SASKAŅOTS
Profesionālās izglītības un nodarbinātības
trīspusējās sadarbības apakšpadomes
2024. gada 7. augusta sēdē, protokols Nr. 5.

PROFESIJAS STANDARTS
INFORMĀCIJAS DROŠĪBA

KIBERDROŠĪBAS TEHNIĶIS
PROFESIONĀLĀS KVALIFIKĀCIJAS PRASĪBAS

1. Profesionālās kvalifikācijas nosaukums, kvalifikācijas līmenis, prasības izglītībai	
Kiberdrošības tehniķis ESCO 3512.3	**Kvalifikācijas līmenis:** Ceturtais profesionālās kvalifikācijas līmenis (4. PKL)
	Prasības attiecībā uz iepriekš iegūto izglītību: Nav
2. Profesionālās kvalifikācijas daļas un profesionālās kvalifikācijas prasības attiecībā uz specializāciju un saistītu profesionālo kvalifikāciju	
Prasības attiecībā uz darba tirgū atpazīstamu kvalifikācijas daļu: Nav	
Profesionālās kvalifikācijas specializācijas: Nav	
Saistītās profesionālās kvalifikācijas, kvalifikācijas līmenis: Informācijas sistēmu drošības speciālists, 5. PKL	
3. Profesionālās darbības pienākumu un uzdevumu kopsavilkums	
Kiberdrošības tehniķis ir speciālists (junior) , kurš organizācijā atbildīgi veic uzticētos darba pienākumus, kas ietver organizācijas kiberdrošības risinājumu uzturēšanu, reaģēšanu uz kiberdrošības incidentiem un informācijas un komunikāciju tehnoloģiju (turpmāk - IKT) sistēmu drošības testēšanu un ievainojamību ziņojumu apstrādi, nodrošinot datu apstrādi atbilstoši normatīvajiem regulējumiem, nozares prasībām un organizācijas noteiktajai kārtībai. Kiberdrošības tehniķa pienākumi un uzdevumi: **3.1. Organizācijas IKT vides un kiberdrošības prasību apzināšana:** 3.1.1. iepazīt organizācijas IKT vidi un drošības arhitektūru; 3.1.2. apzināt spēkā esošās kiberdrošības prasības, kas piemērojamas organizācijai; 3.1.3. iepazīt esošās kiberdrošības prasības; 3.1.4. novērtēt esošo kiberdrošības prasību izpildi; 3.1.5. piedāvāt iespējamos uzlabojumus savas kompetences ietvaros; 3.1.6. konsultēt gala lietotājus kiberdrošības prasību īstenošanas jautājumos. **3.2. Reaģēšana uz kiberdrošības incidentiem:** 3.2.1. kiberdrošības incidentu identificēšana; 3.2.2. kiberdrošības incidentu klasificēšana;	

3.2.3. kiberdrošības incidentu izpēte;
3.2.4. kiberdrošības incidentu un ar to saistītās informācijas apstrāde;
3.2.5. pēc-incidenta datu apkopošana;
3.2.6. pēc incidenta rezultātu apkopošana un uzlabojumu ieteikšana.

3.3. Kiberdrošības risinājumu(turpmāk - risinājumi) izmantošana organizācijā (sistēmas, programmatūru, vadlīnijas un pakalpojumus):
3.3.1. novērtēt organizācijas risinājumus;
3.3.2. apzināt tehniskās prasības nepieciešamajam risinājumam;
3.3.3. salīdzināt līdzvērtīgus tirgū pieejamos risinājumus;
3.3.4. kiberdrošības risinājumu ieviešana/uzstādīšana pēc iepriekš noteiktām instrukcijām;
3.3.5. kiberdrošības risinājumu uzturēšana;
3.3.6. apkopot risinājumu rezultatīvos rādījumus.

3.4. IKT sistēmu drošības testēšana:
3.4.1. apzināties drošības testu tvērumu;
3.4.2. iepazīties ar testa plānu;
3.4.3. iepazīties ar testa scenāriju;
3.4.4. veikt drošības testēšanu atbilstoši scenārijiem;
3.4.5. apstrādāt drošības testu rezultātus;
3.4.6. iepazīstināt tiešo vadītāju ar drošības testu rezultātiem.

3.5. Profesionālās darbības pamatuzdevumu un pienākumu izpildei nepieciešamās prasmes un attieksmes, vispārējās zināšanas un kompetences:
3.5.1. lietot valsts valodu;
3.5.2. lietot starpkultūru komunikācijas principus un daudzvalodu kompetenci;
3.5.3. lietot IKT lietpratēja līmenī;
3.5.4. ievērot darba tiesību normas, vides aizsardzības un civilās aizsardzības prasības;
3.5.5. ievērot tiesību aktu prasības elektrodrošības un ugunsdrošības jomā;
3.5.6. nelaimes gadījumā rīkoties atbilstoši situācijai un sniegt pirmo palīdzību;
3.5.7. pilnveidot savu profesionālo kvalifikāciju, zināšanas un prasmes;
3.5.8. pielietot matemātisko un kritisko domāšanu;
3.5.9. iesaistīties uzņēmuma darbības attīstībā.

