informatikos ir ryšių departamentas

VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ VALSTYBĖS INFORMACINIŲ SISTEMŲ IR REGISTRŲ ELEKTRONINĖS INFORMACIJOS SAUGOS UŽTIKRINIMAS

Vilnius
2016-09-30

Turinys

- Vidaus reikalų informacinės sistemos (VRIS), Lietuvos nacionalinės Šengeno informacinės sistemos (NSIS), Lietuvos nacionalinės vizų informacinės sistemos (NVIS), Integruotos baudžiamojo proceso informacinės sistemos (IBPS), Administracinių teisės pažeidimų registro (ATPR), kitų informacinių sistemų ir registrų saugos dokumentai.
- Saugos įgaliotinių funkcijos. Pagrindinio saugos įgaliotinio ir kitų saugos įgaliotinių teisės, pareigos ir atsakomybė.

Vidaus reikalų informacinės sistemos saugos dokumentai

- Vidaus reikalų informacinės sistemos duomenų saugos nuostatai, patvirtinti VRM 2007-01-02 įsakymu Nr. 1V-1 „Dėl Vidaus reikalų informacinės sistemos nuostatų ir Vidaus reikalų informacinės sistemos duomenų saugos nuostatų patvirtinimo“;
- Vidaus reikalų informacinės sistemos veiklos tęstinumo valdymo planas ir Vidaus reikalų informacinės sistemos duomenų saugaus tvarkymo taisyklės, patvirtintos VRM 2007-12-27 įsakymu Nr. 1V-449 „Dėl Vidaus reikalų informacinės sistemos veiklos tęstinumo valdymo plano ir Vidaus reikalų informacinės sistemos duomenų saugaus tvarkymo taisyklių patvirtinimo“;
- Vidaus reikalų informacinės sistemos centrinio duomenų banko naudotojų administravimo taisyklės, patvirtintos VRM 2008-05-06 d. įsakymu Nr. 1V-165 „Dėl Vidaus reikalų informacinės sistemos centrinio duomenų banko naudotojų administravimo taisyklių patvirtinimo“.

Lietuvos nacionalinės Šengeno informacinės sistemos (NSIS) saugos dokumentai

- Lietuvos nacionalinės Šengeno informacinės sistemos duomenų saugos nuostatai, patvirtinti VRM 2007-09-18 įsakymu Nr. 1V-325 „Dėl Lietuvos nacionalinės Šengeno informacinės sistemos duomenų saugos nuostatų patvirtinimo“;
- Lietuvos nacionalinės Šengeno informacinės sistemos naudotojų administravimo tvarka, patvirtintos VRM 2008-02-01 įsakymu Nr. 1V-46 „Dėl Lietuvos nacionalinės Šengeno informacinės sistemos naudotojų administravimo tvarkos patvirtinimo“;
- Lietuvos nacionalinės Šengeno informacinės sistemos veiklos tęstinumo valdymo planas ir Lietuvos nacionalinės Šengeno informacinės sistemos duomenų saugaus tvarkymo taisyklės, patvirtintos VRM 2007-12-29 įsakymu Nr. 1V-454 „Dėl Lietuvos nacionalinės Šengeno informacinės sistemos veikos tęstinumo valdymo plano ir Lietuvos nacionalinės Šengeno informacinės sistemos duomenų saugaus tvarkymo taisyklių patvirtinimo“.

Lietuvos nacionalinės vizų informacinės sistemos (NVIS) saugos dokumentai

- Lietuvos nacionalinės vizų informacinės sistemos duomenų saugos nuostatai, patvirtinti VRM 2011-06-17 įsakymu Nr. 1V-469 „Dėl Lietuvos nacionalinės vizų informacinės sistemos duomenų saugos nuostatų patvirtinimo, saugos įgaliotinio ir saugos politiką įgyvendinančių dokumentų rengėjo paskyrimo“;
- Lietuvos nacionalinės vizų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės, Lietuvos nacionalinės vizų informacinės sistemos naudotojų administravimo taisyklės ir Lietuvos nacionalinės vizų informacinės sistemos veiklos tęstinumo valdymo planas, patvirtinti VRM 2016-05-26 įsakymu Nr. 1V-389 „Dėl Lietuvos nacionalinės vizų informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, naudotojų administravimo taisyklių ir veiklos tęstinumo valdymo plano patvirtinimo“.

Integruotos baudžiamojo proceso informacinės sistemos (IBPS) saugos dokumentai

- Integruotos baudžiamojo proceso informacinės sistemos duomenų saugos nuostatai, patvirtinti VRM 2015-11-06 įsakymu Nr. 1V-876 „Dėl Integruotos baudžiamojo proceso informacinės sistemos duomenų saugos nuostatų patvirtinimo“;
- Integruotos baudžiamojo proceso informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklės, Integruotos baudžiamojo proceso informacinės sistemos veiklos tęstinumo valdymo planas ir Integruotos baudžiamojo proceso informacinės sistemos naudotojų administravimo taisyklės, patvirtintos VRM 2016-02-01 įsakymu Nr. 1V-73 „Dėl Integruotos baudžiamojo proceso informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, Integruotos baudžiamojo proceso informacinės sistemos veiklos tęstinumo valdymo plano ir Integruotos baudžiamojo proceso informacinės sistemos naudotojų administravimo taisyklių patvirtinimo“.

Administracinių teisės pažeidimų registro (ATPR) saugos dokumentai

- Administracinių teisės pažeidimų registro duomenų saugos nuostatai, patvirtinti, Lietuvos Respublikos vidaus reikalų ministro 2015 m. spalio 5 d. įsakymu Nr. 1V-781 „Dėl Administracinių teisės pažeidimų registro duomenų saugos nuostatų patvirtinimo“;
- Administracinių teisės pažeidimų registro saugaus elektroninės informacijos tvarkymo taisyklės, Administracinių teisės pažeidimų registro naudotojų administravimo taisyklės ir Administracinių teisės pažeidimų registro veiklos tęstinumo valdymo planas, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2016 m. gegužės 10 d. d. įsakymu Nr. 1V-351 „Dėl Administracinių teisės pažeidimų registro saugaus elektroninės informacijos tvarkymo taisyklių, Administracinių teisės pažeidimų registro naudotojų administravimo taisyklių ir Administracinių teisės pažeidimų registro veiklos tęstinumo valdymo plano patvirtinimo“.

