

SASKAŅOTS

Profesionālās izglītības un nodarbinātības
trīspusējas sadarbības apakšpadomes
20.01.2026 sēdē, PINTSA protokols Nr.6
2025.gada 9.oktobrī.pdf

PROFESIJAS STANDARTS

**"Elektronisko un optisko iekārtu ražošana, informācijas un
komunikācijas tehnoloģija"**

PROFESIONĀLĀS KVALIFIKĀCIJAS PRASĪBAS

"Kiberdrošības tehniķis"

1. Profesionālās kvalifikācijas nosaukums, kvalifikācijas līmenis, prasības izglītībai	
"Kiberdrošības tehniķis"	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 datu	
Profesionālās kvalifikācijas specializācijas: Nav datu	
Saistītās profesionālās kvalifikācijas, kvalifikācijas līmenis: Datorsistēmu tehniķis (4.PKL) Programmēšanas tehniķis (4.PKL)	
3. Profesionālās darbības pienākumu un uzdevumu kopsavilkums	
Kiberdrošības tehniķis ir speciālists, kurš organizācijā atbildīgi veic uzticētos darba pienākumus, kas ietver organizācijas kiberdrošības risinājumu uzturēšanu, reaģēšanu uz kiberdrošības incidentiem un informācijas un komunikāciju tehnoloģiju sistēmu drošības testēšanu un ievainojamību ziņojumu apstrādi, nodrošinot datu apstrādi atbilstoši normatīvajiem regulējumiem, nozares prasībām un organizācijas noteiktajai kārtībai. Kvalifikācijas "Kiberdrošības tehniķis" 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 iespējamus uzlabojumus savas kompetences ietvaros. 3.1.6 Sniegt informāciju gala lietotājiem 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 izmantošana organizācijā (sistēmas, programmatūru, vadlīnijas un pakalpojumus). 3.3.1 Novērtēt organizācijas kiberdrošības risinājumus.	

3. Profesionālās darbības pienākumu un uzdevumu kopsavilkums

3.3.2 Apzināt tehniskās un funkcionālās prasības nepieciešamajam risinājumam.

3.3.3 Salīdzināt līdzvērtīgus tirgū pieejamos kibernetikas drošības risinājumus.

3.3.4 Kibernetikas drošības risinājumu ieviešana/uzstādīšana pēc iepriekš noteiktām instrukcijām.

3.3.5 Kibernetikas drošības risinājumu uzturēšana.

3.3.6 Apkopot risinājumu rezultātus rādījumus.

3.4 IKT sistēmu drošības testēšana.

3.4.1 Apzināties kibernetikas drošības testu tvērumu.

3.4.2 Iepazīties ar testa plānu.

3.4.3 Iepazīties ar testa scenāriju.

3.4.4 Veikt IKT drošības testēšanu atbilstoši scenārijiem.

3.4.5 Apstrādāt IKT drošības testu rezultātus.

3.4.6 Iepazīstināt tiešo vadītāju ar drošības testu rezultātiem.

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence (profesionālo zināšanu, prasmju, patstāvības un atbildības kopums)					
Nr.p. k.	Uzdevumi	Prasmes	Profesionālās zināšanas	Kompetence (kvalifikācijas līmenis)	
Organizācijas IKT vides un kiberdrošības prasību apzināšana.					
4.1.	Iepazīt organizācijas IKT vidi un drošības arhitektūru.	Apzināt organizācijas plānos iekļauto drošības pārvaldības aspektus.	Izpratne: 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. Lietošana: 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
		Identificēt organizācijā izmantotos tehnoloģiskos risinājumus.			
		Iepazīt organizācijas kiberdrošības prasības.			
		Iepazīties ar IKT infrastruktūras uzbūves shēmām.			
		Iepazīties ar organizācijas IKT dokumentāciju.			

