Saskaņots PINTSA sēdē 2014.gada 16.aprīlī

Informācijas drošības vadītāja profesijas standarts

1. Vispārīgie jautājumi

1. Profesijas nosaukums – informācijas drošības vadītājs.
2. Profesijas kods – 1330 09.

2. Nodarbinātības apraksts

1. Profesionālās kvalifikācijas līmenis – piektais profesionālās kvalifikācijas līmenis.
2. Profesionālās darbības pamatuzdevumu kopsavilkums:

– informācijas drošības vadītājs organizē un vada informācijas drošības pārvaldības sistēmas (stratēģija, arhitektūra/struktūra pārvaldības sistēmai, kā arī pasākumu, iekšējo normatīvo aktu, ar tiem saistīto procesu kopums) plānošanu, īstenošanu un uzraudzību.

Informācijas drošības vadītājs strādā gan valsts un pašvaldību iestādēs, gan uzņēmumos jebkurā tautsaimniecības nozarē.

3. Profesionālās darbības veikšanai nepieciešamās profesionālās kompetences

1. Spēja izstrādāt informācijas drošības pārvaldības struktūru/arhitektūru, t.sk. aprakstīt atbildīgo personu lomas, pienākumus, atbildības.
2. Spēja izstrādāt, analizēt, kontrolēt un koriģēt informācijas drošības pārvaldības īstermiņa un ilgtermiņa plānus.
3. Spēja noteikt un uzraudzīt mērījumus (indikatorus, rādītājus, metrikas) informācijas drošības pārvaldības sasniedzamo rezultātu novērtēšanai.
4. Spēja analizēt un novērtēt sasniegtos rezultātus, pieņemt lēmumus un korekcijas operatīvās un stratēģiskās darbības optimizēšanai.
5. Spēja identificēt informācijas drošības ievainojamības, draudus, novērtēt un aprēķināt apdraudējuma ietekmi, noteikt varbūtību.
6. Spēja prognozēt urķu uzbrucēja taktiku, izstrādāt riska realizēšanās scenārijus.
7. Spēja orientēties informācijas drošības pārvaldības un informācijas un komunikāciju tehnoloģiju (IKT) normatīvo aktu prasībās un starptautiskajos standartos, kā arī informācijas drošības jomas vispārpieņemtajā praksē.
8. Spēja izvērtēt, apkopot, atlasīt un adaptēt minimālās drošības prasības informācijas komunikāciju tehnoloģijām, pakalpojumiem un projektiem.
9. Spēja analizēt un novērtēt informācijas drošības līmeni, izstrādāt priekšlikumus informācijas drošības līmeņa uzlabošanai.
10. Spēja orientēties uzņēmuma darbības nepārtrauktības procesos un nodrošināt informācijas sistēmu atjaunošanas pasākumu plānošanu un uzraudzību.
11. Spēja izstrādāt ārkārtas situācijas rīcības scenārijus un vadīt personālu ārkārtas situācijās.
12. Spēja sadarboties, komunicēt, konsultēt, skaidrot un argumentēt informācijas drošības pārvaldības mērķus un rezultātus ieinteresētajām pusēm, ievērojot profesionālās un vispārējās ētikas pamatprincipus.
13. Spēja vadīt apmācības, izstrādāt to saturu, novērtēt zināšanu līmeni informācijas drošības, fizisko personu datu aizsardzības un saistītajos jautājumos.
14. Spēja organizēt uzņēmuma struktūrvienības racionālu un saskaņotu darbību, motivēt un kontrolēt sev pakļautā personāla pienākumu izpildi.
15. Spēja ieviest progresīvus risinājumus un metodes informācijas drošības efektivitātes veicināšanai.
16. Spēja nodrošināt darba aizsardzības, ugunsdrošības un vides aizsardzības normatīvo aktu prasības.
17. Spēja nodrošināt darba tiesisko attiecību normu ievērošanu.
18. Spēja sazināties valsts valodā un vismaz divās svešvalodās.