Valstybės ir žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų saugos įgaliotiniai

Bendrųjų elektroninės informacijos saugos reikalavimų aprašas (BSR aprašas)

Informacinės sistemos saugos įgaliotinis (toliau – saugos įgaliotinis) – institucijos valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį, koordinuojantis ir prižiūrintis saugos politikos įgyvendinimą informacinėje sistemoje.

Saugos įgaliotinių funkcijos (1)

Valstybės informacinių išteklių valdymo įstatymas (VIIVĮ)

44 straipsnis. Saugos įgaliotinis

- 1. Saugos įgaliotiniu skiriamas darbuotojas, kuris atsako už saugos reikalavimų vykdymą ir atlieka kitas teisės aktuose nustatytas funkcijas.
- 2. Saugos įgaliotinis skiriamas teisės aktu, kuriuo tvirtinami registro ar valstybės informacinės sistemos saugos nuostatai, arba registro ar valstybės informacinės sistemos valdytojas paveda registro arba valstybės informacinės sistemos tvarkytojui paskirti saugos įgaliotinį. Saugos įgaliotinis gali būti paskiriamas keliems registrams, valstybės informacinėms sistemoms ar posistemiams. Saugos įgaliotinis ir šio įstatymo 8 straipsnyje nurodytas duomenų valdymo įgaliotinis gali būti tas pats asmuo.
- 3. Saugos įgaliotinis atlieka registro ar valstybės informacinės sistemos saugos nuostatuose ir kituose teisės aktuose nustatytas funkcijas.

Saugos įgaliotinių funkcijos (2)

BSR aprašo 22, 25 punktai:

- teikia registro ar informacinės sistemos (RIS) valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, vadovui pasiūlymus dėl:
  - administratoriaus (administratorių) paskyrimo ir reikalavimų administratoriui, (administratoriams) nustatymo,
  - institucijos IT saugos atitikties vertinimo atlikimo;
- teikia RIS valdytojo vadovui pasiūlymus dėl saugos dokumentų priėmimo, keitimo;
- koordinuoja elektroninės informacijos saugos (EIS) incidentų, įvykusių IS, tyrimą ir bendradarbiauja su kompetentingoms institucijoms, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su EIS incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos darbo grupės;

Saugos įgaliotinių funkcijos (3)

- teikia administratoriui (administratoriams) ir RIS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su saugos politikos įgyvendinimu;
- organizuoja rizikos įvertinimą;
- periodiškai organizuoja RIS naudotojų mokymą EIS klausimais, informuoja juos apie EIS problemas:
  - mokymo ir informavimo būdai pasirenkami atsižvelgiant į RIS specifiką;
  - mokymas planuojamas, organizuojamas ir vykdomas RIS valdytojo tvirtinamuose DSN nuostatuose nustatyta tvarka;
- atlieka kitas Saugos nuostatuose, kituose teisės aktuose, reglamentuojančiuose EIS, nustatytas ir BSR aprašo jam priskirtas funkcijas.

IBPS pagrindinio saugos įgaliotinio funkcijos

1. koordinuoja IBPS tvarkytojų saugos įgaliotinių veiklą, supažindina juos su Saugos nuostatais, IBPS saugos politiką įgyvendinančiais dokumentais, kitais Saugos nuostatų 38 punkte nurodytais dokumentais ir atsakomybe už juose nustatytų reikalavimų nesilaikymą;

2. rengia IBPS saugos politiką įgyvendinančių dokumentų projektus;

3. koordinuoja ir prižiūri IBPS elektroninės informacijos saugos politikos įgyvendinimą;

4. koordinuoja IBPS elektroninės informacijos saugos incidentų tyrimą;

5. teikia pasiūlymus Informatikos ir ryšių departamento direktoriui ir IBPS valdytojui dėl:

5.1. saugos dokumentų – Saugos nuostatų ir IBPS saugos politiką įgyvendinančių dokumentų – priėmimo, keitimo ar panaikinimo;

5.2. IBPS IT atitikties saugos reikalavimams vertinimo atlikimo;

5.3. IBPS pagrindinio (pagrindinių) administratoriaus (administratorių) paskyrimo;

6. teikia IBPS saugos įgaliotiniams, IBPS pagrindiniam (pagrindiniams) administratoriui (administratoriams) ir IBPS administratoriams, prireikus ir kitiems IBPS valdytojo ir tvarkytojų darbuotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su IBPS saugos politikos įgyvendinimu;

7. kasmet organizuoja IBPS saugos įgaliotinių, IBPS administratorių saugos mokymus, reguliariai jiems primena saugos problemas, teikia konsultacijas (elektroniniu paštu, telefonu, prireikus rengia atmintines IBPS naudotojams ir pan.);

8. vykdo kitas Saugos nuostatų, IBPS nuostatų, Saugos reikalavimų aprašo ir kitų teisės aktų nustatytas funkcijas.

IBPS saugos įgaliotinio funkcijos (1)

1. koordinuoja ir prižiūri IBPS elektroninės informacijos saugos politikos įgyvendinimą tvarkytojo įstaigoje bei tvarkytojo įstaigos reguliavimo ar veiklos sričiai priskirtose kitose įstaigose (teritorinėse, specializuotose, atskaitingose ir kitose), turinčiose IBPS naudotojų darbo vietas;

2. teikia pasiūlymus tvarkytojų vadovams dėl IBPS administratorių paskyrimo;

3. teikia IBPS pagrindiniam saugos įgaliotiniui siūlymus dėl:

3.1. saugos dokumentų – Saugos nuostatų ir IBPS saugos politiką įgyvendinančių dokumentų – priėmimo, keitimo ar panaikinimo;

3.2. IBPS informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

3.3. saugos mokymų organizavimo;

4. teikia savo tvarkytojo įstaigos ir jos reguliavimo ar veiklos sričiai priskirtų kitų įstaigų IBPS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su IBPS saugos politikos įgyvendinimu;

5. informuoja IBPS pagrindinį saugos įgaliotinį apie IBPS elektroninės informacijos saugos incidentus ir teikia siūlymus dėl minėtų incidentų pašalinimo;

