Informācijas un informācijas resursu klasifikācijas procedūra

SIGNET
PRIVATE BANK

Saturs

I Izmantotie termini

1. **Banka** – Signet Bank AS.
2. **DD** – Bankas Drošības daļa.
3. **Informācija vai Dokuments** – ziņas (dati), kurām ir jēga un saturiska interpretācija, kas radušās, saņemtas vai pārvērstas citā formā, uz jebkura informācijas nesēja, ierosinot, turpinot, mainot vai izbeidzot kādu darbību, un kas apliecina šo darbību.
4. **Informācijas vai dokumenta īpašnieks** – Bankas darbinieks, kas ir radījis informāciju/ dokumentu vai to saņēmis no trešajām personām (ārpus Bankas).
5. **Informācijas integritāte** – raksturo, cik lielā mērā informācija ir pilnīga, patiesa, precīza un aktuāla.
6. **Informācijas konfidencialitāte** – piekļuves nodrošināšana informācijai tikai pilnvarotām personām vai procesiem.

7. **Informācijas pieejamība** – raksturo, vai Lietotāji var piekļūt nepieciešamajai informācijai ne vēlāk kā noteiktā laikā pēc informācijas pieprasīšanas brīža.
8. **Informācijas vērtība** – informācijas nozīmīgums Bankas darbības nodrošināšanai.
9. **IR** – informācijas resursi (informācijas vienības, kurās ietilpst datu datnes, kas satur IS glabājamo, apstrādājamo un IS Lietotājiem pieejamo informāciju, kā arī visi IS ievades un izvades dokumenti neatkarīgi no datu nesēja veida).
10. **IR turētājs** – persona, kas ir atbildīga par IR un rīkojas ar tiem Bankas pienākumu/ funkciju veikšanai.
11. **IS** – informācijas sistēma; informācijas ievades, uzglabāšanas un apstrādes datorizēta sistēma, kas nodrošina noteikto funkciju izpildi un paredz Lietotāja pieeju tajā glabātajiem datiem vai informācijai.
12. **IS auditācijas pieraksti** – analīzei pieejami pieraksti, kuros reģistrēti dati par noteiktiem notikumiem IS (piekļuve, datu ievade, maiņa, dzēšana, izvade u.c.).
13. **ITD** – Bankas IT daļa.
14. ***First North*** – tirgus daudzpusējā tirdzniecības sistēma, ko izveido un pārvalda *Nasdaq Riga*, bet kas nav regulētais tirgus Finanšu instrumentu tirgus likuma un citu normatīvo aktu izpratnē.
15. **Grupa** – Banka un tās meitas sabiedrības.
16. **Klienta pārstāvis** – Klienta likumiskais pārstāvis (fiziska persona, kura pārstāv citu fizisko personu vai juridisko personu uz likuma pamata (aizbildnis, aizgādnis, persona ar tiesībām pārstāvēt sabiedrību, piemēram, valdes loceklis utt.) vai Klienta līgumiskais pārstāvis (fiziska persona, kura pārstāv citu fizisko personu vai juridisko personu uz pilnvaras pamata, kā arī prokūrists).
17. **Klients** – Procedūras izpratnē: fiziskā vai juridiskā persona, kurai Banka sniedz finanšu pakalpojumus, t.sk. Sertificētā konsultanta pakalpojumus.
18. **Konfidenciālā informācija** – jebkāda Bankas vai tās Klientu, vai sadarbības partneru informācija, kas nav publiska informācija.
19. **Lietotājs** – darbinieks, kurš izpilda noteiktus pienākumus, atbilstoši kuriem viņam ir piešķirtas tiesības lietot noteiktus IS resursus.
20. **Procedūra** – Bankas iekšējais normatīvais dokuments „Informācijas un Informācijas sistēmu resursu klasifikācijas procedūra".
21. **RAP** – Bankas Risku un atbilstības pārvalde.
22. **Sertificētais konsultants** - juridiska persona, kas atbilst *Nasdaq Riga Alternatīvā tirgus First North* noteikumu prasībām un ir noslēgusi līgumu ar *Nasdaq Riga* par palīdzības sniegšanu emitentiem un Sertificēta konsultanta pienākumu veikšanu *First North* tirgū.
23. **„Tīrā galda politika"** – darbinieka uzvedība/ rīcība, kas balstīta uz savas darba vietas sakārtošanu, nodrošinot Konfidenciālas informācijas glabāšanas/ iznīcināšanas prasības.

24. **TR** - tehnoloģiskie resursi (IS sastāvdaļa, kurā ietilpst sistēmprogrammas, lietojumprogrammas, palīgprogrammas, sistēmas datnes, datori, datortīkli, aparatūra un citas iekārtas, kas nodrošina IS darbību).
25. **TR turētājs** – Bankas pilnvarots ITD darbinieks, kas ir atbildīgs par TR.