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence					
Nr.p.k.	**Uzdevumi**	**Prasmes**	**Profesionālās zināšanas**	**Kompetence (kvalifikācijas līmenis)**	
4.1. **Organizācijas IKT vides un kiberdrošības prasību apzināšana:**					
4.1.1.	Iepazīt organizācijas IKT vidi un drošības arhitektūru.	Iepazīties ar organizācijas IKT dokumentāciju. Iepazīties ar IKT infrastruktūras uzbūves shēmām. Identificēt organizācijā izmantotos tehnoloģiskos risinājumus. Iepazīt organizācijas kiberdrošības prasības. Apzināt organizācijas plānos iekļauto drošības pārvaldības aspektus.	**Izpratnes līmenī:** IKT infrastruktūras uzbūve. Informācijas sistēmu (turpmāk – IS) uzbūve un komponentes. Tehnoloģiju attīstības tendences. Autentifikācija/autorizācija. Integrācija ar datubāzēm. Mikroservisu arhitektūra. Mākoņplatformas. TCP/IP protokolu kopa. **Lietošanas līmenī:** Datu pārraides tīklu darbība. Klienta-Servera modeļa darbība. *Windows* sistēmu pārvaldība. *Linux* sistēmu pārvaldība. Tehniskās dokumentācijas izprašana.	Spēja iepazīties ar organizācijas IKT vidi un esošo drošības arhitektūru, vadoties pēc organizācijas IKT un IKT drošības aktuālās dokumentācijas (Drošības politikas, procedūras, tehniskā dokumentācija).	LKI 4. līmenis

4.1.2.	Apzināt spēkā esošās kiberdrošības prasības, kas piemērojamas organizācijai.	Veikt kiberdrošības normu izpēti un analīzi. Veikt spēkā esošo normatīvo regulējumu izpēti. Sadarbībā ar organizācijas ekspertiem veikt kiberdrošības prasību apzināšanu.	**Izpratnes līmenī:** Informācijas drošības standarti un labā prakse (Piemēram, ISO 27001, 27002, OWASP). Izprot kiberdrošības stratēģiju nacionālā līmenī. **Lietošanas līmenī:** Kiberdrošības prasību labā prakse un standarti attiecībā uz incidentu pārvaldību (Piemēram, ITIL).	Spēja patstāvīgi apzināt un apkopot organizācijas kiberdrošības prasības.	LKI 4. līmenis
4.1.3.	Iepazīt esošās kiberdrošības prasības.	Veikt ārējo un iekšējo kiberdrošības prasību apzināšanu.	**Izpratnes līmenī:** Normatīvo aktu analīzes metodes un paņēmieni.	Spēja apkopot un analizēt esošās ārējās un iekšējās kiberdrošības prasības organizācijā.	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence					
Nr.p.k.	**Uzdevumi**	**Prasmes**	**Profesionālās zināšanas**	**Kompetence (kvalifikācijas līmenis)**	
		Pielietot dažādus digitālos rīkus kiberdrošības prasību izvērtēšanas procesā.	Organizācijas kiberdrošības politika, procedūra, vadlīnijas, instrukcijas. **Lietošanas līmenī:** Lēmumu pieņemšanas koki. Normatīvo aktu analīzes rīki. Metodes un rīki, kas atbalsta prasību apkopošanu un lēmumu pieņemšanu.		