IBPS saugos įgaliotinio funkcijos (2)

6. supažindina savo tvarkytojo įstaigos ir jos reguliavimo ar veiklos sričiai priskirtų kitų įstaigų IBPS administratorius ir IBPS naudotojus su Saugos nuostatais, IBPS saugos politiką įgyvendinančiais dokumentais, kitais Saugos nuostatų 38 punkte nurodytais dokumentais ir atsakomybe už juose nustatytų reikalavimų nesilaikymą; supažindinimo su šiame punkte nurodytais dokumentais būdą pasirenka patys IBPS saugos įgaliotiniai, tačiau turi būti užtikrintas susipažinimo įrodomumas;

7. kasmet organizuoja savo tvarkytojo įstaigos ir jos reguliavimo ar veiklos sričiai priskirtų kitų įstaigų IBPS administratorių ir IBPS naudotojų saugos mokymus, reguliariai jiems primena saugos problemas, teikia konsultacijas (elektroniniu paštu, telefonu, prireikus rengia atmintines IBPS naudotojams ir pan.). Saugos mokymai organizuojami po to, kai IBPS tvarkytojų vadovų paskirtus saugos įgaliotinius apmoko IBPS pagrindinis saugos įgaliotinis;

8. dalyvauja tiriant IBPS tvarkytojo elektroninės informacijos saugos incidentus;

9. atlieka kitas Saugos nuostatuose ir kituose saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas, susijusias su IBPS elektroninės informacijos sauga.

Informatikos ir ryšių departamento paskirto ATPR saugos įgaliotinio funkcijos

1. rengia ATPR saugos politiką įgyvendinančių dokumentų projektus;

2. koordinuoja kitų ATPR saugos įgaliotinių veiklą, supažindina juos su Saugos nuostatais, ATPR saugos politiką įgyvendinančiais dokumentais bei atsakomybe už juose nustatytų reikalavimų nesilaikymą;

3. koordinuoja ir prižiūri ATPR elektroninės informacijos saugos politikos įgyvendinimą;

4. koordinuoja ATPR elektroninės informacijos saugos incidentų tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais;

5. teikia pasiūlymus Informatikos ir ryšių departamento direktoriui dėl:

5.1. ATPR administratoriaus (administratorių) paskyrimo ir reikalavimų jam nustatymo;

5.2. Saugos nuostatų ir ATPR saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar pripažinimo netekus galios;

5.3. ATPR informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

6. teikia kitiems ATPR saugos įgaliotiniams, ATPR administratoriui (administratoriams), ATPR naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su ATPR saugos politikos įgyvendinimu;

7. periodiškai, ne rečiau kaip kartą per kalendorinius metus, organizuoja ATPR saugos įgaliotinių, ATPR administratorių saugos mokymus, reguliariai jiems primena saugos problemas, teikia konsultacijas (elektroniniu paštu, telefonu, prireikus rengia atmintines naujai priimtiems darbuotojams ir pan.);

8. organizuoja ATPR rizikos įvertinimą;

9. vykdo kitas Saugos nuostatų, ATPR nuostatų, Saugos reikalavimų aprašo ir kitų teisės aktų nustatytas funkcijas.

ATPR saugos įgaliotinio funkcijos (1)

1. koordinuoja ir prižiūri ATPR elektroninės informacijos saugos politikos įgyvendinimą tvarkytojo įstaigoje ir tvarkytojo įstaigos reguliavimo sričiai priskirtose kitose įstaigose (teritorinėse, specializuotose, atskaitingose ir kitose), turinčiose ATPR naudotojų darbo vietas;

2. teikia Informatikos ir ryšių departamento paskirtam ATPR saugos įgaliotiniui siūlymus dėl:

2.1. Saugos nuostatų ir ATPR saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar pripažinimo netekusiais galios;

2.2. ATPR informacinių technologijų atitikties saugos reikalavimams vertinimo atlikimo;

2.3. saugos mokymų organizavimo;

3. teikia savo tvarkytojo įstaigos ir jos reguliavimo sričiai priskirtų kitų įstaigų ATPR naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su ATPR saugos politikos įgyvendinimu;

4. informuoja Informatikos ir ryšių departamento paskirtą ATPR saugos įgaliotinį apie ATPR elektroninės informacijos saugos incidentus ir teikia siūlymus dėl minėtų incidentų pašalinimo;

ATPR saugos įgaliotinio funkcijos (2)

5. supažindina savo tvarkytojo įstaigos ir jos reguliavimo sričiai priskirtų kitų įstaigų ATPR naudotojus su Saugos nuostatais ir ATPR saugos politiką įgyvendinančiais dokumentais bei atsakomybe už šių reikalavimų nesilaikymą;

6. ne rečiau kaip kartą per kalendorinius metus organizuoja savo tvarkytojo įstaigos ir jos reguliavimo sričiai priskirtų kitų įstaigų ATPR naudotojų saugos mokymus, reguliariai jiems primena saugos problemas, teikia konsultacijas (elektroniniu paštu, telefonu, prireikus rengia atmintines naujai priimtiems darbuotojams ir pan.);

7. dalyvauja tiriant ATPR tvarkytojo įstaigoje (ir jos reguliavimo sričiai priskirtose kitose įstaigose) įvykusius elektroninės informacijos saugos incidentus;

8. atlieka kitas Saugos nuostatuose ir kituose ATPR saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas, susijusias su ATPR elektroninės informacijos sauga.

Pagrindinės problemos rengiant saugos dokumentus (1)

Bendrosios pastabos

- RIS duomenų saugos nuostatų (DSN) projektai teikiami derinti nepatvirtinus RIS nuostatų;
- RIS nuostatų ir RIS DSN projektai teikiami derinti be teisės akto, kuriuo jie bus patvirtinti, projekto (projektų);
- saugos politiką įgyvendinantys dokumentai teikiami derinti nepatvirtinus RIS DSN;
- teikiami derinti teisės aktų pakeitimų projektai be teisės aktų, kurie yra keičiami (jie nepaskelbti RISR ir (arba) e-TAR);
- saugos dokumentų projektuose apibrėžiamos naujos, negaliojančios teisės aktuose sąvokos, arba naudojamos niekur neapibrėžtos sąvokos, pavyzdžiui:

  informacijos saugumo įgaliotinis (= IS saugos įgaliotinis);

  nenumatyta situacija (=elektroninės informacijos saugos incidentas);

  duomenų saugos dokumentai (=saugos politiką įgyvendinantys dokumentai);

  IS duomenų tvarkytojai (= IS naudotojai) ir kt.