II Vispārīgie noteikumi

26. Procedūra nosaka kārtību, kādā Bankā tiek veikta Informācijas un IR klasifikācija.
27. Procedūrā noteiktie Informācijas un IR klasifikācijas principi tiek pielietoti visās Grupas sabiedrībās.
28. Bankas meitas sabiedrības, ņemot vērā to biznesa modeļus, var izstrādāt un apstiprināt savus iekšējos normatīvos dokumentus, kas detalizēti regulē dažādus ar Informācijas un IR klasifikāciju saistītus jautājumus, ievērojot Procedūrā noteiktos principus. Gadījumā, ja meitas sabiedrība izvēlas neizstrādāt atsevišķu Informācijas un IR klasifikācijas procedūru, šī Procedūra ir tai saistoša pilnā mērā.
29. Katrā Grupas sabiedrībā ir noteikta par informācijas un IR klasifikācijas jautājumiem atbildīgā struktūrvienība/ persona/ koleģiālā institūcija (turpmāk – Atbildīgā struktūrvienība).
30. Informācijas un IR klasifikācijas mērķis ir novērtēt Informācijas un IR nozīmību un nodrošināt to aizsardzību atbilstoši nozīmībai un piemērojamajiem operacionālajiem un drošības riskiem.
31. Procedūra balstās uz principu, ka klasificējama ir visa Informācija/ IR, neatkarīgi no informācijas nesēja.
32. Katras Bankas struktūrvienības vadītājs atbild par savā pakļautībā esošo darbinieku iepazīstināšanu ar Informācijas un IR klasificēšanu.
33. Bankas valdes locekļi un darbinieki ir atbildīgi par Informācijas un IR lietošanu Procedūrā noteiktajā kārtībā. Rīcība, kas būs pretēja Procedūrā noteiktajam, tiks uzskatīta par darba līguma pārkāpumu.
34. Visai Informācijai, kas saistīta ar Bankas darbību, jābūt klasificētai saskaņā ar Procedūru, un darbiniekiem ar to jārīkojas atbilstoši attiecīgai klasifikācijas grupai. Informācijas klasificēšanas grupa sniedz darbiniekam priekšstatu par Dokumenta saturu, piekļuves tiesībām Dokumentam un/vai Informācijai, kā arī par to, kā apstrādāt un aizsargāt Dokumentu un tajā esošo Informāciju.
35. Kopējot, drukājot vai citādā veidā izmainot Dokumenta formu un strādājot ar Dokumenta oriģināla atvasinājumiem, jāievēro tādi paši noteikumi, kā darbā ar Dokumenta oriģinālu.
36. Lai novērstu risku, ka Konfidenciālai informācijai var piekļūt nepiederošas personas, strādājot ar Dokumentiem, darbiniekam jāievēro „Tīrā galda politika".
37. Atrodoties ārpus Bankas telpām, darbiniekam ir atļauts strādāt ar Konfidenciālu informāciju tikai tad, ja tiek nodrošināts, ka tās saturs nav pieejams trešajām

personām.

38. Konfidenciālu informāciju drīkst apstrādāt tikai Bankas apstiprinātos un atbilstoši aizsargātos galda datoros, klēpjdatoros un citās informācijas tehnoloģiju ierīcēs (piemēram, mobilajos tālruņos).
39. ITD Bankā veido un uztur IS sarakstu. Bankas struktūrvienību vadītāju pienākums ir informēt ITD par viņu pakļautībā esošo struktūrvienību izmantotajām IS.
40. Pamatojoties uz Informācijas un IR klasifikāciju, Banka izvērtē tai piemītošos riskus un tos ņem vērā, veidojot savu infrastruktūru/ vidi – iestrādājot kontroles, aizsardzības sistēmas (piekļuves kontrole, serveru telpas, seifus, metāla skapjus, iekšējos tīklus, uguns sienas, *VPN* tuneļus utt.).
41. Informācijas un informācijas resursu klasifikācija tiek organizēta, ievērojot tiesību aktu prasības un labo praksi fizisko personu datu aizsardzības jomā.
42. Procedūru, kā arī tās grozījumus un papildinājumus apstiprina Bankas valde.
43. Procedūra stājas spēkā ar tās apstiprināšanas brīdi, un ar tās apstiprināšanu spēku zaudē 06.11.2018. apstiprināts Bankas iekšējais normatīvais dokuments „Informācijas un informācijas resursu klasifikācijas procedūra ”.
44. Procedūra ir saistoša visiem Bankas darbiniekiem.

