# Drošības pārvaldības ieviešanas pieredze publiskā sektora iestādē

Arnis Vārslavs

# Profesionālā pieredze

1) Akadēmiskā : 25 gadi dažādās augstskolās – IT, informācijas drošība

- Darbs ar audienci, nepieciešamība izklāstīt materiālu klausītājam saprotamā veidā

2) Profesionālā IT : 30 gadi ar IT tehnoloģijām , IT struktūru veidotājs, vadītājs, konsultācijas

- Izaugsme kopā ar tehnoloģijām to praktiskā pielietojumā (spēja ieraudzīt un risināt problēmas)

3) Profesionālā biznesa : 20 gadi biznesa sfērās, saistītās ar IT

- Skats no lietotāja , ražotāja, pārdevēja skatu punkta

4) Informācijas drošība : 20 gadi sākot «papīru kārtošanas» līdz izmeklēšanai, analīzei un liecināšanām tiesās…

25 gadi privātais sektors <> 2 gadi publiskais sektors

# Saistošie normatīvie akti

## Privātais sektors

Fizisko personu datu aizsardzības likums
MK 30.01.2001 noteikumi Nr 40. «Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības»
MK 15.05.2015 noteikumi Nr. 216 «Kārtība, kādā sagatavo un iesniedz personas datu apstrādes atbilstības novērtējumu»

Krimināllikums

Speciālie korporatīvie likumi – piem. Kredītiestāžu likums

Speciālie uzraugošo institūciju izdotie normatīvie akti – FKTK IT drošības noteikumi utt

Speciālie korporatīvie likumi – piem. Kredītiestāžu likums

Speciālie uzraugošo institūciju izdotie normatīvie akti – FKTK IT drošības noteikumi utt

## Publiskais sektors

Informācijas tehnoloģiju drošības likums
MK 04.08.2015 noteikumi Nr. 442 «Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām»

MK 01.02.2011 noteikumi Nr.100 „Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība”

Valsts informāciju sistēmu likums
MK 15.10.2005 noteikumi Nr. 764 «Valsts informāciju sistēmu vispārējās tehniskās prasības»

# Pārvaldāmie resursi , ierobežojumi

## Privātais sektors

Atļauts viss, kas nav aizliegts

IT kā instruments konkrēta mērķa sasniegšanai

Bizness nosaka
- mērķi
- veidu, kā sasniegt (procedūras)
- KPI (izmērāmus kvalitātes kritērijus)

Mērķis ir DINAMISKS !
Procedūras ir DINAMISKAS (procesa kvalitātes uzlabojamības nepārtrauktība)

**Konstants bizness ir «miris» bizness .....**

Izmaiņu ieviešana un attīstība ir biznesa nepieciešamība !

## Publiskais sektors

Aizliegts viss, kas nav atļauts (ar normatīvajiem aktiem)



IT kā instruments labākas pārvaldības realizācijai, kur pārvaldība ir noteikta ar likuma normām

Pēc idejas pārvaldība var tikt realizēta BEZ IT , izmantojot tikai «papīra» tehnoloģiju

Mērķis un procedūras ir konstantas !

Izmaiņu ienešana procesā (līdz ar to likumdošanas aktos) ir ļoti sarežģīts un laikietilpīgs pasākums

Investīcijas tehnoloģijā ir vienreizējs pasākums, ieviešot konkrēto procesu vai rīku!

# Vēsturiskā bagāža

## Privātais sektors

Atļauts viss, kas nav aizliegts

Izmaiņu ieviešana un attīstība ir biznesa nepieciešamība !

Ir jānodrošina daudzu paralēlu sistēmu attīstības un ekspluatācijas pārvaldība

Primārais ir pārmaiņu pārvaldības uzdevums

Dokumentācija veidojas kā pārvaldības dokumentācija (kopīga visām sistēmām) +atsevišķām sistēmām veltītas komponentes !!

## Publiskais sektors

Aizliegts viss, kas nav atļauts (ar normatīvajiem aktiem)



Investīcijas tehnoloģijā ir vienreizējs pasākums, ieviešot konkrēto procesu vai rīku!

Ir jānodrošina:
- dažu sistēmu pieņemšana ekspluatācijā
- vairāku paralēlu sistēmu ekspluatācijas pārvaldība

Primārais ir ekspluatācijas uzdevums

Dokumentācija veidojas kā sistēmām līdzi nākošās dokumentācijas bibliotēka !!

# Vēsturiskā bagāža

## Privātais sektors

Atļauts viss, kas nav aizliegts

Ir jānodrošina daudzu paralēlu sistēmu attīstības un ekspluatācijas pārvaldība

Primārais ir pārmaiņu pārvaldības uzdevums

Dokumentācija veidojas kā pārvaldības dokumentācija (kopīga visām sistēmām) +atsevišķām sistēmām veltītas komponentes !!