Pagrindinės problemos rengiant saugos dokumentus (2)

RIS duomenų saugos nuostatai (DSN)

- nustatoma žemesnė RIS elektroninės informacijos kategorija (ypatingos svarbos informacija – I; svarbi informacija – II; vidutinės svarbos informacija – III; mažiausios svarbos informacija – IV kategorija);
- nenurodomas IT atitikties vertinimo atlikimo periodiškumas:

  ne rečiau kaip kartą per dvejus metus
- saugos įgaliotiniui klaidingai priskiriamos administratoriaus, RIS valdytojo ar tvarkytojo funkcijos:

  reagavimas į elektroninės informacijos incidentus (RIS administratorius);

  DSN projektų rengimas (RIS valdytojas);

  administracinių, techninių ir organizacinių saugos priemonių įgyvendinimas (RIS tvarkytojas).

Pagrindinės problemos rengiant saugos dokumentus (3)

RIS duomenų saugos nuostatai (DSN)

- nenurodomos specifinės administratoriaus funkcijos:

  nustato RIS pažeidžiamas vietas, reaguoja į EIS incidentus; privalo patikrinti (peržiūrėti) RIS sąranką ir RIS būsenos rodiklius reguliariai, ne rečiau kaip kartą per metus ir (arba) po RIS pokyčio; įgyvendina RIS pokyčius ir kt.;

- pasitaiko RIS DSN ir saugos politiką įgyvendinančiuose dokumentų projektuose nuostatų dėl įslaptintos informacijos

  (įslaptinta informacija turi būti apdorojama ir perduodama tik įteisintomis automatizuoto duomenų apdorojimo sistemomis ir tinklais);

- nenurodoma, kad nuotolinis prisijungimas prie RIS turi būti vykdomas protokolu, skirtu duomenų šifravimui.

Pagrindinės problemos rengiant saugos dokumentus (4)

Saugaus elektroninės informacijos tvarkymo taisyklės (SEITT)

- trūksta nuostatų dėl nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarkos;
- nenurodoma, kad po 15 min. RIS naudotojui neatliekant jokių veiksmų RIS turi užsirakinti;
- nėra nuostatų dėl elektroninės informacijos kopijose užšifravimo, šifravimo raktų saugojimo atskirai nuo kopijų;
- nenurodoma RIS pokyčių valdymo tvarka:

  pokyčių identifikavimas; pokyčių suskirstymas į kategorijas; pokyčių įtakos vertinimas; pokyčių prioritetų nustatymas; pokyčių atlikimas;
- nenurodoma, kad RIS turi būti įrašomi ir nustatytą laiką saugomi duomenys apie tarnybinių stočių, taikomosios programinės įrangos įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis, visus RIS naudotojų vykdomus veiksmus;

Pagrindinės problemos rengiant saugos dokumentus (5)

SEITT

- nenurodomi paslaugų teikėjų prieigos prie informacinės sistemos lygiai ir sąlygos bei kontroliuojantis paslaugų teikėjo darbą asmuo;
- trūksta nuostatų dėl būtinumo RIS tarnybinių stočių patalpose įrengti gaisro ir įsilaužimo daviklius, prijungiant juos prie pastato signalizacijos ir (arba) apsaugos tarnybos stebėjimo pulto;
- trūksta nuostatų dėl RIS elektroninės informacijos perdavimo tinklo, kuris turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienę; ugniasienės įvykių žurnalai (angl. *Logs*) turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;
- nenurodomi papildomi RIS elektroninės informacijos saugos techniniai reikalavimai trečiajai, antrajai ir pirmajai RIS kategorijoms.

Pagrindinės problemos rengiant saugos dokumentus (6)

Naudotojų administravimo taisyklės(NAT)

- trūksta nuostatos dėl laikino slaptažodžio ir prisijungimo vardo perdavimo atviru tekstu sąlygų;
- RIS naudotojų teisės neatskirtos nuo RIS administratoriaus teisių;
- nėra atskirai pateiktų nuostatų dėl reikalavimų administratorių slaptažodžiams;
- nenurodoma arba netiksliai nurodoma, kada sustabdomos arba naikinamos naudotojo prieigos prie RIS teisės.

Pagrindinės problemos rengiant saugos dokumentus (7)

Veiklos tęstinumo valdymo planas (VTV planas)

- nenurodoma, kad VTV planas įsigalioja įvykus EIS incidentui;
- trūksta informacijos apie patekimą į atsargines patalpas (atsarginių patalpų adresai ir būdai, kaip iki jų nuvykti).

Saugos įgaliotinis – svarbus žmogus, nes...

atsako už saugos reikalavimų vykdymą ir atlieka kitas registro ar valstybės informacinės sistemos saugos nuostatuose ir kituose teisės aktuose nustatytas funkcijas, t. y. jis užtikrina, kad elektroninės informacijos grėsmės būtų suvaldytos.

Ar tikrai?

http://awesometoyblog.com/wp-content/uploads/2013/06/44022_Superman_R1_Bank.jpg

Saugos įgaliotinio funkcijos

Nustatytos:

- Bendrųjų el. informacijos saugos reikalavimų apraše, patvirtintame LRV 2013 m. liepos 24 d. nutarimu Nr. 716 (pakeistas LRV 2016-08-11 nutarimu Nr. 826)
- IS ir registro duomenų saugos nuostatuose

Rizikos vertinimas

Bendrųjų elektroninės informacijos saugos reikalavimų 35 p.:

Saugos įgaliotinis kasmet organizuoja visų informacinių sistemų rizikos įvertinimą