III Informācijas klasificēšana un tās lietošanas pamatprincipi

A. Vispārīgie noteikumi

45. Visu Bankā esošo Informāciju (t.sk. Dokumentus) klasificē vienā no 3 (trim) Informācijas klasifikācijas grupām, kuru nosaka atbilstoši Informācijas saturam:
    - 45.1. Publiskā informācija;
    - 45.2. Iekšējā jeb dienesta lietošanas informācija;
    - 45.3. Ierobežotas pieejas informācija.
46. Informācijas un/ vai Dokumenta īpašnieks nosaka, kurai Informācijas klasifikācijas grupai Informācija/ Dokuments pieder.
47. Informācijas un/ vai Dokumenta īpašnieks savas kompetences ietvaros var noteikt papildu Informācijas un/ vai Dokumenta lietošanas ierobežojumus:
    - 47.1. ierobežot personu loku, kam ir tiesības iepazīties ar Informāciju un/ vai Dokumentu;
    - 47.2. noteikt Informācijas un/ vai Dokumenta apjomu un to ierobežoto pavairošanu (noteikts eksemplāru skaits);
    - 47.3. noteikt pārsūtīšanas ierobežojums (piemēram, tiek nodots ar pavadvēstuli, pieņemšanas - nodošanas aktu, pārsūtīšana tiek saskaņota ar informācijas īpašnieku utt.);
    - 47.4. noteikt glabāšanas ierobežojums (piemēram, pēc konkrēta laika iznīcināms, glabājams seifā utt.).
48. Dokumentiem, kuriem Informācijas klasifikācijas grupa ir mainīga, Dokumenta

īpašnieks tā sagatavošanas laikā vai pēc Informācijas statusa maiņas Dokumentā norāda tā jauno klasificēšanas grupu (piemēram, gada pārskati sākotnēji ir Ierobežotas pieejamības, taču pēc to publicēšanas tie kļūst Publiski dokumenti). Šādā gadījumā Dokumenta īpašnieks rīkojas sekojoši:

48.1. Dokumenta izstrādes sākumā kopā ar sākotnējo klasificēšanas grupu norāda nākotnes statusu un izmaiņu termiņu; vai

48.2. nomaina Dokumenta klasificēšanas grupu Dokumentā pēc tā publicēšanas.

49. Dokumenta saņēmējs nedrīkst mainīt Dokumenta klasifikāciju bez iepriekšējas saskaņošanas ar Informācijas/ Dokumenta īpašnieku.

50. Ja nosakot Informācijas un/ vai Dokumenta klasifikācijas grupu, Dokumenta īpašniekam rodas šaubas par to, kurai Informācijas klasificēšanas grupai Informācija un/ vai Dokuments atbilst, viņš konsultējas ar savu tiešo vadītāju. Neskaidrību gadījumā var konsultēties ar DD vai RAP.

51. Informācijas klasifikācijas principi tiek piemēroti, veicot IR un Bankas Lietu nomenklatūras klasifikāciju.

B. Publiskā informācija

52. **Publiskā informācija** – Informācija, kas ir oficiāli publiskota vai ir pieejama no publiska avota, piemēram:

52.1. Klientiem pieejamie mārketinga un reklāmas materiāli;

52.2. Bankas paziņojumi medijiem (plašsaziņas līdzekļiem);

52.3. Bankas tīmekļa vietnē publicētā Informācija, t.sk. Klientiem pieejamie Bankas līgumu noteikumu apraksti, iesniegumi, tarifi utt.;

52.4. Dokumenti, kas lejupielādēti no tīmekļa vietnēm, kurām nav noteikti piekļuves ierobežojumi (valsts pārvaldes iestāžu dokumenti, likumprojekti, normatīvie akti);

52.5. Bankas finanšu rādītāji pēc to publicēšanas utt.

53. Šo statusu izmanto, lai norādītu, ka Informācija un/ vai Dokuments nav īpaši jāaizsargā.

54. Publiski pieejamo Informāciju var brīvi pārsūtīt, nodot trešajām personām. Publiskās Informācijas un/ vai Dokumentu glabāšanu un iznīcināšanu Banka nekontrolē. Drukātus un tipogrāfiski iespiestus publiskos dokumentus drīkst nodot makulatūrā.

55. Publiskā informācija var saturēt personas datus tikai tad, ja pastāv attiecīgais tiesiskais pamats, piemēram, finanšu pārskatos tiek iekļauti Bankas padomes un valdes locekļu personas dati, jo pastāv tiesiskais pamats - uz Banku kā uz pārzini ir attiecināms juridisks pienākums, kas izriet no normatīvajiem aktiem finanšu pārskatu sagatavošanas jomā, atklāt šāda veida informāciju. Apstrādājot Publisko informāciju, Darbiniekam rūpīgi jāizvērtē, vai Publiskā informācija satur personas datus un vai pastāv tiesiskais pamats tos apstrādāt (t. sk. publiskot).