4.1.4.	Novērtēt esošo kiberdrošības prasību izpildi.	Izmantot novērtējuma kritēriju kopu. Pielietot novērtējuma matricas rezultātu apkopošanai.	**Lietošanas līmenī:** Novērtējuma matricas.	Spēja novērtēt esošo kiberdrošības prasību izpildi organizācijā.	LKI 4. līmenis
4.1.5.	Piedāvāt iespējamos uzlabojumus savas kompetences ietvaros.	Piedāvāt uzlabojumus, balstoties uz novērtējuma rezultātiem, savas kompetences ietvaros..	**Lietošanas līmenī:** Pārmaiņu vadība. Izmaiņu pārvaldība.	Spēja piedāvāt nepieciešamos kiberdrošības uzlabojumus organizācijā.	LKI 4. līmenis
4.1.6.	Sniegt informāciju gala lietotājiem kiberdrošības prasību īstenošanas jautājumos.	Informēt saprotami un uztverami par kiberdrošības prasību īstenošanas pasākumiem. Sniegt ar kiberdrošību saistīto tehnisko atbalstu gala lietotājiem.	**Lietošanas līmenī:** Dažādas ar kiberdrošību saistītas vispārīgās teorijas, koncepti, mērķi un prasības. Dažādas sociālās inženierijas un krāpniecības metodes. Lietišķās komunikācijas veidi. Kiberhigiēnas pamatprincipi.	Spēja konsultēt gala lietotājus kiberdrošības prasību īstenošanas jautājumos.	LKI 4. līmenis
4.2. Reaģēšana uz kiberdrošības incidentiem:					
4.2.1.	Kiberdrošības incidentu identificēšana.	Noteikt ietekmētos resursus. Apzināt ietekmētos resursus, lietotājus, iespējamos cēloņus.	**Izpratnes līmenī:** Incidentu ap strādes standarti. Incidentu apstrādes rīki. Incidentu veidi/sadalījums.	Spēja identificēt kiberdrošības incidentus, ietekmētos resursus un iesaistītās puses. Spēja veikt kiberdrošības incidentu reģistrēšanu.	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence					
Nr.p.k.	**Uzdevumi**	**Prasmes**	**Profesionālās zināšanas**	**Kompetence (kvalifikācijas līmenis)**	
			Lietošanas līmenī: Incidentu priekšizpēte. Incidentu reģistrēšanas kritēriji. Incidentu reģistrēšanas rīki.	Spēja veikt incidentu ziņošanu saskaņā ar organizācijas incidentu apstrādes procedūrām.	
4.2.2.	Kiberdrošības incidentu klasificēšana.	Veikt kiberdrošības incidenta ietekmes novērtēšanu. Klasificēt kiberdrošības incidentus atbilstoši organizācijas izvēlētajai kritēriju kopai (uzbrukuma vektors, avots).	**Lietošanas līmenī:** Apdraudējumu klasifikācija. Incidentu apstrādes kārtība organizācijā. Kiberuzbrukumu vektori, avoti.	Spēja patstāvīgi veikt incidentu klasifikāciju atbilstoši organizācijas norādījumiem.	LKI 4. līmenis
4.2.3.	Kiberdrošības incidentu izpēte.	Veikt kiberdrošības incidentu izpēti. Analizēt IS apdraudējumus vai dažādas to kļūmes pēc žurnālu ierakstiem. Analizēt dažādu žurnālu (tīklu, serveru, gala lietotāju sistēmu) ierakstus.	**Izpratnes līmenī:** Incidentu reaģēšanas soļi. Iesaistītās puses, to atbildības. Dažādi ietekmes novērtējumu veidi (piem., organizācijai, datu subjektam, industrijai). **Lietošanas līmenī:** Operētājsistēmu darbība. Datu pārraides tīklu uzbūve un darbības principi. Dažādu sistēmu ievainojamības. Kiberdrošības uzbrukumu metodes. Žurnālu ierakstu apstrāde.	Spēja veikt kiberdrošības incidentu izpēti sadarbībā ar incidentu izpētē iesaistītajām pusēm.	LKI 4. līmenis
4.2.4.	Kiberdrošības incidentu un ar to saistītās informācijas apstrāde.	Sadarboties ar kiberdrošības incidentu novēršanā iesaistītajām pusēm. Sniegt atbalstu incidenta ierobežošanā un novēršanā iesaistītajām pusēm.	**Izpratnes līmenī:** SOC darbības pamatprincipi. Latvijas kiberdrošības atbildīgo institūciju hierarhija un to uzdevumi.	Spēja veikt kiberdrošības incidentu informācijas apstrādi. Spēja sekot organizācijas noteiktajai incidentu apstrādes kārtībai un	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence					
Nr.p.k.	**Uzdevumi**	**Prasmes**	**Profesionālās zināšanas**	**Kompetence (kvalifikācijas līmenis)**	
		Apkopot digitālos pierādījumus, nodrošinot to integritāti. Ziņot par drošības incidentiem saskaņā ar organizācijas drošības politikas vadlīnijām, incidentu apstrādes procedūrām. Dokumentēt organizācijas kiberdrošības incidentus. Uzturēt aktuālu kiberdrošības incidentu reģistru.	Digitālās izmeklēšanas metodes un rīki. Krīzes reaģēšanas soļi. **Lietošanas līmenī:** Incidentu apstrādes labā prakse. Digitālo pierādījumu dokumentēšana. Kiberdrošības incidentu reģistrs.	sadarboties ar incidenta reaģēšanā iesaistītajām pusēm.	