## Publiskais sektors

Aizliegts viss, kas nav atļauts (ar normatīvajiem aktiem)



Ir jānodrošina:
- dažu sistēmu pieņemšana ekspluatācijā
- vairāku paralēlu sistēmu ekspluatācijas pārvaldība

Primārais ir ekspluatācijas uzdevums

Dokumentācija veidojas kā sistēmām līdzi nākošās dokumentācijas bibliotēka !!

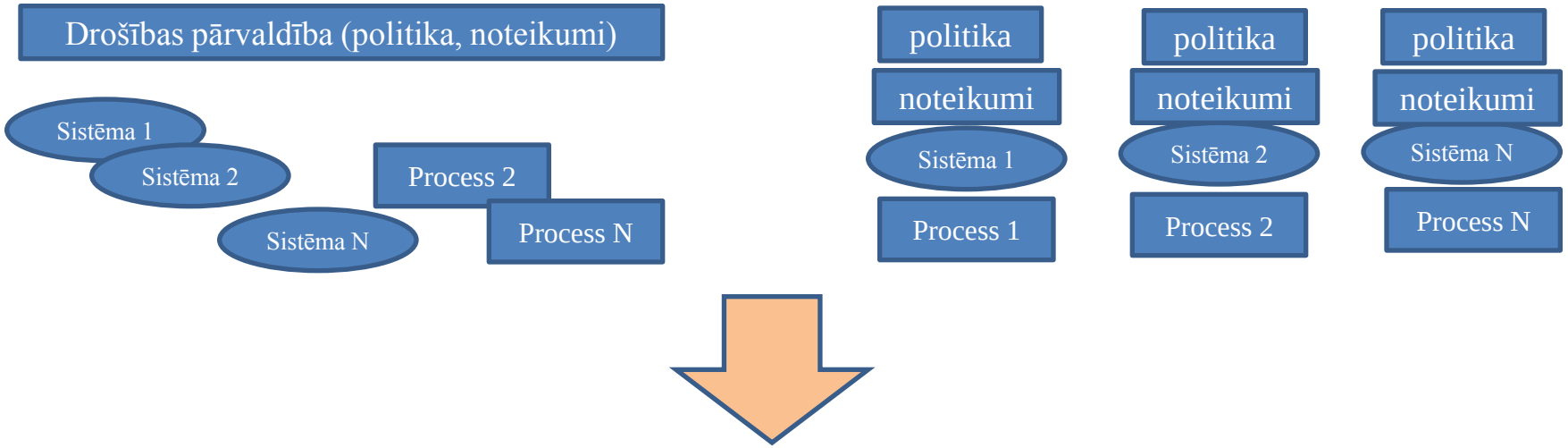
Informācijas drošība ir organizējama un pārvaldāma konceptuāli vienoti (ISO 2700x) …

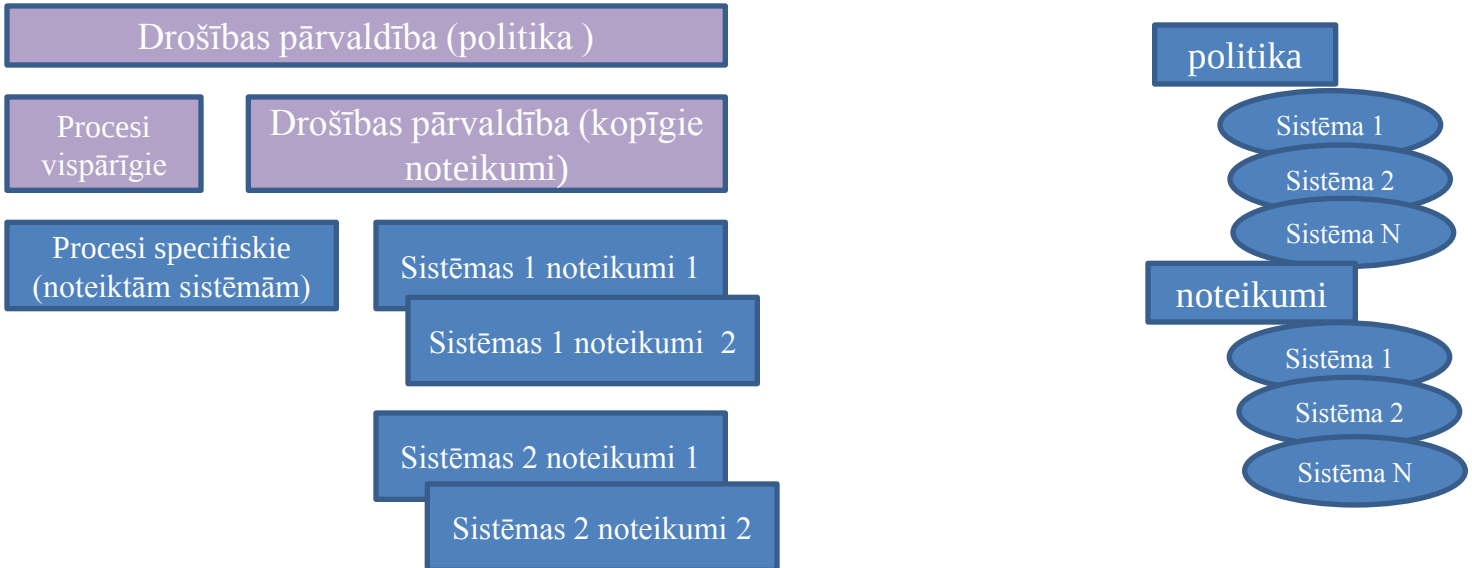
# Vēsturiskā bagāža

Privātais sektors

Publiskais sektors

Informācijas drošība ir organizējama un pārvaldāma konceptuāli vienoti (ISO 2700x) …