C. Iekšējā jeb dienesta lietošanas informācija

56. **<u>Iekšējā jeb dienesta lietošanas informācija</u>** – Informācija, kas ir pieejama visiem darbiniekiem viņu kompetences ietvaros, taču nav izpaužama trešajām personām bez īpaša pilnvarojuma, piemēram:
    56.1. Bankas iekšējie normatīvie dokumenti (instrukcijas, procedūras, noteikumi, nolikumi, politikas, stratēģijas utt.), ja tiem nav noteikta ierobežota pieejamība;
    56.2. Bankas IS dokumentācija (lietošanas rokasgrāmatas);
    56.3. Bankas projektu dokumentācija, ja tai nav noteikta ierobežota pieejamība;
    56.4. Informācija no *Mysignet* u.c. informatīvām aplikācijām;
    56.5. Bankas iekšējie tālruņa numuri un kontaktinformācija utt.
57. Iekšējai informācijai drīkst piekļūt visi darbinieki, taču to nedrīkst izpaust vai citādā veidā atļaut piekļuvi trešajām personām, izņemot LR normatīvajos aktos paredzētajos gadījumos, Bankas noteiktajā kārtībā, kā arī ar Bankas valdes pilnvarojumu.
58. Rīcību ar Iekšējo informāciju nosaka tabula Nr.1 „Iekšējās informācijas lietošanas pamatprincipi".

Tabula Nr.1

„Iekšējās informācijas lietošanas pamatprincipi"

Rīcība	Papīrveidā	Elektroniski
Informācija brīvi pārvietojama/ izmantojama Bankas iekšējos tīklos un iekšējā e-pasta ietvaros		X
Dokumentu pārsūtīšana ar ierakstītu vēstuli vai kurjeru	X	
Uzglabāšana skapjos un atvilktnēs	X	
Dokumenta iznīcināšana smalcināšanas iekārtā	X	
Uzglabāšana Bankas servera iekšējos tīklos		X
Pārdomāta Dokumenta oriģinālu atvasinājumu lietošana (pēc to izmantošanas informācija iznīcināma)	X	X
Aizliegts lasīt nepilnvarotu personu klātbūtnē, ja saturs var tikt atklāts trešajām personām	X	X
Dokumentu pārsūtīšana trešajai pusei, ja ir saņemts pilnvarojums (Procedūras 57. punktā minētais)		Šifrēta / ar paroli aizsargāta datne
Personas datu apstrāde tikai tad, ja pastāv tiesiskais pamats, ievērojot Bankas iekšējā normatīvajā dokumentā „Privātuma politika" noteiktos principus, t. sk. attiecībā uz apstrādes nolūka ierobežojumu un datu minimizēšanu	X	X

D. <u>Ierobežotas pieejas informācija</u>

59. **<u>Ierobežotas pieejas informācija</u>** – nozīmīga iekšējā informācija, kuras izpaušanas rezultātā Bankai var rasties ne tikai materiāli, bet arī reputācijas zaudējumi. Ierobežotas pieejas informācija ir pieejama tikai tiem darbiniekiem, kuriem tā ir nepieciešama tiešo amata pienākumu veikšanai, piemēram:

59.1. Informācija par Bankas klientiem (t.sk., saskaņā ar Kredītiestāžu likuma 61. panta pirmajā daļā minēto);

59.2. Informācija par Bankas darbinieku atalgojumu un motivācijas programmām;

59.3. Informācija par Bankas potenciāliem Klientiem, sadarbības partneriem;

59.4. Bankas gada pārskati un cita finanšu informācija pirms tās publicēšanas;

59.5. IS drošības arhitektūra, Lietotāju paroles, Informācija par īpašās piekļuves objektiem (vērtību glabātuve, serveru telpa, depozitārijs, arhīvs utt.);

59.6. iekšējo un ārējo auditu pārskati par Bankas darbību;

59.7. sarakste ar FKTK;

59.8. stratēģiskie plāni, Klientu piesaistes stratēģijas utt.

60. Ierobežotas pieejas informāciju ir aizliegts atklāti izplatīt, parādīt vai padarīt pieejamu personām, kuras šai Informācijai nedrīkst piekļūt, izņemot situācijas, kad Informācija var tikt atklāta valsts pārvaldes un citām oficiālām iestādēm, pamatojoties uz Kredītiestāžu likuma 62. – 63. pantiem, un citiem normatīviem dokumentiem, sadarbības partneru noslēgtiem līgumiem, kas reglamentē ierobežotas pieejas informācijas sniegšanu utt.

61. Struktūrvienības vadītājs ir atbildīgs par Ierobežotas pieejas dokumentu glabāšanas noteikumu ievērošanu struktūrvienībā.

62. Rīcību ar Ierobežotas pieejas informāciju nosaka tabula Nr.2 „Ierobežotas informācijas lietošanas pamatprincipi”.

Tabula Nr.2

„Ierobežotas informācijas lietošanas pamatprincipi”