4.2.5.	Pēc-incidenta datu apkopošana.	Apkopot informāciju pēc-incidenta ziņojumiem. Piedalīties incidentu reaģēšanas aktivitāšu apkopošanā.	**Izpratnes līmenī:** Incidentu pārvaldības process. Kiberdrošības saistošā likumdošana un tiesību akti. **Lietošanas līmenī:** Incidentu reģistrēšanas rīki. Incidentu ziņojumu analīze.	Spēja apkopot informāciju pēc-incidenta ziņojuma sagatavošanai. Spēja apkopot incidenta reģistra datus/veiktos pasākumus incidenta reaģēšanas aktivitāšu izvērtēšanai.	LKI 4. līmenis
4.2.6.	Pēc-incidenta rezultātu apkopošana un uzlabojumu ieteikšana.	Piedalīties incidentu reaģēšanas aktivitāšu uzlabojumu identificēšanā. Sniegt pēc-incidenta analīzes apkopotos rezultātus iesaistītajām pusēm.	**Lietošanas līmenī:** Incidentu reaģēšanas labā prakse. Incidentu apstrādes kārtība organizācijā. Incidentu reaģēšanas vadlīnijas un standarti.	Spēja veidot pēc-incidenta ziņojumus reaģēšanā iesaistītajām pusēm. Spēja identificēt potenciālos incidentu reaģēšanas uzlabojumus.	LKI 4. līmenis
4.3.Kiberdrošības risinājumu izmantošana nodrošināšana organizācijā (sistēmas, programmatūru, vadlīnijas un pakalpojumus):					
4.3.1.	Novērtēt organizācijas kiberdrošības risinājumus.	Izvērtēt esošos kiberdrošības risinājumu atbilstību organizācijas identificētajām (iekšējām un ārējām) prasībām.	**Izpratnes līmenī:** Kiberdrošības standarti un ietvari. Kiberhigiēnas pamatprincipi.	Spēja novērtēt organizācijas kiberdrošības risinājumus.	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence					
Nr.p.k.	**Uzdevumi**	**Prasmes**	**Profesionālās zināšanas**	**Kompetence (kvalifikācijas līmenis)**	
		Identificēt kiberdrošības risinājumu iespējamos uzlabojumus.	Kiberdrošības risinājumu tehniskās prasības. **Lietošanas līmenī:** Drošības sistēmu veidi. Drošības sistēmu izvērtēšana. Datu pārraides tīklu infrastruktūra un tās komponentes. OS iestatīšana, izmantojot labo praksi. OS kiberdrošības rīku konfigurēšana un izmantošana.	Spēja identificēt iespējamos kiberdrošības risinājumu uzlabojumus.	
4.3.2.	Apzināt tehniskās un funkcionālās prasības nepieciešamajam risinājumam.	Noskaidrot kiberdrosības risinājumu tehniskās prasības. Noskaidrot kiberdrošības risinājumu funkcionālās prasības.	**Izpratnes līmenī:** Infrastruktūras arhitektūras prasības. Simetriskās un asimetriskās šifrēšanas darbības pamatprincipi un algoritmi. Tehniskās dokumentācijas avoti. Tehniskā terminoloģija. **Lietošanas līmenī:** Tehniskās dokumentācijas analīze.	Spēja apzināt tehniskās un funkcionālās prasības nepieciešamajam risinājumam.	LKI 4. līmenis
4.3.3.	Salīdzināt līdzvērtīgus tirgū pieejamos kiberdrošības risinājumus.	Apzināt iespējamos kiberdrošības risinājumus. Salīdzināt iespējamos kiberdrošības risinājumus.	**Lietošanas līmenī:** Tehniskās dokumentācijas interpretācija. Risinājumu licencēšanas prasību izvērtēšana.	Spēja salīdzināt līdzvērtīgus tirgū pieejamos kiberdrošības risinājumus.	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence					
Nr.p.k.	**Uzdevumi**	**Prasmes**	**Profesionālās zināšanas**	**Kompetence (kvalifikācijas līmenis)**	
4.3.4.	Kiberdrošības risinājumu ieviešana/uzstādīšana pēc iepriekš noteiktām instrukcijām	Uzstādīt datu pārraides tīklu drošības sistēmas (ugunsmūrus, IDS, IPS u.c.). Uzstādīt gala ierīču drošības sistēmas (anti-vīrusi, ugunsmūri u.c.). Integrēt kiberdrošības risinājumus organizācijas infrastruktūrā.	**Izpratnes līmenī:** Drošas programmatūras izstrādes dzīvescikls. **Lietošanas līmenī:** Skriptu (īsu programmu) veidošana (piem. *Python, Bash*).	Spēja uzstādīt/ieviest atbilstošākos kiberdrošības risinājumus organizācijas drošības arhitektūrā (infrastruktūra, procesi, dati u.c.) pēc iepriekš noteiktām instrukcijām.	LKI 4. līmenis
