas līmenī* Integrēšanas pārbaudes paņēmieni. Izstrādes rīki (piemēram, izstrādes vide, pārvalde, pirmkoda piekļuves/versiju kontrole).	Spēja noteikt sistēmas veiktspēju un pārliecināties, ka integrētās sistēmas iespējas un efektivitāte atbilst specifikācijai. Spēja dokumentēt un reģistrēt darbības, problēmas un ar tām saistītos labojumus, aizsargāt/dublēt datus, lai sistēmas integrēšanas laikā nodrošinātu integritāti.	*5.LKI*
3.4.	Veikt nepieciešamās drošības pārbaudes un atjaunināšanu.	Sistemātiski rīkoties, lai izstrādātu sistēmas elementus, identificētu kļūdainās komponentes un noteiktu kļūmju pamatcēloņus. Rīkoties saskaņā ar norādījumiem, lai reģistrētu un izsekotu uzticamības datus un salīdzinātu tos ar pakalpojuma līmeņa līgumiem. Sistemātiski analizēt veiktspējas datus un eskalēt iespējamās servisa līmeņa kļūmes un drošības riskus, lai uzlabotu pakalpojuma uzticamību.	*Priekšstata līmenī* Tīmekļa, mākoņa, mobilo tehnoloģiju un vides prasības. Labā prakse. *Izpratnes līmenī* Programmatūras iepakošanas un izplatīšanas metodes un paņēmieni. Pakalpojumu sniegšanas pārraudzība. *Lietošanas līmenī* Problēmu pārvaldības paņēmieni (darbība, veiktspēja, saderība).	Spēja organizēt datubāzu aizpildīšanu un pārvaldīt datu migrāciju, organizēt un plānot beta testa darbības, testēšanas risinājumu gatavajā operatīvajā vidē. Spēja konfigurēt komponentus jebkurā līmenī, identificēt un veikt ekspertīzi, kas nepieciešama sadarbspējas problēmu risināšanai.	*5.LKI*

3.5.	Izvēlēties un izmantot drošības līdzekļus.	Izmantot padziļinātu ekspertīzi un gūt labumu no ārējiem standartiem un labākajām praksēm. Vadīt un piedalīties drošības vadlīniju un instrukciju izstrādē.	*Priekšstata līmenī* Atbilstošo standartu un labāko praksu potenciāls un iespējas. Tiesisko prasību ietekme uz informācijas drošību. *Izpratnes līmenī* Uzņēmuma informācijas stratēģija. Iespējamie drošības draudi. *Lietošanas līmenī* Mobilitātes stratēģija. Dažādi pakalpojumu modeļi (SaaS (Software as a service), PaaS (Platforma as a service, IaaS (Infrastructure as a service) un darbības formas.	Spēja kritiski analizēt un attīstīt uzņēmuma informācijas drošības stratēģiju.	*5.LKI*
3.6.	Kontrolēt un veikt IKT drošības novērtējumus, testus, apskates un auditus.	Identificēt, klasificēt un reģistrēt incidentus un traucējumus pakalpojumu sniegšanā, ievietojot tos katalogā pēc simptoma un risinājuma. Izmantot pieredzi, lai risinātu lietotāju problēmas un pārlūkotu datu bāzi, meklējot iespējamos risinājumus. Sistemātiski pārraudzīt un izpētīt vidi, lai identificētu vājās vietas un draudus, un novērstu jebkādus drošības pārkāpumus. Reģistrēt un eskalēt neatbilstības un sarežģītus un neatrisināmus incidentus.	*Priekšstata līmenī* Saikne starp sistēmas infrastruktūras elementiem un kļūmes ietekme uz biznesa procesiem, kas ar to saistīti. Uzņēmuma/iestādes infrastruktūra, kas var būt drošības incidentu mērķis. Tīmekļa, mākoņa, mobilo tehnoloģiju un vides prasības. *Izpratnes līmenī* Uzņēmuma kritisko situāciju eskalēšanas procedūras. Drošības struktūras principi. Kiberuzbrukumu paņēmieni un pasākumi, lai no tiem izvairītos. Datortehnikas ekspertīze. *Lietošanas līmenī*	Spēja veikt drošības revīzijas, identificēt iespējamas kritiskas komponentu kļūmes un veikt darbības, lai mazinātu kļūmes efektus. Spēja analizēt uzņēmuma nozīmīgākos aktīvus un identificēt to trūkumus un vietas, kuras nav pilnībā aizsargātas pret ielaušanos vai uzbrukumu.	*5.LKI*