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence (profesionālo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Uzdevumi	Prasmes	Profesionālās zināšanas	Kompetence (kvalifikācijas līmenis)	
4.2.	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.	Izpratne: Informācijas drošības standarti un labā prakse (Piemēram, ISO 27001, 27002, OWASP). Izprot kiberdrošības stratēģiju nacionālā līmenī. Lietošana: Kiberdrošības prasību labā prakse un standarti attiecībā uz incidentu pārvaldību (piemēram, ITIL).	Spēja patstāvīgi apzināt un apkopot organizācijas kiberdrošības prasības.	LKI 4. līmenis
4.3.	Iepazīt esošās kiberdrošības prasības.	Pielietot dažādus digitālos rīkus kiberdrošības prasību izvērtēšanas procesā.	Izpratne: Normatīvo aktu analīzes metodes un paņēmieni. Organizācijas kiberdrošības politika, procedūra, vadlīnijas, instrukcijas. Lietošana: Lēmumu pieņemšanas koki. Normatīvo aktu analīzes rīki. Metodes un rīki, kas atbalsta prasību apkopošanu un lēmumu pieņemšanu.	Spēja apkopot un analizēt esošās ārējās un iekšējās kiberdrošības prasības organizācijā.	LKI 4. līmenis
		Veikt ārējo un iekšējo kiberdrošības prasību apzināšanu.			

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence (profesionālo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Uzdevumi	Prasmes	Profesionālās zināšanas	Kompetence (kvalifikācijas līmenis)	
4.4.	Novērtēt esošo kiberdrošības prasību izpildi.	Izmantot novērtējuma kritēriju kopu.	Lietošana: Novērtējuma matricas.	Spēja novērtēt esošo kiberdrošības prasību izpildi organizācijā.	LKI 4. līmenis
		Pielietot novērtējuma matricas rezultātu apkopošanai.			
4.5.	Piedāvāt iespējamus uzlabojumus savas kompetences ietvaros.	Piedāvāt uzlabojumus, balstoties uz novērtējuma rezultātiem, savas kompetences ietvaros.	Lietošana: Pārmaiņu vadība. Izmaiņu pārvaldība.	Spēja piedāvāt nepieciešamos kiberdrošības uzlabojumus organizācijā.	LKI 4. līmenis
4.6.	Sniegt informāciju gala lietotājiem kiberdrošības prasību īstenošanas jautājumos.	Informēt saprotami un uztverami par kiberdrošības prasību īstenošanas pasākumiem.	Lietošana: 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
		Sniegt ar kiberdrošību saistīto tehnisko atbalstu gala lietotājiem.			

Reaģēšana uz kiberdrošības incidentiem.

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence (profesionālo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Uzdevumi	Prasmes	Profesionālās zināšanas	Kompetence (kvalifikācijas līmenis)	
4.7.	Kiberdrošības incidentu identificēšana.	Noteikt ietekmētos resursus. Apzināt ietekmētos resursus, lietotājus, iespējamus cēloņus.	Izpratne: Incidentu ap strādes standarti. Incidentu apstrādes rīki. Incidentu veidi/sadalījums. Lietošana: Incidentu priekšizpēte. Incidentu reģistrēšanas kritēriji. Incidentu reģistrēšanas rīki.	Spēja veikt incidentu ziņošanu saskaņā ar organizācijas incidentu apstrādes procedūrām.	LKI 4. līmenis
4.8.	Kiberdrošības incidentu klasificēšana.	Klasificēt kiberdrošības incidentus atbilstoši organizācijas izvēlētajai kritēriju kopai (uzbrukuma vektors, avots).	Lietošana: Apdraudējumu klasifikācija. Incidentu apstrādes kārtība organizācijā. Kiberuzbrukumu vektori, avoti.	Spēja patstāvīgi veikt incidentu klasifikāciju atbilstoši organizācijas norādījumiem.	LKI 4. līmenis
		Veikt kiberdrošības incidenta ietekmes novērtēšanu.			
4.9.	Kiberdrošības incidentu izpēte.	Analizēt dažādu žurnālu (tīklu, serveru, gala lietotāju sistēmu) ierakstus.	Izpratne: Incidentu reaģēšanas soļi. Iesaistītās puses, to atbildības. Dažādi ietekmes novērtējumu veidi (piem., organizācijai, datu subjektam, industrijai). Lietošana:	Spēja veikt kiberdrošības incidentu izpēti sadarbībā ar incidentu izpētē iesaistītajām pusēm.	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence (profesionālo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Uzdevumi	Prasmes	Profesionālās zināšanas	Kompetence (kvalifikācijas līmenis)	
		Analizēt IS apdraudējumus vai dažādas to kļūmes pēc žurnālu ierakstiem.	Operētājsistēmu darbība. Datu pārraides tīklu uzbūve un darbības principi. Dažādu sistēmu ievainojamības. Kiberdrošības uzbrukumu metodes. Žurnālu ierakstu apstrāde.		
		Veikt kiberdrošības incidentu izpēti.			
4.10.	Kiberdrošības incidentu un ar to saistītās informācijas apstrāde.	Apkopot digitālos pierādījumus, nodrošinot to integritāti.	Izpratne: SOC darbības pamatprincipi. Latvijas kiberdrošības atbildīgo institūciju hierarhija un to uzdevumi. Digitālās izmeklēšanas metodes un rīki. Krīzes reaģēšanas soļi. Lietošana: Incidentu apstrādes labā prakse. Digitālo pierādījumu dokumentēšana. Kiberdrošības incidentu reģistrs.	Spēja veikt kiberdrošības incidentu informācijas apstrādi.	LKI 4. līmenis
		Dokumentēt organizācijas kiberdrošības incidentus.			
		Sadarboties ar kiberdrošības incidentu novēršanā iesaistītajām pusēm.			
		Sniegt atbalstu incidenta ierobežošanā un novēršanā iesaistītajām pusēm.			