Prireikus gali organizuoti neeilinį rizikos įvertinimą

Svarbiausieji rizikos veiksniai

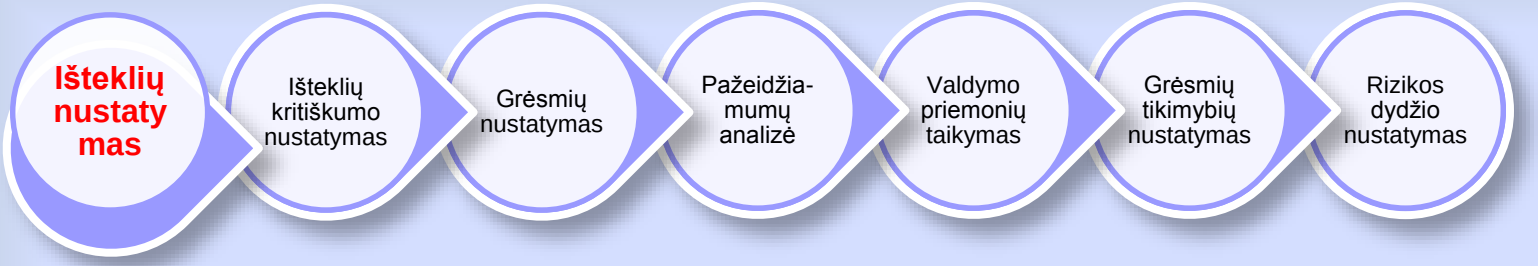
Nustatyti Bendruosiuose el. informacijos saugos reikalavimuose:

- Subjektyvūs netyčiniai
- Subjektyvūs tyčiniai
- Veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių 3 punkte

Rizikos vertinimo modeliai

- Atsižvelgti į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės standartus.
- **ISO/IEC 27005 –** tai svarbiausias tarptautinis standartas, apibrėžiantis kaip turi būti vertinama ir valdoma informaciniams ištekliams kylanti rizika.

Rizikos vertinimo procesas ARSIS metodu



Nustatoma, kokie yra **turimi organizacijos ištekliai** ir į kokias kategorijas jie skirstomi. Pagal *ISO 27001:2013 standartą* ištekliai rūšiuojami į šias kategorijas:

- **Techninė įranga** – kompiuteriai, tarnybinės stotys, spausdintuvai, nešiojamieji įrenginiai, atmintukai ir kt.
- **Programinė įranga** - licencijuojama ir nemokama programinė įranga
- **Informacija –** duomenų bazės, failai, spausdinta informacija ir kt.
- **Infrastruktūra –** biuro patalpos, komunikacijos ir kt.
- **Žmogiškieji ištekliai –** organizacijos darbuotojai taip pat yra informacinis turtas
- **Išorinių teikėjų paslaugos –** visos paslaugos, kurios turi sąlytį su informacija

Nustatomas turimų **organizacijos išteklių kritiškumas veiklos procesams.**

- Ištekliai **reitinguojami pagal kritiškumą**.
- Kritiškiausi ištekliai yra tie, dėl **kurių sutrikimo sutriktų organizacijos veikla**.

Rezultatas – išteklių sąvadas su nurodytu kritiškumo įvertinimu trims parametrams – *konfidencialumui, vientisumui ir prieinamumui*

Išteklių nustatymas → Išteklių kritiškumo nustatymas → **Grėsmių nustatymas** → Pažeidžia-mumų analizė → Valdymo priemonių taikymas → Grėsmių tikimybių nustatymas → Rizikos dydžio nustatymas

Grėsmių nustatymas apibrėžia, kokios yra galimos grėsmės informaciniams ištekliams.

Sudarant grėsmių sąrašą rekomenduojama naudotis Vokietijos federalinės informacinių technologijų saugumo tarnybos (Bundesamt für Sicherheit in der Informationstechnik) **BSI-Standart 100-3, v.2.5** pateiktu grėsmių katalogu.

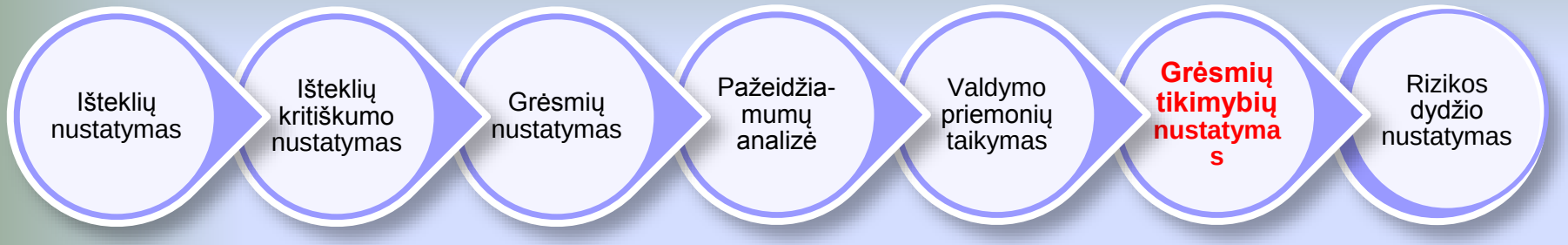
Remiantis sudarytu grėsmių sąrašu gilinamasi į:

- **Techninių komponentų trūkumus –** reikalingų apsaugos priemonių nebuvimą, neatnaujintą programinę įrangą, architektūrinius saugumo trūkumus ir kt.
- **Veiklos procesų trūkumus –** formaliųjų procedūrų aprašų nebuvimą ar jų nesilaikymą, naudojamas nesaugias, su saugumo standartais nesuderinamas veiklos procedūras.

Rezultatas – aprašas, kuriame nurodomi nustatyti pažeidžiamumai, atsirandantys dėl techninių komponentų ir/ar veiklos procesų trūkumų

Įvertinamos **taikomos valdymo priemonės**, skirtos suvaldyti esamus pažeidžiamumus.