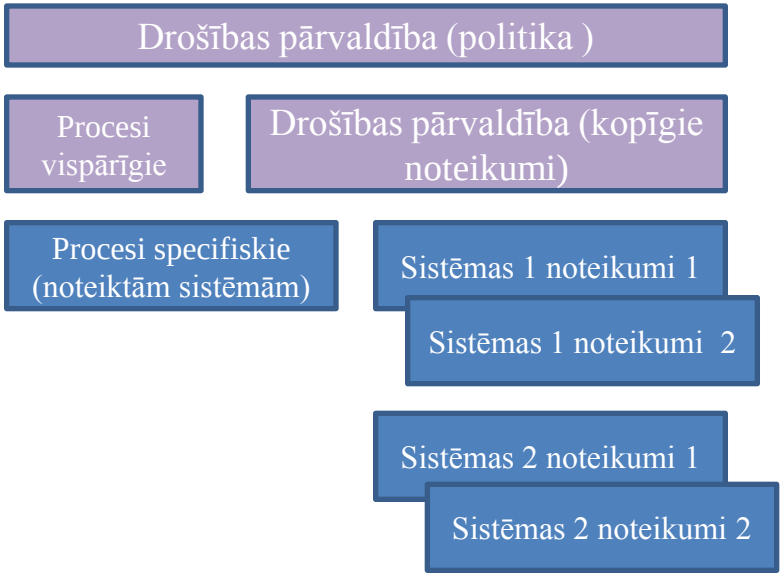



# Vēsturiskā bagāža

Privātais sektors Publiskais sektors

Informācijas drošība ir organizējama un pārvaldāma konceptuāli vienoti (ISO 2700x) …

Lai pārvaldība «strādātu un tiktu realizēta»
nedrīkstam pazaudēt pārskatāmību un savstarpējo sasaisti !




Atceramies, ka

- iekšējiem normatīvajiem aktiem var būt pielikumi vai norādes uz citiem normatīvajiem aktiem !

- Izveidojam normatīvo aktu (noteikumus) un ar vadītāju rīkojumu «sasienam kopā» konkrētu sistēmu sarakstu ar noteikumu paketi (sistēmas VAR «nepārskaitīt» pašos noteikumos )

# Pārvaldāmie resursi : darbinieki

Darbinieks kā resurss

- Izpildītāja lomā

Darbu izpilde:

- Spēja pildīt uzdevumu
  - darbinieks kā eksperts (darbinieka prasmes, kompetence, pieredze)
- spēja pārvarēt nestandarta situācijas (spēja pieņemt lēmumu, uzņemties atbildību)

Darbinieks kā resurss

- Vadītāja lomā

Darbu izpilde:

- spēja uzņemties atbildību,
- spēja aizstāvēt savu viedokli , spēja pārliecināt
- griba un prasme veikt deleģēšanu,
- spēja kontrolēt izpildīto

# Pārvaldāmie resursi, atbildība

## Darbinieks kā resurss

- Izpildītāja lomā

Darbu izpilde:

- Spēja pildīt uzdevumu
  - darbinieks kā eksperts (darbinieka prasmes, kompetence, pieredze)
- spēja pārvarēt nestandarta situācijas (spēja pieņemt lēmumu, uzņemties atbildību)

## Darbinieks kā resurss

- Vadītāja lomā

Darbu izpilde:

- spēja uzņemties atbildību,
- spēja aizstāvēt savu viedokli , spēja pārliecināt
- griba un prasme veikt deleģēšanu,
- spēja kontrolēt izpildīto

## Privātais sektors

Ir pieļaujamas darbinieku kļūdas

Vadītājs deleģē savus pienākumus, veidojot komandu !

## Publiskais sektors

Kļūdas nav pieļaujamas

Vadītājs kontrolē darbinieku darbību, kā KPI izmantojot normatīvo bāzi !

# Pārvaldāmie resursi , atbildība

## Privātais sektors

Ir pieļaujamas darbinieku kļūdas

Vadītājs deleģē savus pienākumus, veidojot komandu !

Lēmumi tiek pieņemti un realizēti komandas (darba grupas) ietvaros

Komandas locekļu aizvietojamība

Komanda nejūt kāda darbinieka iztrūkumu, elastīgi reaģē uz darbinieku pieejamību

## Publiskais sektors

Kļūdas nav pieļaujamas

Vadītājs kontrolē darbinieku darbību, kā KPI izmantojot normatīvo bāzi !