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence (profesionālo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Uzdevumi	Prasmes	Profesionālās zināšanas	Kompetence (kvalifikācijas līmenis)	
		Uzturēt aktuālu kiberdrošības incidentu reģistru.		Spēja sekot organizācijas noteiktajai incidentu apstrādes kārtībai un sadarboties ar incidenta reaģēšanā iesaistītajām pusēm.	LKI 4. līmenis
		Ziņot par drošības incidentiem saskaņā ar organizācijas drošības politikas vadlīnijām, incidentu apstrādes procedūrām.			
4.11.	Pēc-incidenta datu apkopošana.	Apkopot informāciju pēc-incidenta ziņojumiem.	Izpratne: Incidentu pārvaldības process. Kiberdrošības saistošā likumdošana un tiesību akti. Lietošana: Incidentu reģistrēšanas rīki. Incidentu ziņojumu analīze.	Spēja apkopot informāciju pēc-incidenta ziņojuma sagatavošanai.	LKI 4. līmenis
		Piedalīties incidentu reaģēšanas aktivitāšu apkopšanā.		Spēja apkopot incidenta reģistra datus/veiktos pasākumus incidenta reaģēšanas aktivitāšu izvērtēšanai.	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence (profesionālo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Uzdevumi	Prasmes	Profesionālās zināšanas	Kompetence (kvalifikācijas līmenis)	
4.12.	Pēc-incidenta rezultātu apkopošana un uzlabojumu ieteikšana.	Piedalīties incidentu reaģēšanas aktivitāšu uzlabojumu identificēšanā.	Lietošana: Incidentu reaģēšanas labā prakse. Incidentu apstrādes kārtība organizācijā. Incidentu reaģēšanas vadlīnijas un standarti.	Spēja veidot pēc-incidenta ziņojumus reaģēšanā iesaistītajām pusēm.	LKI 4. līmenis
		Sniegt pēc-incidenta analīzes apkopotos rezultātus iesaistītajām pusēm.		Spēja identificēt potenciālos incidentu reaģēšanas uzlabojumus.	LKI 4. līmenis
Kiberdrošības risinājumu izmantošana organizācijā (sistēmas, programmatūru, vadlīnijas un pakalpojumus).					
4.13.	Novērtēt organizācijas kiberdrošības risinājumus.	Identificēt kiberdrošības risinājumu iespējamus uzlabojumus.	Izpratne: Kiberdrošības standarti un ietvari. Kiberhigiēnas pamatprincipi. Kiberdrošības risinājumu tehniskās prasības. Lietošana: 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 novērtēt organizācijas kiberdrošības risinājumus.	LKI 4. līmenis
		Izvērtēt esošos kiberdrošības risinājumu atbilstību organizācijas identificētajām (iekšējām un ārējām) prasībām.		Spēja identificēt iespējamus kiberdrošības risinājumu uzlabojumus.	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence (profesionālo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Uzdevumi	Prasmes	Profesionālās zināšanas	Kompetence (kvalifikācijas līmenis)	
4.14.	Apzināt tehniskās un funkcionālās prasības nepieciešamajam risinājumam.	Noskaidrot kiberdrošības risinājumu tehniskās prasības.	Izpratne: Infrastruktūras arhitektūras prasības. Simetriskās un asimetriskās šifrēšanas darbības pamatprincipi un algoritmi. Tehniskās dokumentācijas avoti. Tehniskā terminoloģija. Lietošana: Tehniskās dokumentācijas analīze.	Spēja apzināt tehniskās un funkcionālās prasības nepieciešamajam risinājumam.	LKI 4. līmenis
		Noskaidrot kiberdrošības risinājumu funkcionālās prasības.			
4.15.	Salīdzināt līdzvērtīgus tirgū pieejamos kiberdrošības risinājumus.	Apzināt iespējamus kiberdrošības risinājumus.	Lietošana: Tehniskās dokumentācijas interpretācija. Risinājumu licencēšanas prasību izvērtēšana.	Spēja salīdzināt līdzvērtīgus tirgū pieejamos kiberdrošības risinājumus.	LKI 4. līmenis
		Salīdzināt iespējamus kiberdrošības risinājumus.			
4.16.	Kiberdrošības risinājumu ieviešana/uzstādīšana pēc iepriekš noteiktām instrukcijām.	Integrēt kiberdrošības risinājumus organizācijas infrastruktūrā.	Izpratne: Drošas programmatūras izstrādes dzīvescikls. Lietošana:	Spēja uzstādīt/ieviest atbilstošākos kiberdrošības risinājumus organizācijas drošības arhitektūrā (infrastruktūra, procesi,	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence (profesionālo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Uzdevumi	Prasmes	Profesionālās zināšanas	Kompetence (kvalifikācijas līmenis)	
		Uzstādīt datu pārraides tīklu drošības sistēmas(ugunsmūrus, IDS, IPS u.c.).	Skriptu (īsu programmu) veidošana (piem. Python, Bash).	dati u.c.) pēc iepriekš noteiktām instrukcijām.	
		Uzstādīt gala ierīču drošības sistēmas (anti-vīrusi, ugunsmūri u.c.).			
4.17.	Kiberdrošības risinājumu uzturēšana.	Ieviest izmaiņas kiberdrošības tehniskajos risinājumos savas kompetences ietvaros.	Izpratne: Organizācijas kiberdrošības procedūras un kontroles. Lietošana: 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.	LKI 4. līmenis
		Konfigurēt sistēmas un servissus atbilstoši kiberdrošības prasībām savas kompetences ietvaros.		Spēja ieviest izmaiņas esošajā infrastruktūrā atbilstoši organizācijas kiberdrošības prasībām.	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence (profesionālo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Uzdevumi	Prasmes	Profesionālās zināšanas	Kompetence (kvalifikācijas līmenis)	
4.18.	Apkopot risinājumu rezultātīvos rādījumus.	Interpretēt kiberdrošības risinājumu rezultātīvos rādītājus sadarbībā ar citiem speciālistiem.	Izpratne: Organizācijas kiberdrošības politika, procedūra, vadlīnijas, instrukcijas. Lietošana: Drošas IS darbības principi. Virtuālais privātais tīkls (VPN) darbības principi. Konfigurācijasfailu izveide un analīze. Drošības bāzes līnijas (Security baseline). Kiberdrošības kontroļu novērtēšanas paņēmieni.	Spēja sagatavot kiberdrošības risinājumu rezultātu apkopojumu tālākai analīzei.	LKI 4. līmenis
		Nodrošināt kiberdrošības risinājumu rezultātīvo rādītāju apkopošanu atbilstoši noteiktajiem uzdevumiem.		Spēja interpretēt no risinājumiem iegūtos rezultātus.	LKI 4. līmenis
IKT sistēmu drošības testēšana.					
4.19.	Apzināties kiberdrošības testu tvērumu.	Iepazīties ar kiberdrošībastesta tvērumā iekļaujamajām IKT komponentēm un atļautajām metodēm.	Izpratne: Informācijas sistēmu uzbūve. Operētājsistēmu arhitektūra un darbības principi. Drošības testēšanas standarti un ietvari. Lietošana: Operētājsistēmu drošība. Datu pārraides tīklu uzbūve un darbība, tīklu drošība.	Spēja iepazīties ar noteiktiem kiberdrošības testu uzdevumiem.	LKI 4. līmenis
		Iepazīties ar noteiktiem kiberdrošības testu uzdevumiem.		Spēja apzināt kiberdrošības testu tvērumā iekļautās IKT komponentes.	LKI 4. līmenis