19. Spēja veikt pētījumus un prezentēt iegūtos rezultātus.

4. Profesionālās darbības pamatuzdevumu veikšanai nepieciešamās prasmes

1. Veikt informācijas drošības risku analīzi.
2. Izstrādāt un vadīt uzņēmuma informācijas drošības pasākumus.
3. Veikt drošības pasākumu plānošanu un drošības plāna vadīšanu.
4. Vadīt datu aizsardzības un informācijas drošības pasākumus.
5. Izstrādāt un uzturēt ar informācijas drošību saistītos dokumentus un iekšējos normatīvos aktus.
6. Kontrolēt informācijas drošības pasākumu izpildi un nodrošināt kontroles rezultātu izmantošanu drošības uzlabošanā.
7. Pieņemt lēmumus par informācijas drošības risku pārvaldības pasākumu plāna izmaiņu nepieciešamību.
8. Nodrošināt efektīvu informācijas drošības pasākumu plāna izpildes gaitu.
9. Vadīt IKT pārbaudes un izmeklēšanas procesus uzņēmumā.
10. Apkopot un analizēt datus, izmantot modernās IKT darbības plānošanai, kontrolei un koriģēšanai.
11. Sagatavot pārskatus par informācijas drošības pasākumu plāna izpildi.
12. Izstrādāt ar drošību saistītus projektus un piedalīties to vadīšanā.
13. Vērtēt informācijas drošības attīstības projektu efektivitāti.
14. Pārzināt un pielietot risku identificēšanas, novērtēšanas un novēršanas metodes.
15. Izmantot nozares drošības standartus faktu vērtēšanā un analīzē un vispārpieņemto praksi informācijas drošības pārvaldības jomā.
16. Veikt uzņēmuma darbinieku apmācību par informācijas drošības jautājumiem.
17. Lietot modernās informācijas tehnoloģijas, savas darbības veikšanai.
18. Izmantot secinājumu veidošanas loģiskās metodes.
19. Vadīt padoto personālu.
20. Strādāt komandā.
21. Veikt darbu patstāvīgi, plānot izpildāmos darbus un noteikt to prioritātes.
22. Noformēt lietišķos dokumentus.
23. Ievērot profesionālās un vispārējās ētikas pamatprincipus.
24. Formulēt problēmas un to cēloņus, dot uzdevuma nostādni.
25. Veikt zinātnisko un pētniecisko darbu un pētījumu rezultātus ieviest praksē.
26. Sagatavot prezentācijas un uzstāties ar ziņojumiem par profesionāliem jautājumiem konferencēs, semināros, sanāksmēs.
27. Pārvaldīt valsts valodu.
28. Pārvaldīt vismaz divas svešvalodas saziņas līmenī.
29. Lietot profesionālo terminoloģiju valsts valodā un vismaz divās svešvalodās.
30. Patstāvīgi pilnveidot profesionālās zināšanas.
31. Ievērot darba tiesisko attiecību normas.
32. Ievērot darba aizsardzības, ugunsdrošības un vides aizsardzības normatīvo aktu prasības.

5. Profesionālās darbības pamatuzdevumu veikšanai nepieciešamās zināšanas

1. Profesionālās darbības pamatuzdevumu veikšanai nepieciešamās zināšanas priekšstata līmenī:
1.1. informācijas drošības arhitektūra;
1.2. programmatūras izstrādes dzīvescikls;
1.3. kvalitatīvās un kvantitatīvās pētniecības metodes informācijas drošības jomā;
1.4. finanšu ekonomikas pamati;
1.5. inovācijas informācijas un komunikāciju tehnoloģiju jomā;
1.6. IKT pakalpojumu pārvaldība;
1.7. kibernoziegumu analīze;
1.8. kriptogrāfija (sertifikāti un paraksti).

2. Profesionālās darbības pamatuzdevumu veikšanai nepieciešamās zināšanas izpratnes līmenī:
2.1. IKT infrastruktūras aizsardzība;
2.2. informācijas drošības tiesiskais regulējums;
2.3 privātuma un personas datu aizsardzība;
2.4. kritiskās infrastruktūras tiesiskais regulējums un standarti;
2.5. informācijas analīzes metodes;
2.6. pamatdarbības procesu ietekmes analīze;
2.7. informācijas resursu klasifikācija, metodes, labā prakse;
2.8. organizācijas pamatdarbības procesu nepārtrauktība;
2.9. vispārējā kvalitātes vadība;
2.10. iekšējo normatīvo aktu izstrādes metodoloģija;
2.11. modernās apmācības metodes;
2.12. kibernoziegumu izmeklēšanas process un pierādījumu vākšana;
2.13. kiberuzbrukuma atvairīšanas un aizsardzības taktikas un tehnoloģijas;
2.14. ārkārtas situāciju pārvaldība un krīzes komunikācijas stratēģijas;
2.15. informācijas drošības tehnoloģijas un risinājumi;
2.16. fiziskās piekļuves kontroles un perimetra aizsardzība;
2.17. sociālā inženierija;
2.18. lietvedība;
2.19. personāla vadība;
2.20. profesionālie termini valsts valodā un divās svešvalodās.