Lēmumi tiek pieņemti vai nu vadītāja līmenī vai koleģiāli, realizēti , ja apstiprina augstākā vadība

N-tie saskaņojumi + paraksts → **laiks**

Neaizvietojamu ekspertu komanda

Jebkura saslimšana vai atvaļinājums «izsit» no termiņiem

«Risinājums» -ārpakalpojums !

# Pārvaldāmie resursi, atbildība

Publiskais sektors

«Risinājums» -ārpakalpojums!

Ārpakalpojumu problemātika

- izstrāde un izmaiņas (strikta fiksācija, ko īsti gribam: ko darīt, ja tomēr mainās normatīvie akti, vēl lielāka neskaidrība, ja pasūtījums tiek veikts, kamēr normatīvais akts nav pieņemts (nav izgājis saskaņošanas ciklu !)
- uzturēšanas posms :
  - piekļuve produkcijas videi – klātienes, attālinātā
  - piekļuve produkcijas datiem – to anonimizācija, depersonalizācija (skatīt informācijas klasifikācija «Informācijas atklātības likums» (ierobežotas pieejamības informācija)
- Datu glabāšanas ārpakalpojums – vai ir pieļaujams ?
  - pieejamība – atkarība no sakaru kanāliem
  - konfidencialitāte – nodalām «neizdodamo daļu» (atslēgas) no «izdodamās» – šifrēti dati

# Pārvaldāmie resursi, atbildība

Valsts vai pašvaldību institūcija

## Iestādes vadītājs

Valsts un pašvaldību institūciju informācijas tehnoloģiju drošības pārvaldību nodrošina katras attiecīgās institūcijas vadītājs.

Institūcijas vadītājs savā pārziņā esošām sistēmām pilda Fizisko personu likumā noteiktās «pārziņa» pienākumus

## Atbildīgā persona

Valsts vai pašvaldības institūcijas vadītājs nosaka atbildīgo personu, kura īsteno informācijas tehnoloģiju drošības pārvaldību attiecīgajā institūcijā

## Novērtētājs

Sagatavo novērtējumu par personas datu apstrādes atbilstību, kas ir jāiesniedz Datu Valsts inspekcijā

# Pārvaldāmie resursi , atbildība

Valsts vai pašvaldību institūcija

## Iestādes vadītājs

Valsts un pašvaldību institūciju informācijas tehnoloģiju drošības pārvaldību nodrošina katras attiecīgās institūcijas vadītājs.

Institūcijas vadītājs savā pārziņā esošām sistēmām pilda Fiziskā persona likumā noteiktās «pārziņa» pienākumus

## Atbildīgā persona

Valsts vai pašvaldības institūcijas vadītājs nosaka atbildīgo personu, kura īsteno informācijas tehnoloģiju drošības pārvaldību attiecīgajā institūcijā

## Novērtētājs

Sagatavo novērtējumu personas datu apstrādes atbilstību, kas ir Datu Valsts inspekcijā

**Reālā situācija –** personu neesamība ar atbilstošām kompetencēm:

**Informācijas drošības vadītājs** - profesijas standarts, kods 1330 09
**personas datu aizsardzības speciālists** vai persona, kurai ir zināšanas personas datu aizsardzības jomā un kurai ir vismaz viena gada pieredze personas datu aizsardzības vai informācijas tehnoloģiju drošībā

# Pārvaldāmie resursi , atbildība

# Loma nevis amats !!

Valsts vai pašvaldību institūcija

Iestādes vadītājs

Nosaka

Pilnvaro un deleģē

## Atbildīgā persona

Valsts vai pašvaldības institūcijas vadītājs nosaka atbildīgo personu savā iestādē, kura

- **pārstāv,**
- **komunicē,**
- **koordinē**

## Ministrija

Informācijas drošības darba grupa:

**Stratēģiskā plānošana**, Minimāli nepieciešamo saistošo normatīvo aktu bāzes izstrāde un uzturēšana, vadlīnijas un labās prakses īstenošana

## IT kompetences centrs

Operatīvā plānošana, ieviešana;
Operatīvā incidentu pārvaldība;
Atbalsts (tai skaitā drošības darbu īstenošana);
Operatīvā kontrole
Personas datu apstrādes procesu uzraudzība (tai skaitā novērtējumi)

## Ministrija

Informācijas drošības kontroles (uzraudzības) funkcija

**Reālā situācija –** personu neesamība ar atbilstošām kompetencēm:

**Informācijas drošības vadītājs** - profesijas standarts, kods 1330 09
**personas datu aizsardzības speciālists** vai persona, kurai ir zināšanas personas datu aizsardzības jomā un kurai ir vismaz viena gada pieredze personas datu aizsardzības vai informācijas tehnoloģiju drošībā

Atbildīgās personas (loma kā pienākumu kopa) «sadalīšana»:

- konkrētās iestādes pārstāvniecība (paliek iestādē)
- drošības pārvaldība (normatīvie akti) - uz ministriju
- drošības pārvaldība (praktiskā) – uz IT kompetences centru
- drošības uzraudzība (kontrole) – uz ministriju