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence (profesionālo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Uzdevumi	Prasmes	Profesionālās zināšanas	Kompetence (kvalifikācijas līmenis)	
4.20.	Iepazīties ar testa plānu.	Izvēlēties piemērotas drošības testēšanas metodes un rīkus savas kompetences ietvaros.	Izpratne: Testēšanas standarti un vadlīnijas. Testēšanas ietekmes apzināšana uz testējamajām IKT komponentēm. Lietošana: 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 noteiktu iespējamās kiberuzbrukumu vektorus.	LKI 4. līmenis
		Noteikt iespējamās kiberuzbrukumu vektorus, kas attiecas uz testējamajām IKT komponentēm.			
4.21.	Iepazīties ar testa scenāriju.	Iepazīstas ar kiberdrošības scenāriju atbilstoši kiberdrošībastesta plānam.	Izpratne: Datu pārraides tīklu darbība. Informācijas sistēmu uzbūve. Sociālās inženierijas metodes un paņēmieni. Lietošana: Scenāriju izstrādes procedūras, izmaiņu pārvaldība. Kiberuzbrukumu metodes. Tīmekļa aplikāciju uzbūve. Kiberdrošības risinājumi.	Spēja apgūt testa scenārijus un pēc nepieciešamības pielāgot tos aktuālajai situācijai.	LKI 4. līmenis
		Veikt izpildāmo testēšanas scenāriju pielāgošanu aktuālajai situācijai, ja tas ir nepieciešams.			