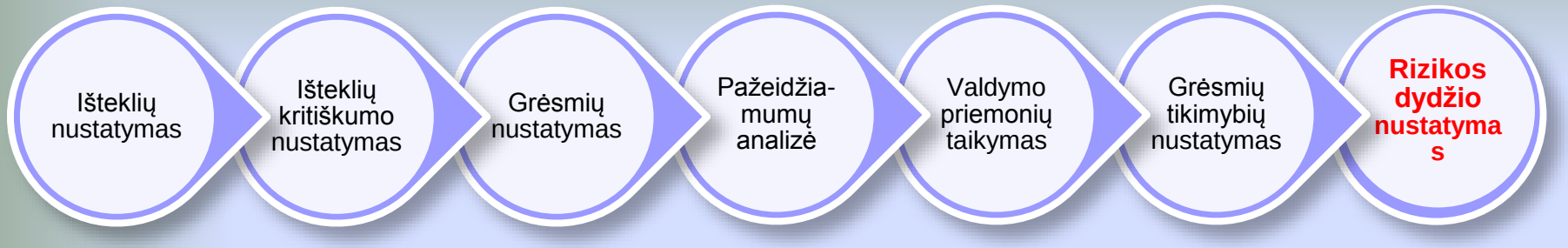
- Analizuojant kontrolės priemones rekomenduojama vadovautis **ISO/IEC 27002:2013** priede pateikiamu **valdymo priemonių sąrašu**, kuriame detaliai aprašoma:
  - Valdymo priemonė
  - Saugumo reikalavimai, kuriuos tenkina ši valdymo priemonė
  - Priemonės taikymo pobūdis



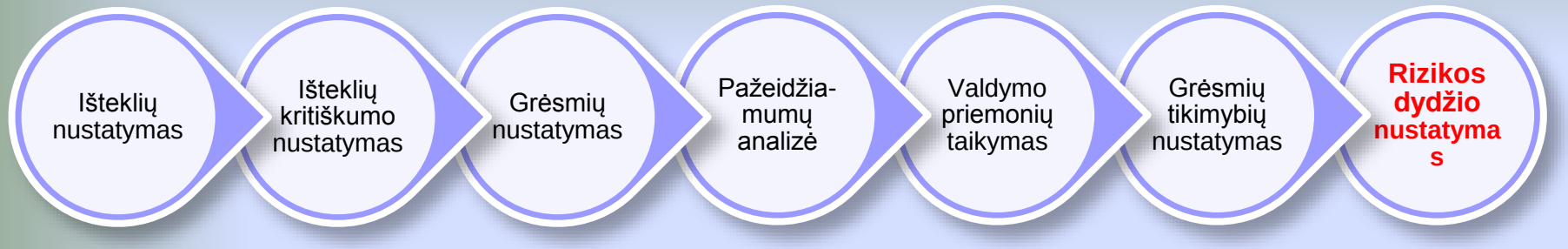
Grėsmės tikimybė nustatoma įvertinant:

- Grėsmės taikymo sritį
- Scenarijus grėsmės įvykimui

- Esamų valdymo priemonių efektyvumą



- Remiantis surinktais duomenimis, atliekamas informaciniams ištekliams kylančių rizikų vertinimas nustatant kylančias grėsmes, pažeidžiamumus bei galimą poveikį informacinei sistemai ir/arba institucijos veiklai
- Įvertinus riziką nustatoma priimtina ir nepriimtina rizika
- Nepriimtinos rizikos valdymui sudaromas priemonių planas



Rizikos vertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama informacinės sistemos valdytojo ar tvarkytojo, jeigu jis paskyrė saugos įgaliotinį, vadovui.

Atsižvelgdamas į rizikos įvertinimo ataskaitą, informacinės sistemos valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

Rizikos ataskaita

Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 38 punktas:

Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijos teikiamos Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai (ARSIS)

Informacinių technologijų saugos atitikties vertinimas

Informacinių technologijų saugos atitikties vertinimas (Atitikties vertinimas) atliekamas pagal Informacinių technologijų saugos atitikties vertinimo metodiką (Vidaus reikalų ministro 2016 m. rugpjūčio 2 d. įsakymas Nr. 1V-634)

Saugos įgaliotinis teikia informacinės sistemos valdytojo/tvarkytojo vadovui siūlymus dėl informacinių technologijų saugos atitikties vertinimo atlikimo

Atitikties vertinimo atlikimo dažnis

3 ir 4 kategorijos informacinių sistemų	ne rečiau kaip kartą per dvejus metus, jei teisės aktuose nenustatyta kitaip
1 ir 2 kategorijos informacinių sistemų	ne rečiau kaip kartą per metus, jei teisės aktuose nenustatyta kitaip

Informacinių technologijų saugos reikalavimų atitikties vertinimo metu:

nustatomas saugos reikalavimų įgyvendinimo lygis pagal 5 balų skalę:

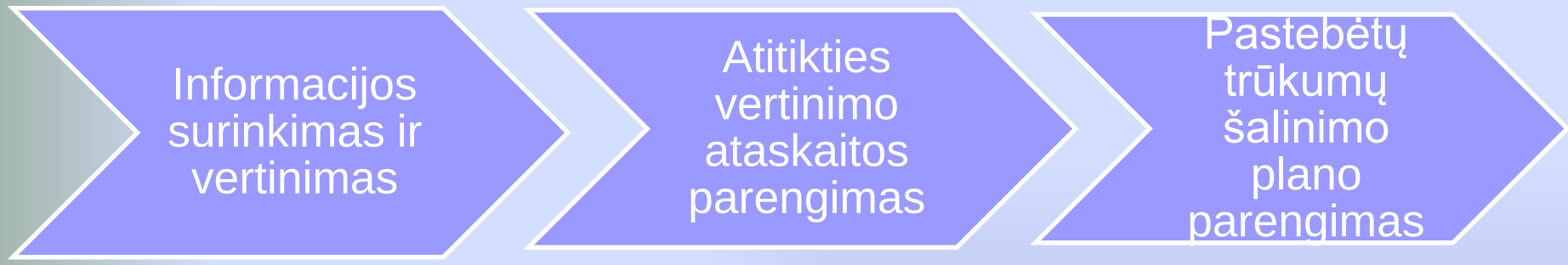
- Bendrųjų el. informacijos saugos reikalavimų apraše ;
- Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų el. informacijos saugos reikalavimuose;
- Bendruosiuose reikalavimuose organizacinėms ir techninėms asmens duomenų saugumo priemonėms;
- Lietuvos stantartuose LST ISO/IEC 27001:2013 ir LST ISO/IEC 27002:2014;

Informacinių technologijų saugos reikalavimų atitikties vertinimo metu :

Rekomenduojama :

- patikrinti, ar IS saugos dokumentai persvarstomi (peržiūrimi) saugos reikalavimuose nustatyti metu, ir įvertinama jų kokybė;
- inventorizuoti IS techninę ir programinę įrangą;
- patikrinti ne mažiau kaip 10 procentų atsitiktinai parinktų IS naudotojų kompiuterizuotų darbo vietų, visose tarnybinėse stotyse įdiegtas programas bei jų sąranką (konfigūraciją);
- patikrinti IS naudotojams suteiktų teisių ir vykdomų funkcijų atitiktį;
- įvertinti pasirengimą užtikrinti IS veiklos tęstinumą įvykus el. informacijos saugos incidentui;
- Įvertinti IS rizikos įvertinimo ir valdymo būklę;.