			Uzņēmuma kopējā informācijas un komunikāciju tehnoloģiju infrastruktūra un galvenie komponenti. Atbilstošas informācijas un komunikāciju tehnoloģiju lietotāja lietotnes. Datu bāžu struktūras un satura organizācija. Informācijas un komunikāciju tehnoloģiju iekšējā revīzija un drošības problēmu atklāšanas paņēmieni.		
3.7.	Kontrolēt IKT resursu drošību un novērtēt riskus.	Piemērot riska pārvaldības principus un izpētīt informācijas un komunikāciju tehnoloģiju risinājumus, lai pielāgotu drošību un mazinātu riskus. Veikt informācijas un komunikāciju tehnoloģiju procesu un vides revīziju.	*Priekšstata līmenī* Labā prakse (metodoloģijas) un standarti risku analīzē**.** *Izpratnes līmenī* Pretpasākumu riska nepieļaušana plānošanā. *Lietošanas līmenī* Risku analīzes pielietojums, ņemot vērā uzņēmuma vērtības un intereses.	Spēja izstrādāt riska pārvaldības plānu, lai identificētu nepieciešamās profilakses darbības, izstrādāt un dokumentēt risku analīzes iznākumus un risku pārvaldības procesus.	*5.LKI*
3.8.	Testēt IKT nepārtrauktības plānu.	Organizēt testēšanas programmas un veidot skriptus, lai veiktu iespējamo vājo vietu slodzes testus, un dokumentēt iznākumus. Sistemātiski rīkoties, lai atbildētu uz ikdienas operatīvajām vajadzībām un reaģētu uz tām, izvairoties no pārtraukuma pakalpojuma sniegšanā un ievērojot pakalpojuma līmeņa līgumu un informācijas drošības prasības.	*Priekšstata līmenī* Dažādi tehniskie dokumenti, kas nepieciešami produktu, lietotņu un pakalpojumu izstrādei, pilnveidošanai un izvietošanai. Uzņēmējdarbības izaicinājumi un riski. *Izpratnes līmenī* Produktu versiju kontroles dokumentācija. Resursi, lai tiktu izpildītas ieinteresēto pušu prasības. *Lietošanas līmenī* Uzņēmuma drošības dokumentācija un procesi, tai skaitā lēmumu pieņemšana, budžeta un pārvaldības struktūra.	Spēja uzturēt atjauninātu uzņēmuma drošības dokumentāciju, noteikt reālus sagaidāmos rezultātus un izskaidrot drošības darbību nepieciešamību.	*5.LKI*

3.9.	Rūpēties par uzņēmuma/iestādes IKT drošības sistēmu atbilstību normatīvajiem dokumentiem	Noteikt dokumentācijas prasības, ņemot vērā tās pielietojuma mērķi un mērķauditoriju. Atbildēt par savām un citu darbībām, pārvaldot ierobežotu skaitu ieinteresēto pušu. Komunicēt ar personālu un sniegt visiem darbiniekiem nepieciešamo drošības informāciju.	*Priekšstata līmenī* Dažādi tehniskie dokumenti, kas nepieciešami produktu, lietotņu un pakalpojumu izstrādei, pilnveidošanai un izvietošanai. Uzņēmējdarbības izaicinājumi un riski. *Izpratnes līmenī* Produktu versiju kontroles dokumentācija. Resursi, lai tiktu izpildītas ieinteresēto pušu prasības. *Lietošanas līmenī* Uzņēmuma drošības dokumentācija un procesi, tai skaitā lēmumu pieņemšana, budžeta un pārvaldības struktūra.	Spēja uzturēt atjauninātu uzņēmuma drošības dokumentāciju, noteikt reālus sagaidāmos rezultātus un izskaidrot drošības darbību nepieciešamību.	*5.LKI*

Vispārīga informācija	
Profesionālās kvalifikācijas prasību iesniedzējs	***Latvijas Informācijas un komunikācijas tehnoloģijas asociācija (LIKTA)*** - Toms Lasmanis, IK „Awtech" izpilddirektors, - Vita Balikova, PIKC „Rīgas Tehniskā koledža" studiju programmas „Informācijas tehnoloģijas" direktore, docente - Andris Jaunkalns, PIKC „Rīgas Tehniskā koledža" datorsistēmu un datortīklu – administrators - Igors Būmanis, PIKC „Rīgas Tehniskā koledža" datorsistēmu un datortīklu administrators - Artūrs Maskalāns, AS Meridian Trade Bank IS drošības speciālists CISSP - Ainis Mūsiņš, Baltijas Datoru akadēmija, Nowell un Microsoft pasniedzējs - Aleksandrs Skritņiks, SIA „Eiropas Servisa centrs" datortehnikas servisa vadītājs - Daina Kārkliņa, „Tet" SIA pakalpojumu un partnerattiecību attīstības nodaļas vadītāja - Andris Kovaļevskis, LR Iekšlietu ministrijas Informācijas centra stacionāro komunikāciju nodrošināšanas nodaļas priekšnieks - Didzis Kukainis, VSIA Bērnu klīniskās slimnīcas IT daļas vadītājs**.**
Profesionālās kvalifikācijas prasību ekspertu darba grupa	- Una Rogule-Lazdiņa – Ekonomikas ministrija, Nozaru politikas departaments direktora vietniece, eksperts, - Andris Melnūdris – Latvijas Informācijas un komunikācijas tehnoloģijas asociācijas ģenerāldirektors,eksperts/iesniedzējs; - Igors Būmanis - PIKC Rīgas Tehniskā koledža Datorsistēmu un datortīkluadministrators, eksperts/iesniedzējs; - Jānis Brants – Latvijas Koledžu asociācijas eksperts, Rīgas Tehniskā koledža lektors,eksperts; - Anete Jekuma – EIKT nozares ekspertu padome eksperte, NEP koordinatore; - Inese Paudere – Valsts izglītības satura centrs Profesionālās izglītības departaments Profesionālās izglītības satura nodrošinājuma nodaļa vecākā referente.
Profesionālās kvalifikācijas prasību NEP atzinums	30.05.2022.
Profesionālās kvalifikācijas prasību saskaņošana PINTSA	08.06.2022.
Profesionālās kvalifikācijas prasību iepriekš saskaņotās redakcijas	-