Vispārīgā datu aizsardzības regula - Ar 2017. gadu katrā publiskā sektora iestādē būs nepieciešams Fizisko personu datu aizsardzības speciālists/inspektors (sertificēts)

# Terminoloģijas radītās sekas

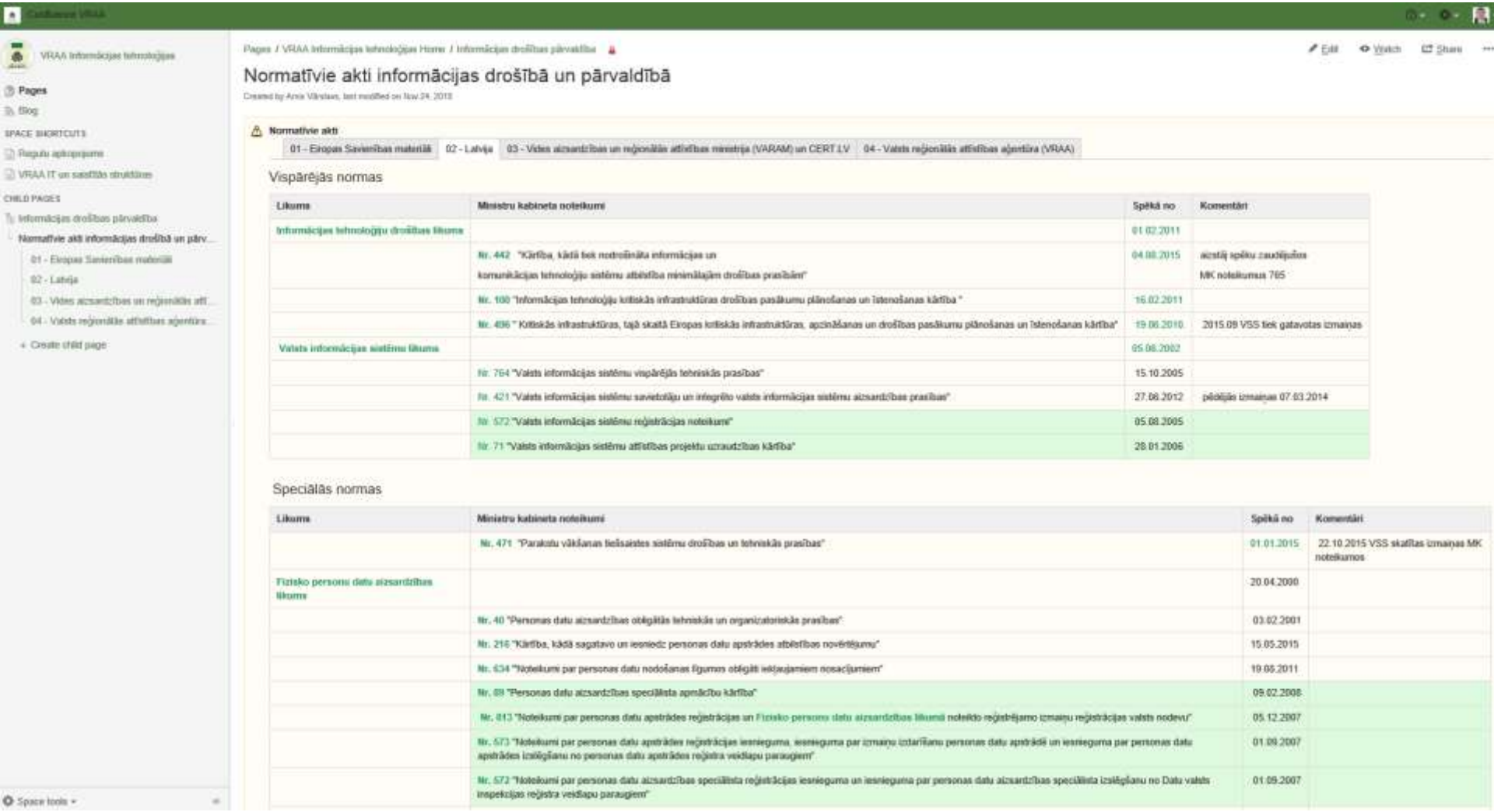
- Pārzinis, turētājs – normatīvajos aktos noteiktas kā juridiskās personas
- Juridiskās personas personalizācija notiek caur tās vadītāju
- Procedūras/noteikumi pieprasa personalizēt darbību veicējus

- Pārziņa personalizētājs – informācijas resursu valdītājs
- Turētāja personalizētājs – tehnisko resursu valdītājs