Atitikties vertinimo eiga



Informacijos surinkimas ir vertinimas

- Surenkama vertinimui būtina informacija apie informacinių technologijų saugos padėtį įstaigos informacinėse sistemose ir dokumentai, būtini užtikrinant informacinės sistemos saugą
- Informacijai surinkti arba patikslinti gali būti atlikta įstaigos valstybės tarnautojų ir darbuotojų apklausa

Atitikties vertinimo ataskaitos parengimas

- Užpildoma informacinių sistemų saugos atitikties vertinimo lentelė, kurioje yra įvertinama saugos dokumentų ir kitų objektų atitiktis elektroninės informacijos saugos reikalavimams
- Ataskaitoje nurodomi vertinimo metu rasti trūkumai ir pateikiamos rekomendacijos

Atitikties vertinimo ataskaitos parengimas

- Užpildoma informacinių sistemų saugos atitikties vertinimo lentelė, kurioje yra įvertinama saugos dokumentų ir kitų objektų atitiktis elektroninės informacijos saugos reikalavimams
- Ataskaitoje nurodomi vertinimo metu rasti trūkumai ir pateikiamos rekomendacijos

Pastebėtų trūkumų šalinimo plano parengimas

- Parengiamas pastebėtų trūkumų šalinimo planas, kuriame pateikiamos rekomendacijos vertinimo metu nustatytiems trūkumams pašalinti
- Planas pateikiamas informacinės sistemos valdytojui, kuris jį patvirtina, paskiria atsakingus vykdytojus ir nustato įgyvendinimo terminus

Informacinių technologijų saugos atitikties vertinimo ataskaita

Bendrųjų elektroninės informacijos saugos reikalavimų aprašo 45 punktas:

Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas IS valdytojas turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai (ARSIS)

informatikos ir ryšių departamentas

TEISĖS AKTUOSE NUSTATYTŲ DUOMENŲ TEIKIMO VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ ATITIKTIES ELEKTRONINĖS INFORMACIJOS SAUGOS REIKALAVIMAMS STEBĖSENOS SISTEMAI (ARSIS) TVARKA

Santrauka

Trumpa ARSIS istorija
ARSIS funkcionalumas saugos įgaliotiniams
ARSIS funkcionalumas kontroliuojančioms institucijoms (VRM, IRD)
Ištekliai ir jų saugą reglamentuojantys dokumentai
Rizikos vertinimas
Atitikties vertinimas
Projektų posistemė
Pagalbinės posistemės
Žinių bazės
Naudotojų registracija ir prisijungimas
Pirmieji žingsniai dirbant su ARSIS
Praktinė informacija ir kontaktai

Trumpa ARSIS istorija

ARSIS sukūrimas numatytas EIS(KS) plėtros programoje

ARSIS bus naudojamas EIS(KS) plėtros programos įgyvendinimo kriterijų skaičiavimui

Nuostatai patvirtinti 2012-10-16 VRM įsakymu Nr. 1V-740

Steigimo pagrindas – VIIVĮ nustatytos VRM funkcijos, VRM nuostatai

Tikslas – IT priemonėmis vykdyti elektroninės informacijos saugos reikalavimams stebėseną

Priėmimo ir tinkamumo eksploatuoti aktas pasirašytas 2015-12-17

Baigiama parengti nauja ARSIS nuostatų redakcija

Naudotojų registracija vyksta nuolat

Tikimasi, kad iki 2016 m. pabaigos institucijos pateiks kasmetinių vertinimų duomenis

ARSIS funkcionalumas saugos įgaliotiniams

Išteklius – valstybės informacinė sistema arba registras
Matoma informacija – visų institucijos valdomų ar tvarkomų išteklių
Tvarkoma informacija – tik priskirtų išteklių

Tvarkyti ištekliaus duomenis ir saugos dokumentus
Atlikti ir pateikti rizikos vertinimą
Atlikti ir pateikti informacinių technologijų saugos atitikties vertinimą
Kontroliuoti saugos priemonių įgyvendinimą
Pateikti informaciją apie užregistruotus informacijos saugos incidentus
Analizuoti prižiūrimų išteklių saugos situaciją
Žinių bazės

ARSIS funkcionalumas VRM (IRD)

Matoma visų išteklių informacija, jos keisti neleidžiama, išskyrus tam tikrus atvejus

Pateikiamų rizikos vertinimo ataskaitų, rizikos valdymo planų peržiūra

Pateikiamų atitikties ataskaitų, neatitikčių šalinimo planų peržiūra

Saugos priemonių įgyvendinimo priežiūra

Duomenų kokybės kontrolė

Žinių bazių tvarkymas

ARSIS tinkamas atitikties bet kokios srities reikalavimams stebėsenai, todėl su laiku gali daugėti reikalavimų ir kontroliuojančių institucijų

Pvz., kibernetinis saugumas ir Nacionalinis kibernetinio saugumo centras

Ištekliai ir saugos dokumentai

Dauguma duomenų paimama iš RISR

Reikia užpildyti: saugos įgaliotinis, kategorija, asmens duomenų saugumo lygis, ištekliaus rūšis, informacijos svarba

Reikia pateikti: duomenų saugos nuostatai, saugos politiką įgyvendinantys dokumentai (.docx formatu)

Informacija turi būti atnaujinama pasikeitus duomenims ir (ar) dokumentams

Rizikos vertinimas

Galimybė įvesti atliktą rizikos vertinimą arba atlikti jį ARSIS pagalba

Galimybė „keli ištekliai - vienas vertinimas“

Įvedant atliktą rizikos vertinimą:

Būtina apjungti su ARSIS duomenimis: rizikų klasifikatoriumi, vertinimo lygiais ir pan.