4.3.5.	Kiberdrošības risinājumu uzturēšana.	Konfigurēt sistēmas un servisus atbilstoši kiberdrošības prasībām savas kompetences ietvaros. Ieviest izmaiņas kiberdrošības tehniskajos risinājumos savas kompetences ietvaros.	**Izpratnes līmenī:** Organizācijas kiberdrošības procedūras un kontroles. **Lietošanas līmenī:** Produktu tehniskā dokumentācija. Informācijas sistēmu (IS) nocietināšanas pasākumi. PKI (Publiskās atslēgas infrastruktūra un sertifikāti).	Spēja nodrošināt ar kiberdrošību saistīto tehnisko risinājumu uzturēšanu atbilstoši organizācijas noteiktajām prasībām un tehniskajai dokumentācijai. Spēja ieviest izmaiņas esošajā infrastruktūrā atbilstoši organizācijas kiberdrošības prasībām.	LKI 4. līmenis
4.3.6.	Apkopot risinājumu rezultatīvos rādījumus	Nodrošināt kiberdrošības risinājumu rezultatīvo rādītāju apkopošanu atbilstoši noteiktajiem uzdevumiem. Interpretēt kiberdrošības risinājumu rezultatīvos rādītājus sadarbībā ar citiem speciālistiem.	**Izpratnes līmenī:** Organizācijas kiberdrošības politika, procedūra, vadlīnijas, instrukcijas. **Lietošanas līmenī:** Drošas IS darbības principi. Virtuālais privātais tīkls (VPN) darbības principi. Konfigurācijas failu izveide un analīze. Drošības bāzes līnijas (Security baseline). Kiberdrošības kontroļu novērtēšanas paņēmieni.	Spēja sagatavot kiberdrošības risinājumu rezultātu apkopojumu tālākai analīzei. Spēja interpretēt no risinājumiem iegūtos rezultātus.	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence					
Nr.p.k.	**Uzdevumi**	**Prasmes**	**Profesionālās zināšanas**	**Kompetence (kvalifikācijas līmenis)**	
4.4. IKT sistēmu drošības testēšana:					
4.4.1.	Apzināties kiberdrošībastestu tvērumu.	Iepazīties ar noteiktiemkiberdrošības testu uzdevumiem. Iepazīties ar kiberdrošības testa tvērumā iekļaujamajām IKT komponentēm un atļautajām metodēm.	**Izpratnes līmenī:** Informācijas sistēmu uzbūve. Operētājsistēmu arhitektūra un darbības principi. Drošības testēšanas standarti un ietvari. **Lietošanas līmenī:** Operētājsistēmu drošība. Datu pārraides tīklu uzbūve un darbība, tīklu drošība.	Spēja iepazīties ar noteiktiem kiberdrošības testu uzdevumiem. Spēja apzināt kiberdrošības testu tvērumā iekļautās IKT komponentes.	LKI 4. līmenis
4.4.2.	Iepazīties ar testa plānu.	Izvēlēties piemērotas drošības testēšanas metodes un rīkus savas kompetences ietvaros. Noteikt iespējamos kiberuzbrukumu vektorus, kas attiecas uz testējamajām IKT komponentēm.	**Izpratnes līmenī:** Testēšanas standarti un vadlīnijas. Testēšanas ietekmes apzināšana uz testējamajām IKT komponentēm. **Lietošanas līmenī:** Dažādas drošības testēšanas metodikas (piem. OWASP). Zināmo ievainojamību avoti (piem. CVE, CERT.LV publicētie u.c.).	Spēja apzināt testa plānu un piemērot drošības testēšanas metodes un rīkus, lai noteiktuiespējamos kiberuzbrukumu vektorus.	LKI 4. līmenis
4.4.3.	Iepazīties ar testa scenāriju.	Iepazīstas ar kiberdrošības scenāriju atbilstoši kiberdrošībastesta plānam. Veikt izpildāmo testēšanas scenāriju pielāgošanu aktuālajai situācijai, ja tas ir nepieciešams.	**Izpratnes līmenī:** Datu pārraides tīklu darbība. Informācijas sistēmu uzbūve. Sociālās inženierijas metodes un paņēmieni. **Lietošanas līmenī:**	Spēja apgūt testa scenārijus un pēc nepieciešamības pielāgot tos aktuālajai situācijai.	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence					
Nr.p.k.	**Uzdevumi**	**Prasmes**	**Profesionālās zināšanas**	**Kompetence (kvalifikācijas līmenis)**	
			Scenāriju izstrādes procedūras, izmaiņu pārvaldība. Kiberuzbrukumu metodes. Tīmekļa aplikāciju uzbūve. Kiberdrošības risinājumi.		