# Terminoloģijas radītās sekas

- Aģentūras informācijas sistēmas (turpmāk - Aģentūras IS) – Aģentūras pārziņā esošo valsts informācijas sistēmu, atsevišķu informācijas sistēmu un apakšsistēmu, kā arī Aģentūras darba telpās vai ārpakalpojumu sniedzēju telpās izmitināto datņu, datu, e-pasta, Web un citu serveru informācijas un tehnisko resursu apvienība, kuras ietvaros tiek uzturēti Aģentūras pārziņā esošie informācijas resursi un nodrošināta to drošība
- IS pārzinis – Aģentūra (AV: kā juridiskā persona), kas organizē un vada Aģentūras IS darbību
- IS turētājs —Aģentūra (AV: kā juridiskā persona !) vai tās pilnvarota institūcija, kas uztur Aģentūras IS informācijas un tehnisko resursu funkcionalitāti un nodrošina informācijas apriti
- IR valdītājs – Aģentūras darbinieks, kas ir atbildīgs par vienu vai vairākiem darbības procesiem organizācijā un par informācijas sistēmu (-ām), kas uztur šo(s) procesu(s).
- IS aizbildnis – darbinieks, kurš pilda IR vai TR valdītāja pienākumus pret viņa pārziņā nodoto IS resursu (resursiem) vai tā daļu (daļām)

# Apmācība – klātiene vai neklātiene ?



VRAA Informācijas tehnoloģijas

Pages

Blog

SPACE SHORTCUTS

Regulu apkopojums

VRAA IT un saistītās struktūras

CHILD PAGES

Informācijas drošības pārvaldība

Normatīvie akti informācijas drošībā un pārv...

01 - Eiropas Savienības materiāli

02 - Latvija

03 - Vides aizsardzības un reģionālās att...

04 - Valsts reģionālās attīstības aģentūra...

+ Create child page

Space tools

Pages / VRAA Informācijas tehnoloģijas Home / Informācijas drošības pārvaldība

Edit Watch Share

## Normatīvie akti informācijas drošībā un pārvaldībā

Created by Arnis Vārslavs, last modified on Nov 24, 2015

**Normatīvie akti**

01 - Eiropas Savienības materiāli | 02 - Latvija | 03 - Vides aizsardzības un reģionālās attīstības ministrija (VARAM) un CERT.LV | 04 - Valsts reģionālās attīstības aģentūra (VRAA)

### Vispārējās normas

| Likums | Ministru kabineta noteikumi | Spēkā no | Komentāri |
|---|---|---|---|
| Informācijas tehnoloģiju drošības likums | | 01.02.2011 | |
| | Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" | 04.08.2015 | aizstāj spēku zaudējušos MK noteikumus 765 |
| | Nr. 100 "Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība " | 16.02.2011 | |
| | Nr. 496 " Kritiskās infrastruktūras, tajā skaitā Eiropas kritiskās infrastruktūras, apzināšanas un drošības pasākumu plānošanas un īstenošanas kārtība" | 19.06.2010. | 2015.09 VSS tiek gatavotas izmaiņas |
| Valsts informācijas sistēmu likums | | 05.06.2002 | |
| | Nr. 764 "Valsts informācijas sistēmu vispārējās tehniskās prasības" | 15.10.2005 | |
| | Nr. 421 "Valsts informācijas sistēmu savietotāju un integrēto valsts informācijas sistēmu aizsardzības prasības" | 27.06.2012 | pēdējās izmaiņas 07.03.2014 |
| | Nr. 572 "Valsts informācijas sistēmu reģistrācijas noteikumi" | 05.08.2005 | |
| | Nr. 71 "Valsts informācijas sistēmu attīstības projektu uzraudzības kārtība" | 28.01.2006 | |

### Speciālās normas

| Likums | Ministru kabineta noteikumi | Spēkā no | Komentāri |
|---|---|---|---|
| | Nr. 471 "Parakstu vākšanas tiešsaistes sistēmu drošības un tehniskās prasības" | 01.01.2015 | 22.10.2015 VSS skatīšas izmaiņas MK noteikumos |
| Fizisko personu datu aizsardzības likums | | 20.04.2000 | |
| | Nr. 40 "Personas datu aizsardzības obligātās tehniskās un organizatoriskās prasības" | 03.02.2001 | |
| | Nr. 216 "Kārtība, kādā sagatavo un iesniedz personas datu apstrādes atbilstības novērtējumu" | 15.05.2015 | |
| | Nr. 634 "Noteikumi par personas datu nodošanas līgumos obligāti ietverjamiem nosacījumiem" | 19.06.2011 | |
| | Nr. 89 "Personas datu aizsardzības speciālista apmācību kārtība" | 09.02.2008 | |
| | Nr. 813 "Noteikumi par personas datu apstrādes reģistrācijas un Fizisko personu datu aizsardzības likumā noteikto reģistrējamo izmaiņu reģistrācijas valsts nodevu" | 05.12.2007 | |
| | Nr. 573 "Noteikumi par personas datu apstrādes reģistrācijas iesnieguma, iesnieguma par izmaiņu izdarīšanu personas datu apstrādē un iesnieguma par personas datu apstrādes izslēgšanu no personas datu apstrādes reģistra veidlapu paraugiem" | 01.09.2007 | |
| | Nr. 572 "Noteikumi par personas datu aizsardzības speciālista reģistrācijas iesnieguma un iesnieguma par personas datu aizsardzības speciālista izslēgšanu no Datu valsts inspekcijas reģistra veidlapu paraugiem" | 01.09.2007 | |