Atliekant rizikos vertinimą ARSIS pagalba:

Žingsnis po žingsnio atliekami visi reikalingi veiksmai: išteklių kritiškumas, grėsmių vertinimas, rizikų priimtinumas, rizikos valdymo priemonių parinkimas

Duomenų išsamumo kontrolė vykdoma automatiškai

Nepriimtinoms rizikoms turi būti parenkamos jų valdymo priemonės (sudaromas rizikų valdymo planas)

Pateikta rizikos vertinimo informacija peržiūrima VRM, gali būti prašoma patikslinti

Rizikų valdymo priemonių įgyvendinimas prižiūrimas Projektų posistemėje

Atitikties vertinimas (auditas)

Principas „vienas išteklius – vienas vertinimas“

Tačiau galima optimizuoti darbo sąnaudas vertinant kelis išteklius

Ištekliams taikytinus reikalavimus atrenka ARSIS

Vertinimo metodika atitinka 2016-08-02 VRM įsakymu Nr. 1V-534 patvirtintą Informacinių technologijų saugos atitikties vertinimo metodiką

Atitikties lygis 1-5

Gali būti reikalaujama paaiškinimo ir (ar) prisegti įrodymus

Nustatytoms neatitiktims turi būti parenkamos jų valdymo priemonės (sudaromas neatitikčių šalinimo planas)

Pateiktas vertinimas peržiūrimas VRM, gali būti prašoma patikslinti

Neatitikčių šalinimo plano įgyvendinimas prižiūrimas Projektų posistemėje

Projektų posistemė

Skirta prižiūrėti rizikos valdymo ir neatitikčių šalinimo priemonių įgyvendinimui

Kaina, terminai, atsakingi vykdytojai

Informacija turėtų būti reguliariai atnaujinama

Incidentų posistemė

Yra funkcionalumas, skirtas incidentų registravimui, susiejimui su rizikomis ir jų įvertinimais

Yra galimybė teikti incidentų informaciją automatizuotai

Šiuo metu nenaudojama

Ataskaitos

Dokumentų šablonai (rizikos vertinimo ataskaitos, audito ataskaitos)

Duomenų analizės ataskaitos (pagal metus, pagal išteklius, pagal valdytojus ir kt.)

EIS(KS) plėtros programos įgyvendinimo kriterijų skaičiavimo ataskaitos

Gali būti sukurtos pagal poreikį

Priminimai ir pranešimai

Apie artėjančius terminus, laiku neatliktus darbus

Apie priimtas arba grąžintas papildyti ataskaitas

Svarbi informacija ARSIS naudotojams (pvz. pasikeitus teisės aktams)

Žinių bazės

Teisės aktai, standartai ir jų reikalavimai

Reikalavimų įgyvendinimo tipiniai būdai, tipinės laiko ir finansinės sąnaudos, neįgyvendinimo keliamos rizikos

Sąvokos

Saugos priemonių katalogai (ISO 27002 ir SANS 20)

Rizikų klasifikatorius (BSI) ir jų valdymo priemonės

Naudotojų registracija ir prisijungimas

Kiekvienam ištekliui turi būti bent vienas jo informaciją tvarkantis asmuo

Saugos įgaliotinis turi gauti prieigą prie ARSIS

Jei prieiga reikalinga keliems asmenims ir dėl kelių išteklių – prašant prieigos būtina nurodyti, kas už ką atsakingas

Prašymą teikia ištekliaus valdytojas arba tvarkytojas, jei jam pavedė valdytojas

Pasižadėjimą pasirašo pats ARSIS naudotojas

Naudotojo rolė – išorinis naudotojas (I)

Reikia nurodyti valstybės tarnautojo kodą ir (ar) asmens kodą

Reikia nurodyti, ar institucija yra įsigijusi ISO 27001 ir 27002 standartus

Pateikiami prašymo ir pasižadėjimo pasirašyti originalai (galima el. parašu)

Po 5 darbo dienų galima bandyti prisijungti, nepavykus - pranešti

http://arsis.vrm.lt/

Prisijungimas per el. paslaugų portalą, nukreipiama iš ARSIS

Sėkmingai prisijungus grąžinama į ARSIS

Praktinė informacija

http://www.ird.lt/arsis

Registracijos formos ir tvarka

Teisinė informacija

Naudotojo vadovas

Mokomoji ir vaizdinė medžiaga

Kontaktai metodinei pagalbai gauti, pastebėtoms klaidoms pranešti

Pirmieji žingsniai dirbant su ARSIS

1. Peržiūrėti priskirtus išteklius, radus netikslumų – informuoti IRD.
   - Ar visi ištekliai priskirti
   - Ar nepriskirti papildomi ištekliai
2. Peržiūrėti iš RISR gautą informaciją apie išteklius, radus netikslumų – ištaisyti juos RISR.
3. Įvesti informaciją apie išteklius, kurios nėra RISR:
   - Saugos įgaliotinis
     - Turi būti registruotas ARSIS naudotojas
   - Kategorija, asmens duomenų saugos lygis, rūšis, tipas, informacijos svarba
     Ypač svarbu, be to negalės būti pradėtas atitikties vertinimas
   - Saugos dokumentai
     Prisegami atskirai, nurodytose vietose
     Prisegamas įsakymas (-ai), kuriuo (-ais) patvirtinti saugos dokumentai
     Jei įsakymu patvirtinti keli dokumentai, pakanka jį prisegti vieną kartą
     Formatas - .docx, .adoc, .pdf (tekstinis). Skanuotas .pdf ar kitas formatas neleidžiami.

Tik po to galima atlikti rizikos ir atitikties vertinimą

Kontaktai

Violeta Križanauskienė
Tel. (8 5) 271 7245, el. p. violeta.krizanauskiene@vrm.lt
Bronius Dručiūnas
Tel. (8 5) 271 7195, el. p. bronius.druciunas@vrm.lt
Valentinas Kraujalis
Tel. (8 5) 271 7376, el. p. valentinas.kraujalis@vrm.lt