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence (profesionālo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Uzdevumi	Prasmes	Profesionālās zināšanas	Kompetence (kvalifikācijas līmenis)	
4.22.	Veikt IKT drošības testēšanu atbilstoši scenārijiem.	Identificēt sistēmu drošības ievainojamības.	Lietošana: 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
		Izmantot drošības testēšanas rīkus un testa programmas.			
		Secīgi izpildīt testus/testēšanas plānu, veicot starprezultātu izvērtējumu.			
		Veikt testēšanas plāna un izpildāmo scenāriju pielāgošanu.			
4.23.	Apstrādāt IKT drošības testu rezultātus.	Dokumentēt drošības testēšanas rezultātus.	Izpratne: Organizācijas biznesa procesi. Kiberdrošības risku klasifikācija. Lietošana: 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.	LKI 4. līmenis
		Gatavot rekomendācijas organizācijas drošības ievainojamību novēršanai.			

4. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā PROFESIONĀLĀ kompetence (profesionālo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Uzdevumi	Prasmes	Profesionālās zināšanas	Kompetence (kvalifikācijas līmenis)	
		Novērtēt testēšanas laikā atklāto konfigurācijas nepilnību un drošības ievainojamību kritiskumu, ņemot vērā ietekmi uz organizācijas kiberdrošību.		Spēja sagatavot rekomendācijas identificēto ievainojamību novēršanai, sistēmu un servisu kiberdrošības uzlabošanai.	LKI 4. līmenis
4.24.	Iepazīstināt tiešo vadītāju ar drošības testu rezultātiem.	Demonstrēt IKT drošības ievainojamības izmantošanu.	<i>Izpratne:</i> Kiberrisku apstrādes stratēģijas. Drošības kontroļu klasifikācija dažādos standartos. Testa ziņojumu veidnes. <i>Lietošana:</i> Kiberriska ietekmes un varbūtības kvalitatīva un kvantitatīva analīze.	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
		Skaidrot IKT drošības testu rezultātus ieinteresētajām pusēm.			

5. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā VISPĀRĒJĀ kompetence (vispārējo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Kompetenču joma	Prasmes	Vispārējās zināšanas	Kompetence (kvalifikācijas līmenis)	
5.1.	Valsts valoda.	Ievērot latviešu literārās valodas normas lietišķajā saziņā.	Izpratne: Vārdu krājums. Gramatika un valodas funkcija. Valodas kultūra. Valodas stili un intonācija Verbālās un neverbālās mijiedarbības veidi. Lietošana: Valsts valoda. Nozares terminoloģija.	Spēja izteikt un interpretēt jēdzienus, domas, faktus un viedokli gan mutiski, gan rakstiski valsts valodā.	LKI 4. līmenis
		Lietot valsts valodā profesionālo terminoloģiju.			
		Sazināties mutvārdos un rakstveidā dažādās profesionālās situācijās valsts valodā.			
5.2.	Daudzvalodu kompetence (t.sk. kultūras izpratnes un izpausmes kompetence).	Lietot profesionālo terminoloģiju svešvalodā.	Izpratne: Vārdu krājums. Gramatika un valodas funkcija. Verbālās un neverbālās mijiedarbības veidi. Valodas komunikācijas konteksts. Lietošana: Svešvalodas lietošana. Starpkultūru mijiedarbība. Nozares terminoloģija.	Spēja toleranti komunicēt multikulturālā vidē, ievērojot starpkultūru komunikācijas principus.	LKI 4. līmenis
		Sazināties ar dažādām sociālām grupām multikulturālā vidē.		Spēja izteikt viedokli gan mutiski, gan rakstiski svešvalodā, lietojot profesionālo terminoloģiju.	LKI 4. līmenis
		Sazināties mutvārdu un rakstveida komunikācijā svešvalodā.			

5. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā VISPĀRĒJĀ kompetence (vispārējo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Kompetenču joma	Prasmes	Vispārējās zināšanas	Kompetence (kvalifikācijas līmenis)	
5.3.	Matemātiskā kompetence un kompetence dabaszinātnēs, tehnoloģijās un inženierzinātnēs.	Identificēt zinātniski tehnoloģiskos pētījumus nozarē.	Izpratne: Dabaszinātņu, tehnoloģiju un inženierzinātņu jēdzieni un teorijas. Nozares tehnoloģiju attīstības virzieni. Lietošana: Nozares tehnoloģiju attīstības virzieni. Mērvienības un formas. Matemātikas instrumenti un metodes. Matemātikas terminoloģija. Statistikas elementi. Algebriskās izteiksmes. Analītiskā ģeometrija. Telpiski ķermeņi.	Spēja izmantot matemātisko domāšanu, metodes, izteiksmes un sakarības modelējot darba situācijas un uzdevumu izpildi.	LKI 4. līmenis
		Lietot matemātiskas metodes, izteiksmes un sakarības darba uzdevumu veikšanā.			
		Modelēt plānotā uzdevuma risinājuma gaitu.		Spēja izmantot zinātnisko pētījumu rezultātus, likumsakarības un tehnoloģiskās attīstības sasniegumus savā profesionālajā darbībā.	LKI 4. līmenis
		Novērtēt nozares tehnoloģiskās attīstības virzienus, sasaistot to ar savu profesionālo darbību.			
5.4.	Digitālā kompetence.	Ievērot informācijas tehnoloģiju drošības un personas datu aizsardzības prasības.	Izpratne: Datora un biroja tehnikas darbības principi. Lietošana: Īpašuma tiesību un personas datu aizsardzības pamatprincipi.	Spēja droši lietot informācijas un komunikācijas tehnoloģijas profesionālajā darbā, ievērojot programmatūras licences nosacījumus,	LKI 4. līmenis

5. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā VISPĀRĒJĀ kompetence (vispārējo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Kompetenču joma	Prasmes	Vispārējās zināšanas	Kompetence (kvalifikācijas līmenis)	
		Lietot informācijas un komunikācijas tehnoloģijas profesionālajā darbībā.	Informācijas un komunikācijas tehnoloģiju lietošana. Informācijas un komunikācijas sistēmu drošība. Datu apstrāde un drošība. Mākslīgā intelekta rīki.	intelektuālā īpašuma un personas datu aizsardzību.	
		Sagatavot profesionālā darba saturu, izmantojot lietojumprogrammas.		Spēja veidot digitālo saturu atbilstoši profesionālās darbības specifikai, ievērojot iespējamās drošības riskus.	LKI 4. līmenis
		Strādāt ar digitālām un analogām sistēmām.			
5.5.	Uzņēmējdarbības kompetence.	Iesaistīties jaunu ideju radīšanā, izrādot iniciatīvu. Izvērtēt ekonomiskos riskus un darba prioritātes.	Darba vides organizācijas process. Pašorganizēts darba process. Komandas darba organizēšana. Lēmumu pieņemšanas metodes. Plānošana metodes. Pašnovērtējuma mehānismi. Dokumentu noformēšanas prasības. Sadarbības principi. Priekšstats: Uzņēmējdarbības pamati. Normatīvie akti darbības jomā. Izpratne:	Spēja plānot un sekot līdzi darba izpildes termiņiem un kvalitātei, sabalansējot darba apjomu, laiku un racionālu resursu izmantošanu.	LKI 4. līmenis

5. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā VISPĀRĒJĀ kompetence (vispārējo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Kompetenču joma	Prasmes	Vispārējās zināšanas	Kompetence (kvalifikācijas līmenis)	
		Organizēt savu un komandas darbu kvalitatīvai uzdevumu izpildei.	Komercdarbības veidi. Tirgzinības pamati. Ekonomiskie resursi. Ekonomisko risku novērtēšana. Ilgtspējīgas ekonomikas pamatprincipi.	Spēja organizēt komandas darbu, izvērtējot ekonomiskos riskus un pieņemot pamatotus lēmumus atbilstoši savai kompetencei.	LKI 4. līmenis
		Pieņemt lēmumu par problēmu risinājumu savas kompetences ietvaros konkrētā situācijā.		Spēja aktīvi iesaistīties uzņēmuma darbības attīstībā, piedāvājot jaunas, racionālas idejas uzņēmuma efektivitātes paaugstināšanai.	LKI 4. līmenis
		Plānot darba apjomu, laiku un racionālu resursu izmantošanu.			
5.6.	Pilsoniskuma kompetence (t.sk. sociālā kompetence).	Apzināties pilsoniskas sabiedrības lomu un savu iesaisti demokrātijas attīstībā.	Priekšstats: Starptautiskie cilvēktiesību dokumenti. Izpratne: Latvijas Republikas valstiskums un tā juridiskais ietvars.	Spēja pildīt pilsoniskos pienākumus, nodrošinot sabiedrības tiesību ievērošanu.	LKI 4. līmenis

5. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā VISPĀRĒJĀ kompetence (vispārējo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Kompetenču joma	Prasmes	Vispārējās zināšanas	Kompetence (kvalifikācijas līmenis)	
		Ievērot vispārējās un profesionālās ētikas normas.	Sabiedrība un tās attīstības virzieni. Tiesiskās attiecības. Sociālā dialoga būtība un sadarbības mehānismi. Efektīvas komunikācijas priekšnoteikumi. Sabiedrības ilgtspējas koncepcija. Lietošana: Indivīda tiesības, pienākumi un atbildība. Vispārējās un profesionālās ētikas pamatprincipi. Sabiedrības sociālā un politiskā struktūra. Sabiedrības labklājības izpausmes/rādītāji/ kritēriji. Pozitīvas saskarsmes paņēmieni.	Spēja apzināti piedalīties pilsoniskajā un sabiedriskajā dzīvē, balstoties uz izpratni par sociālajiem un politiskajiem konceptiem.	LKI 4. līmenis
		Pildīt pilsoniskos pienākumus.			
		Saskatīt dažādu sabiedrības jomu un parādību saistību ar morāli un tikumību.		Spēj iesaistīties demokrātiskā lēmumu pieņemšanā un pilsoniskās aktivitātēs ilgtspējīgai attīstībai.	LKI 4. līmenis
		Uzņemties atbildību par sava dzīvesveida kvalitāti.			
		Veidot mijiedarbību ar citiem cilvēkiem, respektējot sabiedrības daudzveidību un vienlīdzību.			
5.7.	Personīgā un mācīšanās mācīties kompetence.	Apgūt jaunas prasmes karjeras izaugsmei.	Izpratne: Faktu, teoriju un profesionālās darbības procesu likumsakarības. Profesionālās karjeras izaugsme.	Spēja novērtēt savu profesionālo pieredzi un mērķtiecīgi plānot	LKI 4. līmenis

5. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā VISPĀRĒJĀ kompetence (vispārējo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p. k.	Kompetenču joma	Prasmes	Vispārējās zināšanas	Kompetence (kvalifikācijas līmenis)	
		Mērķtiecīgi plānot profesionālo kompetenču pilnveidi.	<i>Lietošana:</i> Pašnovērtējuma mehānismi. Mācīšanās stratēģijas. Mācību un karjeras plānošana. Laika pārvaldības pamatprincipi. Karjeras attīstības novērtēšanas principi.	profesionālo kompetenču pilnveidi.	
		Novērtēt savas personīgās un sociālās attīstības iespējas.		Spēja apzināti mācīties tālāk, pilnveidojot savas profesionālās kompetences.	LKI 4. līmenis
		Novērtēt savu profesionālo pieredzi un profesionālās kompetences izaugsmes iespējas.			
5.8.	Darba tiesības un darba aizsardzība (t.sk. ugunsdrošība, elektrodrošība), vides aizsardzība (t.sk. zaļās prasmes) un civilā aizsardzība.	Atbildīgi rīkoties ārkārtas gadījumā.	<i>Priekšstats:</i> Darba aizsardzības sistēma. Vides aizsardzības sistēma. Civilās aizsardzības sistēma. <i>Izpratne:</i> Darba tiesiskās attiecības. Darba vides riska faktori to novērtēšanas metodes. Aizsardzības pasākumi darba vides faktoru ietekmes uz veselību mazināšanā. <i>Lietošana:</i> Darba tiesību normatīvie akti. Darba koplīgums. Darba līgums.	Spēja nodibināt darba tiesiskās attiecības un ievērot ārējo un organizācijas iekšējo normatīvo aktu prasības.	LKI 4. līmenis
		Ievērot darba tiesiskās attiecības.			
		Ievērot nozares saistošo normatīvo aktu prasības un organizācijas iekšējās kārtības noteikumus.		Spēja ievērot darba un vides aizsardzības, elektrodrošības, ugunsdrošības un civilās aizsardzības prasības,	LKI 4. līmenis
		Īstenot videi draudzīgu dzīvesveidu atbilstoši "zaļās domāšanas" principiem.			

5. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā VISPĀRĒJĀ kompetence (vispārējo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p.k.	Kompetenču joma	Prasmes	Vispārējās zināšanas	Kompetence (kvalifikācijas līmenis)	
		Lietot ABC shēmu kritisku veselības stāvokļu novērtšanai, dzīvības saglabāšanai un uzturēšanai.	Darba aizsardzības noteikumi. Darba vides riska faktoru novērtšanas preventīvie pasākumi. Drošības signāli un zīmes. Darba aizsardzības līdzekļi un to lietošana. Rīcība darba vides risku iestāšanās gadījumā. Ergonomikas prasības. Ugunsdrošības noteikumi. Rīcība ugunsgrēka gadījumā. Elektrodrošības noteikumi. Vides aizsardzības noteikumi. Civilās aizsardzības noteikumi. Rīcība ārkārtas gadījumos. Pirmās palīdzības sniegšana. "Zaļās domāšanas" principi. Ilgtspējīgas attīstības principi. Veselīga prāta, ķermeņa un dzīvesveida komponentes.	atbildīgi veicot profesionālos darba uzdevumus individuāli un komandā.	
		Novērtēt darba vides riska faktorus un to ietekmi uz veselību savas kompetences ietvaros.		Spēja kritiski novērtēt darba vides riska faktorus un novērst tos savas kompetences ietvaros.	LKI 4. līmenis
		Organizēt darbu atbilstoši darba aizsardzības, ugunsdrošības, elektrodrošības un vides aizsardzības prasībām.		Spēja atbildīgi rīkoties ārkārtas gadījumā un sniegt pirmo palīdzību.	LKI 4. līmenis
		Piemērot ergonomikas prasības darba vides iekārtošanai droša darba veikšanai.		Spēja izvērtēt problēmas un rīcību, balstoties uz ilgtspējas vērtībām un principiem.	LKI 4. līmenis

5. Profesionālās darbības pienākumu un uzdevumu izpildei nepieciešamā VISPĀRĒJĀ kompetence (vispārējo zināšanu, prasmju, patstāvības un atbildības kopums)

Nr.p.k.	Kompetenču joma	Prasmes	Vispārējās zināšanas	Kompetence (kvalifikācijas līmenis)	
		Raksturot ilgtspēju kā jēdzienu, kas ietver vides, ekonomikas, sociālos un kultūras aspektus.		Spēja apzināti īstenot videi draudzīgu dzīvesveidu atbilstoši "zaļās domāšanas" principiem, nodrošinot sabiedrības ilgtspēju.	LKI 4. līmenis
		Rīkoties atbilstoši ilgtspējīgas attīstības principiem.			

Vispārīga informācija	
Iesniedzējs	Moderators
Iesniegums	Nav datu
Nozares ekspertu padomes, nozares ministrijas vai tās deleģētas institūcijas vai piesaistīto nozares ekspertu atzinums	Nav datu
Saskaņojums PINTSA	20.01.2026
Iepriekš saskaņotā redakcija	Nav datu