Rīcība	**Papīrveidā**	**Elektroniski**
Dokumentu reģistrēšana atbilstoši Bankas Lietu nomenklatūrai	X	X
Informācija izmantojama Bankas iekšējos tīklos un iekšējā e-pasta ietvaros		X
Pārdomāta Dokumenta oriģinālu atvasinājumu lietošana (pēc to izmantošanas informācija iznīcināma)	X	X
Uzglabāšana Bankas servera iekšējos tīklos ar definētām piekļuves tiesībām		X
Uzglabāšana slēdzamos skapjos un atvilktnēs	X	
Informācijas pārsūtīšana, t.sk. Klientiem, sadarbības partneriem, tikai šifrētā veidā IZŅĒMUMS: pārsūtot Klienta datus, tos var nešifrēt, ja informācija nesatur cita klienta datus un Klients akceptē iespējamos riskus (saskaņā ar FKTK „Informācijas sistēmu drošības normatīvie noteikumu” 67. punktu: „67. Pārsūtot klienta datus, tos aizsargā ar kriptogrāfijas līdzekļiem. Pārsūtot klienta datus, tos var nešifrēt, ja informācija nesatur cita klienta datus un klients akceptē iespējamos riskus.” Visos pārējos gadījumos Bankas darbinieka pienākums ir izmantot risinājumu *Secure Web mail* saskaņā ar lietošanas instrukciju, kas ir pieejama *Mysignet*.		X
Ierobežota pieeja elektroniska formāta Dokumentiem		X
Tikai šifrēto ārējo elektroniskās Informācijas nesēju (ārējie diski, USB		X

atmiņu kartes utt.) izmantošana		
Informācija izpaužama tikai saskaņā ar Kredītiestāžu likuma 62. – 63. pantiem	X	X
Aizliegts lasīt nepilnvarotu personu klātbūtnē, ja saturs var tikt atklāts trešajām personām	X	X
Dokumenta iznīcināšana smalcināšanas iekārtā	X	
Elektronisko datu nesēju iznīcināšana atbilstoši Bankas iekšējam normatīvajam dokumentam „Informācijas un komunikāciju tehnoloģiju iekārtu, kas var saturēt datu nesējus, un datu nesēju iznīcināšanas procedūra”		X
Personas datu apstrāde tikai tad, ja pastāv tiesiskais pamats, ievērojot Bankas iekšējā normatīvajā dokumentā „Privātuma politika” noteiktos principus, t. sk. attiecībā uz apstrādes nolūka ierobežojumu un datu minimizēšanu	X	X

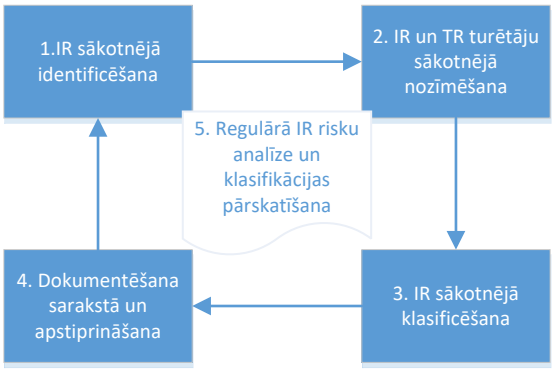
E. Dokumentu marķēšana

63. Informācijas/ Dokumenta īpašnieks izlemj, vai Dokumentam piemērojama īpaša aizsardzības un/ vai apstrādes režīms (piemēram, Dokumentam drīkst būt pieeja tikai noteiktam darbinieku lokam, vai Informācijai jābūt šifrētai utt.). Ja Dokumentam ir vajadzīga īpaša aizsardzība, tad marķējot dokumentu, Dokumenta īpašnieks to norāda.
64. Marķējumu norāda Dokumenta katras lapas augšējā daļā (*Header*) un, ja izmantotais programmnodrošinājums to atļauj, tad pievienojot datnei norādi „Ierobežotas piekļuves”.
65. Ja darbinieks nosūta klasificēto Informāciju elektroniski (elektroniskais pasts, SMS utt.), viņš lieto Informācijas marķēšanu. Piemēram, nosūtot elektronisko pastu, darbinieks ailē *Subject* norāda Informācijas klasificēšanas līmeni.
66. Dokumenta marķēšanu neveic tam Dokumenta eksemplāram, kas ir paredzēts nosūtīšanai adresātam ārpus Bankas.

IV IR klasifikācija

A. Vispārīgie noteikumi

67. IR klasifikācijas piešķiršanas un pārskatīšanas process sastāv no 5 (pieciem) posmiem (sk. attēlu Nr. 1 „Informācijas resursu klasifikācijas process”):



Att. Nr. 1 „Informācijas resursu klasifikācijas process”

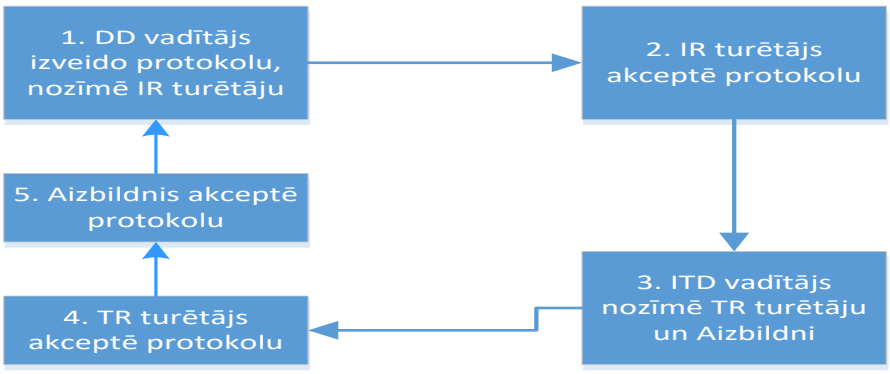
B. IR sākotnējā identificēšana

68. Bankas struktūrvienību vadītājs identificē valdījumā/ rīcībā esošos/ plānotos nozīmīgos IR un elektroniski informē par tiem ITD un DD.