4.4.4.	Veikt IKT drošības testēšanu atbilstoši scenārijiem.	Secīgi izpildīt testus/testēšanas plānu, veicot starprezultātu izvērtējumu. Veikt testēšanas plāna un izpildāmo scenāriju pielāgošanu. Izmantot drošības testēšanas rīkus un testa programmas. Identificēt sistēmu drošības ievainojamības.	**Lietošanas līmenī:** Skriptu (īsu programmu) veidošana (piem. Python, Bash). Drošības testēšanas rīki. Kiberuzbrukumu metodes.	Spēja precīzi izpildīt testēšanas plānu, scenārijus, izmantojot atbilstošus rīkus un metodes sistēmu ievainojamību identificēšanai.	LKI 4. līmenis
4.4.5.	Apstrādāt IKT drošības testu rezultātus.	Novērtēt testēšanas laikā atklāto konfigurācijas nepilnību un drošības ievainojamību kritiskumu, ņemot vērā ietekmi uz organizācijas kiberdrošību. Dokumentēt drošības testēšanas rezultātus. Gatavot rekomendācijas organizācijas drošības ievainojamību novēršanai.	**Izpratnes līmenī:** Organizācijas biznesa procesi. Kiberdrošības risku klasifikācija. **Lietošanas līmenī:** Zināmo ievainojamību avotu analīze un pielietošana (piem. CVE, CERT.LV publicētie u.c.). Ievainojamību aprakstu, ziņojumu un atskaišu veidošana, analīze	Spēja analizēt un dokumentēt testēšanas rezultātus, izstrādāt priekšlikumus organizācijas IS kiberdrošības uzlabošanai. Spēja sagatavot rekomendācijas identificēto ievainojamību novēršanai, sistēmu un servisu kiberdrošības uzlabošanai.	LKI 4. līmenis
4.4.6.	Iepazīstināt tiešo vadītāju ar drošības testu rezultātiem.	Demonstrēt IKT drošības ievainojamības izmantošanu. Skaidrot IKT drošības testu rezultātus ieinteresētajām pusēm.	**Izpratnes līmenī:** Kiberrisku apstrādes stratēģijas Drošības kontroļu klasifikācija dažādos standartos	Spēja sagatavot un iepazīstināt ar IKT drošības testēšanas rezultātiem tiešo vadītāju, pielietojot profesionālo valodu un terminoloģiju, nodrošinot informācijas skaidru un saprotamu izklāstu.	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence					
Nr.p.k.	**Uzdevumi**	**Prasmes**	**Profesionālās zināšanas**	**Kompetence (kvalifikācijas līmenis)**	
			Testa ziņojumu veidnes **Lietošanas līmenī:** Kiberriska ietekmes un varbūtības kvalitatīva un kvantitatīva analīze.		

5. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā VISPĀRĒJĀ kompetence					
Nr.p.k.	**Uzdevumi**	**Prasmes**	**Profesionālās zināšanas**	**Kompetence (kvalifikācijas līmenis)**	
5. Profesionālās darbības pamatuzdevumu un pienākumu izpildei nepieciešamās prasmes un attieksmes, vispārējās zināšanas un kompetences:					
5.1.	Lietot valsts valodu.	Sazināties valsts valodā. Lietot profesionālo IKT terminoloģiju valsts valodā. Pielietot lietišķās komunikācijas metodes un paņēmienus.	**Izpratnes līmenī:** Vārdu krājums. Gramatikas un valodas funkcijas. Valodas un komunikācijas daudzveidība dažādos kontekstos. **Lietošanas līmenī:** Valsts valoda. Profesionālā IKT terminoloģija valsts valodā. Lietišķās komunikācijas metodes un paņēmieni.	Spēja sazināties mutiski un rakstiski valsts valodā, lietojot profesionālo terminoloģiju.	LKI 4. līmenis
5.2.	Lietot starpkultūru komunikācijas principus un daudzvalodu kompetenci.	Sazināties mutiski un rakstiski angļu valodā dažādās profesionālās situācijās un vidēs. Lietot profesionālo terminoloģiju angļu valodā. Ievērot starpkultūru komunikācijas principus daudzkultūru vidē. Iesaistīties uzņēmuma kultūrvidē. Sadarboties komandā.	**Izpratnes līmenī:** Vārdu krājums. Gramatikas un valodas funkcijas. Valodas un komunikācijas daudzveidība dažādos kontekstos. **Lietošanas līmenī:** Prezentēšanas prasmes. Profesionālā terminoloģija angļu valodā. Starpkultūru mijiedarbība. Starpkultūru komunikācijas principi daudzkultūru vidē. Savas nacionālās kultūras un citu kultūru standarti un vērtības.	Spēja sazināties angļu valodā, lietojot profesionālo terminoloģiju. Spēja efektīvi komunicēt daudzkultūru vidē. Spēja efektīvi iesaistīties komandas darbā. Spēja prezentēt informāciju atbilstoši formātam un auditorijai.	LKI 4. līmenis

5. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā VISPĀRĒJĀ kompetence					
Nr.p.k.	**Uzdevumi**	**Prasmes**	**Profesionālās zināšanas**	**Kompetence (kvalifikācijas līmenis)**	
			Sadarbības veicināšanas principi.		