# Apmācība – klātiene un neklātiene

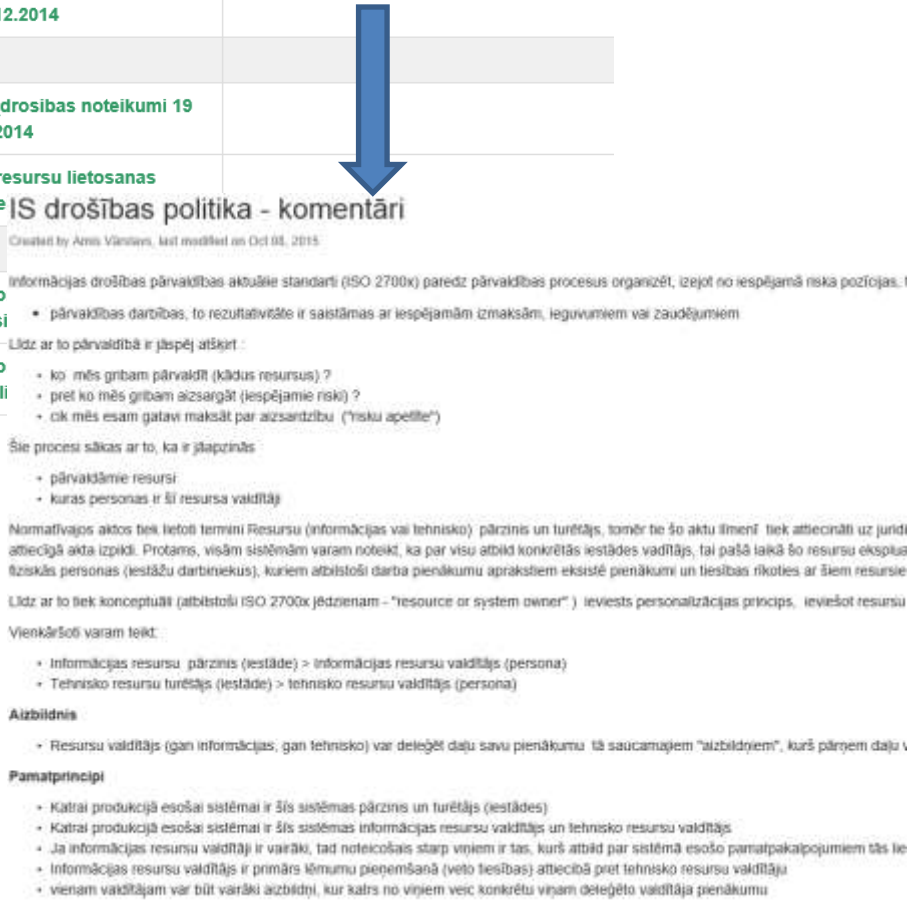
Pages / ... / Normatīvie akti informācijas drošībā un pārvaldībā

Edit

## 04 - Valsts reģionālās attīstības aģentūra (VRAA)

Created by Arnis Vārslavs, last modified on Apr 11, 2016

| Grupa | Pamatredakcija (PDF) | izmaiņas | Aktuālā konsolidētā redakcija ( Word) | Vadlīnijas un komentāri |
|---|---|---|---|---|
| Informācijas drošības politika | IS_drosibas_politika 19.09.2014 | izmaiņas 01 | IS_drosibas_politika 11.12.2014 | IS drošības politika - komentāri |
| | | | | |
| Noteikumi | IS drosibas noteikumi 19 09 2014 | | IS_drosibas noteikumi 19 09.2014 | |
| | IS_resursu lietosanas_noteikumi 2012 | | IS resursu lietosanas note | |
| | | | | |
| Procedūras (vispārējās) | IR klasifikācijas noteikumi 19 09 2014 | | Info klasi | |
| | IS riska analizes noteikumi 19 09 2014 | | Info anali | |
| | IS lietojumprogrammatūras izmaiņu pieteikumu apstiprināšanas noteikumi 2015 | | | |



IS drošības politika - komentāri

Created by Arnis Vārslavs, last modified on Oct 08, 2015

Informācijas drošības pārvaldības aktuālie standarti (ISO 2700x) paredz pārvaldības procesus organizēt, izejot no iespējamā riska pozīcijas.

- pārvaldības darbības, to rezultativitāte ir saistāmas ar iespējamām izmaksām, ieguvumiem vai zaudējumiem

Līdz ar to pārvaldībā ir jāspēj atšķirt :

- ko mēs gribam pārvaldīt (kādus resursus) ?
- pret ko mēs gribam aizsargāt (iespējamie riski) ?
- cik mēs esam gatavi maksāt par aizsardzību ("risku apetīte")

Šie procesi sākas ar to, ka ir jāapzinās

- pārvaldāmie resursi
- kuras personas ir šī resursa valdītāji

Normatīvajos aktos tiek lietoti termini Resursu (informācijas vai tehnisko) pārzinis un turētājs, tomēr tie šo aktu ilmenī tiek attiecināti uz juridi attiecīgā akta izpildi. Protams, visām sistēmām varam noteikt, ka par visu atbild konkrētās iestādes vadītājs, tai pašā laikā šo resursu ekspluā fiziskās personas (iestāžu darbiniekus), kuriem atbilstoši darba pienākumu apraksttiem eksistē pienākumi un tiesības rīkoties ar šiem resursie