C. IR turētāja un TR turētāja sākotnējā nozīmēšana/ maiņa/ anulēšana

69. IR turētāja un TR turētāja sākotnējā nozīmēšana/ maiņa/ anulēšana notiek, izmantojot *Mysignet* (sk. pielikumu Nr. 1 „Turētāju nozīmēšanas/ maiņas/ anulēšanas instrukcija").

70. IR turētāja, TR turētāja un TR turētāja aizbildņa sākotnējās nozīmēšana ir grafiski atspoguļota attēlā Nr. 2 „IR turētāja, TR turētāja un TR turētāja aizbildņa nozīmēšanas process".



Att. Nr. 2 „IR turētāja, TR turētāja un TR turētāja aizbildņa nozīmēšanas process"

71. DD vadītājs katram IR izveido „Turētāju nozīmēšanas protokolu" un pārsūta to potenciālajam IR turētājam akceptēšanai. Akceptējot protokolu, IR turētājs apstiprina, ka iepazinās ar IR turētāja pienākumiem un tiesībām, kas izklāstīti Procedūras V sadaļā „IR turētāju, TR turētāju un DD tiesības un pienākumi", un apņemas tos ievērot. IR turētāja akceptētais protokols automātiski tiek pārsūtīts ITD vadītājam.

72. ITD vadītājs nozīmē TR turētāju un TR turētāja aizbildni un ieraksta tos protokolā. Protokols tiek automātiski pārsūtīts TR turētājam akceptēšanai. Akceptējot protokolu, TR turētājs apstiprina, ka iepazinās ar TR turētāja pienākumiem un tiesībām, kas izklāstīti Procedūras V sadaļā „IR turētāju, TR turētāju un DD tiesības un pienākumi", un apņemas tos ievērot. TR turētāja akceptētais protokols automātiski tiek pārsūtīts TR turētāja aizbildnim akceptēšanai. Akceptējot protokolu, TR turētāja aizbildnis apstiprina, ka iepazinās ar TR turētāja pienākumiem un tiesībām, kas izklāstīti Procedūras V sadaļā „IR turētāju, TR turētāju un DD tiesības un pienākumi", un apņemas tos ievērot.

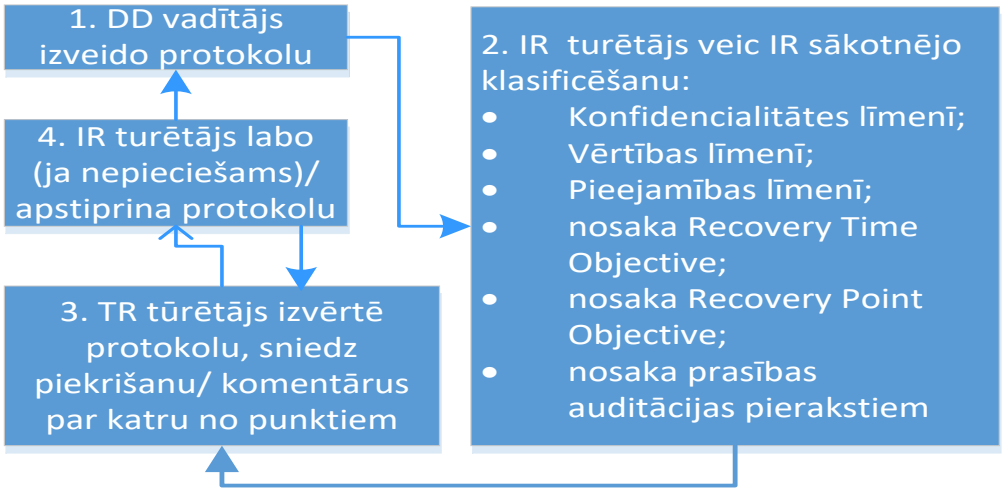
73. Gadījumā, ja rodas nepieciešamība mainīt/ anulēt IR turētāju, TR turētāju vai TR turētāja aizbildni, DD vadītājs izveido „Turētāju maiņas/ anulēšanas protokolu", kura apstrādes process ir tāds pats kā „Turētāju nozīmēšanas protokola" apstrādes process.

D. IR sākotnējā klasificēšana

74. IR sākotnējā klasificēšana notiek, izmantojot *Mysignet* (sk. pielikumu Nr. 2 „Klasifikācijas līmeņa piešķiršanas informācijas resursam instrukcija").