5.3.	Lietot IKT lietpratēja līmenī.	Sagatavot pēc parauga dokumentus, izmantojot lietojumprogrammas. Atrast noteiktu informāciju interneta resursos, datu nesējos. Sazināties, izmantojot IKT rīkus. Piemērot IKT rīkus sava darba pilnveidē	**Izpratnes līmenī:** Normatīvie akti IKT un kiberdrošības jomās. **Lietošanas līmenī:** Darba vides reglamentējošie noteikumi organizācijā. Lietojumprogrammas atbilstoši darba uzdevumam. Kiberdrošības prasības infrastruktūrai, IS komponentēm, fiziskās drošības un cilvēkdrošības jomās.	Spēja pielietot IKT rīkus darba uzdevuma veikšanā. Spēja ievērot valstī un organizācijā noteiktās kiberdrošības prasības.	LKI 4. līmenis
5.4.	Ievērot darba tiesību normas, vides aizsardzības un civilās aizsardzības prasības.	Lietot individuālos un kolektīvos aizsardzības līdzekļus un drošības ierīces. Lietot ergonomiskos darba paņēmienus un instrumentus. Ievērot vides aizsardzības prasības.	**Lietošanas līmenī:** Individuālo un kolektīvo aizsardzības līdzekļu veidi un to lietošana. Ergonomiskie darba paņēmieni, metodes un rīki. Vides aizsardzības prasības biroja darbā.	Spēja ievērot tiesību aktu prasības darba aizsardzības un vides aizsardzības jomā. Spēja ievērot civilās aizsardzības prasības atbilstoši civilās aizsardzības plāniem un normatīvajiem aktiem.	LKI 4. līmenis
5.5.	Ievērot tiesību aktu prasības elektrodrošības un ugunsdrošības jomā.	Veikt darbus atbilstoši elektrodrošības prasībām. Veikt darbus atbilstoši ugunsdrošības prasībām.	**Lietošanas līmenī:** Elektrodrošības prasības darba vietā. Ugunsdrošības prasības darba vietā.	Spēja ievērot tiesību aktu prasības elektrodrošības un ugunsdrošības jomā. Spēja ievērot un uzraudzīt darba drošības, vides aizsardzības, elektrodrošības, ugunsdrošības, higiēnas un kvalitātes prasības, skaidrojot atsevišķiem darba procesa posmiem atbilstošas prasības. Spēja identificēt un izvērtēt riskus, kas var rasties izmantojot IKT.	LKI 4. līmenis

5. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā VISPĀRĒJĀ kompetence					
Nr.p.k.	**Uzdevumi**	**Prasmes**	**Profesionālās zināšanas**	**Kompetence (kvalifikācijas līmenis)**	
5.6.	Nelaimes gadījumā rīkoties atbilstoši situācijai un sniegt pirmo palīdzību.	Izvērtēt ārkārtas situāciju. Rīkoties ārkārtas situācijā. Sniegt pirmo palīdzību.	**Lietošanas līmenī:** Rīcība ārkārtas situācijā (elektrotrauma, ugunsgrēks u.c.). Pirmās palīdzības ABC.	Spēja nelaimes gadījumā rīkoties atbilstoši situācijai un sniegt pirmo palīdzību. Spēja atbildīgi rīkoties ārkārtas situācijā un izņēmuma stāvokļa laikā, ievērojot valsts noteikto regulējumu un apzinoties savu atbildību nacionālās drošības saglabāšanā. Spēja rīkoties atbilstoši organizācijas noteiktajai kārtībai.	LKI 4. līmenis
5.7.	Pilnveidot savu profesionālo kvalifikāciju, zināšanas un prasmes.	Novērtēt savu profesionālo pieredzi un profesionālās kompetences līmeni. Apzināties savas personīgās un sociālās attīstības/ pilnveides vajadzības un iespējas. Mērķtiecīgi plānot profesionālo kompetenču pilnveidi. Sistemātiski apgūt jaunas zināšanas un pieredzi.	**Izpratnes līmenis:** Pašnovērtējuma metodes, paņēmieni un rīki. Mācīšanās stratēģijas. **Lietošanas līmenī:** Mācību, karjeras un darba gaitas plānošana.	Spēja identificēt, izvērtēt un izmantot profesionālās pilnveides informācijas resursus savas kvalifikācijas celšanai. Spēja plānot un pieņemt lēmumus savas profesionālās karjeras veidošanā. Spēja izmantot analītisku pieeju profesionālajā darbībā un profesionālās jomas attīstībā.	LKI 4. līmenis
5.8.	Pielietot matemātisko un kritisko domāšanu.	Lietot pamata matemātikas principus un paņēmienus. Matemātiski pamatot problēmu risinājumu. Lietot dažādas matemātiskās metodes (loģiskā domāšana un telpas uztvere) dažādos līmeņos. Veidot sakarības. Modelēt plānotā uzdevuma risinājuma gaitu.	**Priekšstata līmenī:** Zinātnes teorijas, kas saistītas ar IKT, cilvēk miejdarbību. Matemātisko modeļu konstrukti **Lietošanas līmenī:** Tehnoloģiskie produkti un procesi. Matemātikas praktiskā lietojamība. Matemātikas metodes un instrumenti.	Spēja attīstīt un piemērot matemātisko un tehnoloģisko domāšanu ikdienas problēmsituāciju risināšanā. Spēja piemērot matemātisko domāšanu, modelējot situācijas un plānojot darba uzdevuma izpildi.	LKI 4. līmenis

5. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā VISPĀRĒJĀ kompetence					
Nr.p.k.	**Uzdevumi**	**Prasmes**	**Profesionālās zināšanas**	**Kompetence (kvalifikācijas līmenis)**	
			Kritiskās domāšanas metodes un paņēmieni.		