3. Profesionālās darbības pamatuzdevumu veikšanai nepieciešamās zināšanas lietošanas līmenī:
3.1. incidentu pārvaldība;
3.2. komercdarbības vadības teorijas;
3.3. lietišķā komunikācija un prezentēšanas prasmes;
3.4. informācijas drošības pārvaldība;
3.5. informācijas drošību standarti un labā prakse;
3.6. risku pārvaldības metodoloģijas, standarti un labā prakse;
3.7. kiberdrošība;
3.8. informācijas drošības un informācijas drošības pārvaldības izmērāmie rādītāji;
3.9. stratēģiskā vadība;
3.10. vadības psiholoģija;
3.11. lēmumu pieņemšana, argumentācijas māksla;
3.12. IKT projektu pārvaldība;
3.13. saskarsme, profesionālās un vispārējās ētikas pamatprincipi;
3.14. prezentācijas prasme;
3.15. pētnieciskā darba metodes;
3.16. valsts valoda;
3.17. divas svešvalodas saziņas līmenī;
3.18. darba aizsardzība un ergonomika;
3.19. vides aizsardzība;
3.20. darba tiesiskās attiecības.

Profesijas standarta „ Informācijas drošības vadītāja" pienākumi un uzdevumi:

Pienākumi	Uzdevumi
1. Organizācijas informācijas drošības pārvaldības sistēmas plānošana.	1.1. Novērtēt organizācijas informācijas resursu aizsardzības vajadzības. 1.2. Noteikt informācijas drošības pārvaldības stratēģiskos mērķus. 1.3. Izstrādāt un aktualizēt nepieciešamos iekšējos normatīvos aktus. 1.4. Ieviest informācijas drošības pārvaldības sistēmas iekļaušanu organizācijas (biznesa) procesos.

	1.5. Nodrošināt organizācijas vadības atbalstu un iesaisti informācijas drošības pārvaldībā. 1.6. Izstrādāt informācijas drošības pārvaldības sistēmas arhitektūru, noteikt atbildīgo personu lomas un pienākumus. 1.7. Izstrādāt informācijas drošības pārvaldības kvalitātes vērtēšanas kritērijus un izmērāmos rādītājus. 1.8. Pārzināt un piemērot IKT nozares normatīvajos aktos noteiktās prasības. 1.9. Koordinēt informācijas drošības pārvaldības sistēmas atbilstību ārējiem, nozares starptautiskajiem normatīvajiem aktiem.
2. Informācijas drošības risku pārvaldība.	2.1. Koordinēt informācijas resursu klasifikācijas izstrādes procesu. 2.2. Izstrādāt informācijas drošības risku analīzes metodiku. 2.3. Koordinēt informācijas drošības risku pārvaldības procesu. 2.4. Organizēt komunikāciju par informācijas drošības riskiem ar visām ieinteresētajām pusēm.
3. Informācijas drošības pasākumu ieviešana, īstenošana un uzraudzība.	3.1. Izstrādāt, īstenot un ieviest informācijas drošības pārvaldības īstermiņa un ilgtermiņa plānus, programmas. 3.2. Informēt un skaidrot organizācijas informācijas drošības pārvaldības mērķus un rezultātus. 3.3. Izstrādāt un īstenot informācijas drošības izpratnes veicināšanas kampaņas/apmācību programmas, veikt zināšanu novērtēšanu. 3.4. Nodrošina aktīvu dalību krīzes, ārkārtas situācijas, biznesa nepārtrauktības pārvaldības plānošanā un pasākumu īstenošanā. 3.5. Koordinēt informācijas drošības pārvaldības izmērāmo rādītāju monitoringu. 3.6. Izvērtēt, analizēt un sniegt priekšlikumus par informācijas drošības pārvaldības sistēmas efektivitāti.
4. Informācijas drošības incidentu pārvaldība.	4.1. Izstrādāt un ieviest informācijas drošības incidentu pārvaldības procesu. 4.2. Koordinēt informācijas drošības incidentu analīzes un izmeklēšanas procesu.

Profesijas standarta projekta izstrādes darba grupas sastāvs:

Dalībnieka vārds, uzvārds	Darba vieta un amats
Vladislavs Minkevičs	Finanšu ministrija, informācijas sistēmu drošības pārvaldnieks, CISA, CISSP
Egils Stūrmanis	Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (CERT.LV), attīstības projektu vadītājs.
Sintija Deruma	Biedrība "Latvijas Informācijas un komunikācijas tehnoloģijas asociācija" eksperte, AS „Latvenergo”, informācijas tehnoloģiju projektu vadītāja, CISM
Arnis Vārslavs	Pamatdarba vieta – Exigen Services Latvija, kvalitātes vadītājs, CISM Vieslektors – RISEBA
Mārtiņš Tarasovs	Vides aizsardzības un reģionālās attīstības ministrija, informācijas sistēmu drošības pārvaldnieks