75. IR sākotnējās klasificēšanas ir grafiski atspoguļots attēlā Nr. 3 „Informācijas resursa

sākotnējās klasificēšanas process".



Att. Nr. 3 „Informācijas resursa sākotnējās klasificēšanas process"

76. DD vadītājs katram IR izveido „Klasifikācijas līmeņa piešķiršanas protokolu" un pārsūta to IR turētājam aizpildīšanai.

77. IR turētājs veic IR klasifikāciju, ievērojot prasības, kas ir aprakstītas zemāk.

78. IR turētājs piešķir/ maina klasifikācijas līmeni atbilstoši Procedūrā aprakstītiem 3 (trim) līmeņiem:

78.1. Konfidencialitātes;

78.2. Vērtības;

78.3. Pieejamības.

D1. IR klasifikācija konfidencialitātes līmenī

79. Konfidencialitāte ir Informācijas drošības sastāvdaļa, kas raksturo, cik lielā mērā IS ir pieejama pilnvarotām personām.

80. Konfidencialitātes līmeni IR piešķir atkarībā no kaitējuma, kas varētu tikt nodarīts Informācijas devējam vai Bankai, ja tiek pieļauts, ka šai IS piekļūst personas, kas nav pilnvarotas.

81. IR turētājs un Lietotājs ir atbildīgi par to valdījumā un rīcībā esošo IR konfidencialitātes saglabāšanu atbilstoši sekojošiem konfidencialitātes līmeņiem:

81.1. Publiskā informācija;

81.2. Iekšējā jeb dienesta lietošanas informācija;

81.3. Ierobežotas pieejas informācija.

D2. IR klasifikācija vērtības līmenī

82. Vērtības līmeni IR Banka piešķir atkarībā no kaitējuma, kas varētu tikt nodarīts Informācijas īpašniekam, ja netiktu nodrošinātā IR integritāte.

83. IR turētājs un Lietotājs ir atbildīgi par to valdījumā un rīcībā esošo IR integritātes

saglabāšanu atbilstoši sekojošiem vērtības līmeņiem:

83.1. Augstas vērtības informācija;

83.2. Vidējas vērtības informācija;

83.3. Zemas vērtības informācija.

D3. IR klasifikācija pieejamības līmenī

84. IR pieejamības līmeni piešķir atkarībā no biznesa vajadzībām, ņemot vērā kaitējumu, kas varētu tikt nodarīts Informācijas devējam vai Bankai, ja netiktu nodrošināta IR pieejamība.

85. Informācijas pieejamības līmeni nosaka pēc šādas skalas:

85.1. nepārtraukta pieejamība (24 stundas diennaktī, 7 dienas nedēļā);

85.2. fiksēts pieejamības laiks (Informācija pieejama Bankas darba laikā).

86. IR pieejamības līmeņa klasifikācijai nosaka arī:

86.1. pieļaujamo laiku, kādu IR var nebūt pieejams (*Recovery Time Objective*);

86.2. pieļaujamo laika periodu, par kuru datus var zaudēt (*Recovery Point Objective*).

D4. Prasības auditācijas pierakstiem

87. IR turētājs definē prasības IR auditācijas pierakstu glabāšanas ilgumam un pārsūta protokolu TR turētājam.

88. TR turētājs izvērtē IR turētāja definētas prasības IR klasifikācijas līmenim, sniedz piekrišanu vai komentārus par katru no IR turētāja definētajiem IR klasifikācijas parametriem un pārsūta protokolu IR turētājam.

89. IR turētājs izvērtē TR turētāja sniegtos komentārus, ja nepieciešams, labo IR klasifikācijas parametrus un apstiprina „Klasifikācijas līmeņa piešķiršanas protokolu".

E. Dokumentēšana sarakstā un apstiprināšana

90. DD apkopo datus no dažādiem „Turētāju nozīmēšanas/ maiņas/ anulēšanas protokoliem" un „Klasifikācijas līmeņa piešķiršanas informācijas resursam protokoliem" vienotajā IR klasifikācijas sarakstā un iesniedz izvērtēšanai un apstiprināšanai Bankas valdei.

F. IR klasifikācijas pārskatīšana

91. IR turētājs, piesaistot DD un TR turētāju, ne retāk kā reizi gadā Bankas iekšējā normatīvā dokumentā „Informācijas sistēmu risku analīzes un pārvaldības procedūra" noteiktajā kārtībā veic IR risku analīzi, kuras ietvaros pārskata esošo IR klasifikāciju.

92. DD vadītājs IR risku analīzes ietvaros izveido katram IR risku analīzes protokolu, kura viena no sadaļām ir IR klasifikācijas pārskatīšana, un pārsūta to IR turētājam.

93. DD apkopo datus no dažādiem IR risku analīzes protokoliem vienotajā IR klasifikācijas sarakstā un iesniedz izvērtēšanai un apstiprināšanai Bankas valdei.