5.9.	Iesaistīties uzņēmuma darbības attīstībā.	Veikt darba vadītāja uzdotos uzdevumus. Plānot uzticēto uzdevumu izpildi. Domāt radoši. Aktīvi iesaistīties jaunu ideju radīšanā, izrādot iniciatīvu. Sadarboties ar iesaistītajām pusēm. Patstāvīgi pieņemt lēmumus par problēmu risinājumiem konkrētās darba situācijās. Racionāli izmantot resursus.	**Izpratnes līmenī:** Uzņēmuma darba organizācija pamatprincipi **Lietošanas līmenī:** Ideju ģenerēšanas metodes. Lēmumu pieņemšanas teorijas, metodes un paņēmieni Radošās domāšanas metodes un paņēmieni. Inovāciju vadības pamatrpincipi.	Spēja aktīvi iesaistīties uzņēmuma darbības attīstībā, piedāvājot jaunas, racionālas idejas darba uzdevuma veikšanai.	LKI 4. līmenis

Vispārīga informācija	
Profesionālās kvalifikācijas prasību iesniedzējs	*Saldus tehnikums* **Kate Elizabete Kanasta -** Aizsardzības ministrijas Kiberdrošības politikas koordinācijas nodaļas vadītāja vietniece; **Sanita Vītola -** sistēmanalītiķis, CERT.LV; **Sintija Deruma -** LIKTA kiberizglītības drošības darba grupas eksperte; **Artis Ābolts -** ZS Kiberaizsardzības vienība 2.RAN (reģionālā atbalsta nodaļa); **Dagnis Bračs -** SIA Hollistic drošības speciālists; **Pauls Bračs -** SIA Hollistic drošības analītiķis; **Artūrs Jaunzems -** Saldus tehnikuma pedagogs; **Ingrīda Lazdāne** - Saldus tehnikuma izglītības metodiķe.
Profesionālās kvalifikācijas prasību ekspertu darba grupa	**Ksenija Tkačenko** – Ekonomikas ministrija, Uzņēmējdarbības konkurētspējas departamenta vecākā eksperte; **Matīss Veigurs** – Aizsardzības ministrija, Kiberdrošības politikas departamenta Eiropas Savienības kiberdrošības jautājumu nodaļas sistēmanalītiķis; **Pēteris Paikens** – Dr.sc.comp., Latvijas Universitātes Datorikas fakultātes asociētais profesors, RTU Riga Business School BITL programmas pasniedzējs, LZP eksperts datorzinātnēs; **Kirils Solovjovs** - Mg. sc. comp., Mg.phys., *Possible Security* uzņēmuma vadītājs; **Edmunds Beļskis -** Latvijas Informācijas un komunikācijas tehnoloģijas asociācijas (LIKTA) padomes loceklis un LIKTA kiberdrošības izglītības darba grupas vadītājs; **Elīna Auniņa** – Valsts izglītības satura centrs, Izglītības satura departamenta, Izglītības satura atbalsta nodaļas vecākā eksperte; **Inese Paudere** – Valsts izglītības satura centrs, Izglītības satura departamenta, Izglītības satura atbalsta nodaļas vecākā eksperte.
NEP atzinums par profesionālās kvalifikācijas prasībām	EIKT NEP 23.05.2024.
Profesionālās kvalifikācijas prasību saskaņošana PINTSA	07.08.2024.
Iepriekš saskaņoto profesionālās kvalifikācijas prasību redakcijas	-