Līdz ar to tiek konceptuāli (atbilstoši ISO 2700x jēdzienam - "resource or system owner" ) ieviests personalizācijas princips, ieviešot resursu

Vienkāršoti varam teikt:

- Informācijas resursu pārzinis (iestāde) > informācijas resursu valdītājs (persona)
- Tehnisko resursu turētājs (iestāde) > tehnisko resursu valdītājs (persona)

**Aizbildnis**

- Resursu valdītājs (gan informācijas, gan tehnisko) var deleģēt daļu savu pienākumu tā saucamajiem "aizbildņiem", kuŗš pārņem daļu v

**Pamatprincipi**

- Katrai produkcijā esošai sistēmai ir šīs sistēmas pārzinis un turētājs (iestādes)
- Katrai produkcijā esošai sistēmai ir šīs sistēmas informācijas resursu valdītājs un tehnisko resursu valdītājs
- Ja informācijas resursu valdītāji ir vairāki, tad noteicošais starp viņiem ir tas, kuŗš atbild par sistēmā esošo pamatpakalpojumiem tās ie
- Informācijas resursu valdītājs ir primārs lēmumu pieņemšanā (veto tiesības) attiecībā pret tehnisko resursu valdītāju
- vienam valdītājam var būt vairāki aizbildņi, kur katrs no viņiem veic konkrētu viņam deleģēto valdītāja pienākumu

# Apmācība – klātiene un neklātiene

VRAA informācijas resursu reģistrs

Created by Arnis Vārslavs, last modified on Apr 11, 2016

| Rīkojumi | Datums | Komentāri |
|---|---|---|
| Rīkojums par atbildīgām personām | 06.04.2016 | skaidrojums par personu lomām |

Struktūrvienību vadītāji

00 - paskaidrojumi - VRAA Informācijas resursu reģistrs

Created by Arnis Vārslavs, last modified on Oct 13, 2015

Termiņu skaidrojumi ( Valsts reģionālās attīstības aģentūras informācijas sistēmu drošības KĀRTĪBA )

VRAA Informācijas tehnoloģijas / Pages / ... / VRAA informācijas resursu reģistrs / 04 Riska grupas ( VRAA IR klasifikācijas

# 04 Riska grupas ( VRAA IR klasifikācijas grupas )

No iekšējās kārtības "Valsts reģionālās attīstības aģentūras informācijas resursu klasifikācijas noteikumi" - Visas IS var tikt ie

IS ir uzskatāma par **augsta (R1) riska sistēmu**, ja izpildās **vismaz viena no** sekojošām pazīmēm:

- IS atbild par kādu no drošības infrastruktūras funkcionālo komponenti – pilda AD (Active Directory), ugunssienas, IDS (
- Sistēma apstrādā K1 vai augstāka konfidencialitātes līmeņa informāciju;
- Sistēma apstrādā V1 (augstas vērtības) līmeņa informāciju;
- Sistēma ir ārēji (publiskajā tīklā) eksponēta un ir iesaistīta Aģentūras publiski pieejamo pakalpojumu darbības nodrošinā
- Sistēma apstrādā sensitīvus personas datus;
- Sistēma ir valsts nozīmes IS.

IS ir uzskatāma par **zema (R3) riska sistēmu,** ja izpildās **visas sekojošās** prasības:

- sistēma apstrādā tikai K2 – vispārpieejamu konfidencialitātes līmeņa informāciju;
- sistēma apstrādā V3 (zemas vērtības ) līmeņa informāciju;
- sistēma nestrādā ar personas datiem;

IS ir uzskatāma par **vidēja (R2) riska sistēmu visos pārējos gadījumos**.

pārējos gadījumos sistēma ir uzskatāma par pamata drošības sistēmu.

| | C klase |
|---|---|
| ...ma neplānotam ...ajā darba laikā jābūt **ne** ...kārt) **mēnesī**, ...ām stundām (summāri) | ja sistēmas nodrošinātā pakalpojum neplānots pārtraukums sistēmas paredzētajā darba laikā **drīkst būt i par 24 stundām mēnesī** (summāri) |
| ...integritātes apdraudējums **rada** ...drošināšanai | ja sistēmā glabāto datu integritātes apdraudējums **nerada risku** institūc pamatfunkciju nodrošināšanai |
| ...s pieejamības informācija ...ai sistēmā glabātās ...noplūdes vienīgās sekas ir ...u institūciju vai Latvijas | ja sistēma satur **tikai publiski pieej informāciju** vai sistēmā glabātās informācijas neatļauta izpaušana va noplūde nerada risku institūcijai |

...uzskatāma par paaugstinātas drošības sistēmu,

# Jautājumi ?

Arnis Vārslavs
Arnis.varslavs@vraa.gov.lv 29226945