V IR turētāju, TR turētāju, DD un Atbildīgās struktūrvienības tiesības un pienākumi

A. IR turētāja pienākumi

94. Klasificēt viņa turējumā esošos IR.
95. Piedalīties viņa turējumā esošo IR un saistīto IS risku analīzē.
96. Apstiprināt pieejas tiesības IS.
97. Apstiprināt IS izmaiņu veikšanu un ieviešanu.
98. Noteikt prasības IS auditācijas pierakstu veidošanai.
99. Sadarboties ar IS TR turētāju IS funkcionalitātes un drošības jautājumos.
100. Ilgstošas prombūtnes laikā (ilgstošs komandējums, atvaļinājums, slimība u.c.), ja tas ir nepieciešams, deleģēt savus pienākumus resursu aizbildnim, ja tāds nav ticis iecelts agrāk.
101. Izstrādāt vai piedalīties IR izmantošanas noteikumu izstrādē.
102. Izstrādāt vai piedalīties IR integritātes nodrošināšanas noteikumu izstrādē un (vai) pasākumu realizācijā (sadarbojoties ar citām Bankas struktūrvienībām un DD).
103. Noteikt IS atkopšanas un atjaunināšanas laika prasības, ja IS resursi tiek bojāti un to funkcionēšana ir traucēta vai nav iespējama.

B. TR turētāja pienākumi

104. Nodrošināt TR fizisko un loģisko aizsardzību.
105. Sadarboties ar IR turētāju, lai īstenotu viņa prasības par IR aizsardzību un piekļuvi tiem.
106. Piedalīties IS risku analīzē, noteikt ar TR saistītos IS apdraudējumus un novērtēt šo apdraudējumu īstenošanās varbūtību.
107. Nodrošināt IS atjaunošanas procedūras, ja TR ir bojāti un IS funkcionēšana traucēta vai neiespējama.
108. Tieši piedalīties jaunu IS izstrādē, esošo IS modernizēšanā, paplašināšanā un likvidācijā saskaņā ar Bankas iekšējo normatīvo dokumentu prasībām.
109. Dot norādījumus Bankas darbiniekiem un prasīt to izpildi IS drošības nodrošināšanas jautājumos.
110. Sadarboties ar IR turētāju IS funkcionalitātes un drošības jautājumos.
111. Ilgstošas prombūtnes laikā (ilgstošs komandējums, atvaļinājums, slimība u.c.), ja tas ir nepieciešams, deleģēt savus pienākumus resursu aizbildnim, ja tāds nav ticis iecelts agrāk.

C. DD pienākumi IS drošības jomā

112. Kontrolēt resursu turētāju nozīmēšanas/ nomaiņas procesu, t.sk. uzturēt IR klasifikācijas sarakstu.
113. Analizēt IS auditācijas pierakstus.
114. Nodrošināt IS drošības prasību izpildes kontroli.
115. Izstrādāt vai piedalīties IS drošības nodrošināšanas noteikumu izstrādē.

116. Piedalīties IS resursu risku analīzē saskaņā ar Bankā noteikto risku analīzes metodoloģiju.
117. Informēt Bankas vadību par IS drošības līmeni.
118. Sadarboties ar resursu turētājiem IS funkcionalitātes un drošības jautājumos.
119. Koordinēt ar Informācijas un IR klasifikāciju saistīto jautājumu pārvaldīšanu Grupas mērogā, t. sk. sadarbojoties ar Atbildīgajām struktūrvienībām un nosakot informācijas apmaiņas kārtību šajā jomā.

D. DD pienākumi IS drošības jomā

120. Atbildīgā struktūrvienība ir atbildīga par Informācijas un IR klasifikācijas sistēmas izveidošanu un uzturēšanu konkrētajā sabiedrībā, ievērojot Procedūras pamatprincipus un DD ieteikumus.

E. IR turētāju un TR turētāju tiesības

121. Konsultēt Bankas darbiniekus, dot viņiem norādījumus un prasīt to izpildi IS drošības nodrošināšanas jautājumos savas kompetences ietvaros.
122. Deleģēt resursa turētāja pienākumus (vai atsevišķus pienākumus) resursu aizbildnim, ja tas ir nepieciešams.
123. Iesniegt Bankas vadībai priekšlikumus par Bankas IS attīstības pasākumiem, t. sk. saistītus ar IS drošību.

F. DD tiesības IS drošības jomā

124. Konsultēt Bankas darbiniekus, dot viņiem norādījumus un prasīt to izpildi IS drošības nodrošināšanas jautājumos savas kompetences ietvaros.
125. Iesniegt Bankas vadībai priekšlikumus, saistītus ar IS drošības attīstības pasākumiem.
126. Izstrādāt vai piedalīties IS drošības nodrošināšanas noteikumu izstrādē.

VI Pielikumu saraksts

Nr.	Nosaukums
1.	Turētāju nozīmēšanas/ maiņas/ anulēšanas instrukcija
2.	Klasifikācijas līmeņa piešķiršanas Informācijas resursam instrukcija

* * * * *