Apstiprināta
ar 27.03.2018. valdes
lēmumu Nr.1-9/A1-7

grozījumi
ar 29.03.2023. valdes
lēmumu Nr**. 5**-10/A1-7

VSIA "Latvijas Radio" informācijas tehnoloģiju drošības politika

I Vispārīgie noteikumi

Uzņēmuma informācijas tehnoloģiju (tehnoloģiju, kuras tām paredzēto uzdevumu izpildei veic informācijas elektronisko apstrādi, tajā skaitā, izveidošanu, dzēšanu, glabāšanu, atskaņošanu, attēlošanu vai pārsūtīšanu; turpmāk tekstā - IT) drošības politika nosaka mērķus un darbību pamatprincipus elektroniskās informācijas drošības nodrošināšanas jomā un kalpo par pamatu visām konkrētajām ar IT jomas drošību saistītajām aktivitātēm VSIA „Latvijas Radio" (turpmāk tekstā - Latvijas Radio), attiecībā uz informācijas sistēmām, kādas tiek uzturētas uzņēmuma darbības nodrošināšanas vajadzībām.

IT drošības politika attiecas uz visām Latvijas Radio izmantotajām vai lietotajām informācijas sistēmām (informācijas tehnoloģiju un datu bāzu kopumu, kuru lietojot tiek nodrošināta Latvijas Radio funkciju izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, uzglabāšana, izmantošana un iznīcināšana; turpmāk tekstā - IS).

IT drošības politikā iekļautās prasības ir obligātas un saistošas visiem Latvijas Radio darbiniekiem; atsevišķas IT drošības politikas prasības ir saistošas IS ārējiem lietotājiem, saskaņā ar noslēgtajiem līgumiem.

IT drošības politikas mērķi ir:

- nodrošināt Latvijas Radio lietoto informācijas resursu un IS drošību, vienlaikus apzinoties, ka informācijas drošība nav sinonīms lietoto tehnisko resursu drošībai;
- panākt vienveidīgu un sistemātisku pieeju IT drošības jautājumu risināšanā;
- būt par pamatu attiecīgu noteikumu, instrukciju un citu dokumentu izstrādei un ieviešanai Latvijas Radio IT drošības jomā, ja vien to prasības nenonāk pretrunā ar ārējiem, šo jomu regulējošiem, normatīvajiem aktiem.

IT drošības politikas pamatprincipi ir:

a) vispārējās līdzdalības princips - par IT drošību, savu darba pienākumu izpildes ietvaros, atbildīgs ir ikviens Latvijas Radio darbinieks;
b) samērīguma princips - drošības kontrolēm ir jābūt samērojamām, no to piemērošanai nepieciešamo resursu un laika viedokļa, ar saistītajiem riskiem un to iespējamām sekām;

c) princips "pieejamība pēc nepieciešamības" - IS lietotājiem ir tieši tādas pieejas tiesības informācijas resursiem, kādas izriet no nepieciešamības viņu darba pienākumu izpildei;
d) atbildības princips - par IT drošības politikas ievērošanu, atjaunināšanas ierosināšanu un papildināšanu atbildīga ir Latvijas Radio Informācijas tehnoloģiju daļa (turpmāk tekstā - ITD), kuras darbinieku pienākums ir sekot likumu un citu ārējo tiesību aktu prasībām IT drošības jomā, kopējām IT jomas attīstības tendencēm un plānot lietoto IS attīstību.

II IT lietošanas drošības ietvars

Apdraudējumi (iemesli, kuri samazina lietoto IS drošību):

a) personas vai personu grupas tīšas vai netīšas darbības, atbildīgo personu kļūdaina rīcība vai bezdarbība vai arī jebkurš cits notikums, kura rezultātā IS darbība var tikt iespaidota ārpus tām noteiktajiem drošības aspektiem vai ierobežojumiem.

Apdraudējumu novēršana:

a) Latvijas ITD pienākums ir regulāri īstenot vai organizēt IT jomas risku analīzi, pamatojoties uz kuru, tiek plānoti un realizēti nepieciešamie pasākumi risku samazināšanai;

b) Latvijas Radio ir līgumiski apstiprinātas sadarbības attiecības ar Latvijas Universitātes Matemātikas un informātikas institūtu (turpmāk tekstā - CERT.LV) par IT drošības apdraudējumu agrās brīdināšanas sistēmas izveidi un ekspluatāciju;

c) faktiskās situācijas objektīvai novērtēšanai var tikt izmantota ārējo auditoru kompetenču piesaiste.

IT drošības pamatnostādnes:

a) Latvijas Radio IT drošības politika tiek realizēta atbilstoši Informācijas tehnoloģiju drošības likuma, Latvijas Republikas 01.02.2011. Ministru kabineta noteikumu Nr.100 *Informācijas tehnoloģiju kritiskās infrastruktūras drošības pasākumu plānošanas un īstenošanas kārtība*, 28.07.2015. Ministru kabineta noteikumu Nr.442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām* un citu spēkā esošo tiesību aktu normām;

b) IT jomas drošības prasību ievērošana ir Latvijas Radio darbinieku ikdienas pienākums, ko nosaka spēkā esošais iekšējais regulējums;

c) IT jomas drošības nodrošināšanai nepieciešamo atbalstu, palīdzību un konsultācijas koordinē un realizē ITD.

III IT jomas resursu ekspluatācija

Programmproduktu lietošana:

a) Latvijas Radio IS lietotājiem tiek uzstādīta tikai legālas izcelsmes un darba pienākumu veikšanai nepieciešamā programmatūra;

b) ITD ir atbildīga par lietotās programmatūras kļūdu un/vai drošības kļūdu novēršanas atjauninājumu, komandu kodu un vides iestādījumu, kādus ir

publicējuši uzticami lietotās programmatūras izstrādātāji, operatīvu ieviešanu;

c) IS galvenā administratora funkcija ir deleģēta ITD, t.i., IS lietotājiem ir liegtas tiesības patstāvīgi veikt jebkādas izcelsmes programmproduktu vai to atjauninājumu instalāciju lietošanai nodotajos tehniskajos resursos;

d) uzņēmuma darbības nodrošināšanai nepieciešamā programmatūra, tās versiju atjauninājumi un izstrādātāju atbalsts tiek iegādāti atbilstoši Latvijas Radio budžetam.

Tehnisko resursu drošība:

a) koplietošanas datu apstrādes un pārraides iekārtas, serveri, tīkla komunikācijas pamatelementi, u.tml. uzņēmuma kritiskās infrastruktūras komponentes, fiziski ir novietotas ierobežotas piekļuves zonās;

b) tiešraižu un ierakstu studiju datu apstrādes un pārraides iekārtas, kuru fizisko novietojumu tehnoloģiskie procesi limitē tiešā studiju tuvumā, tiek izvietotas kontrolētas piekļuves konstrukcijās;

c) uzņēmuma tehnisko resursu apkalpošanu veic atbilstoši kvalificēts ITD personāls vai labas reputācijas ārpakalpojumu sniedzēji tiešā ITD darbinieku uzraudzībā;

d) stacionāra pielietojuma tehnisko resursu pārvietošanu, Latvijas Radio darba telpās, ir tiesīgi veikt tikai ITD darbinieki.

Informācijas resursu pieejas loģiskā aizsardzība:

a) individuālās lietošanas datortehnikas pieejas kontrole tiek realizēta izmantojot operāciju sistēmu un tīkla pārvaldības programmproduktu iebūvētos līdzekļus;

b) IS lietotāju piekļuves tiesības konkrētiem informācijas resursiem tiek noteiktas tādā apjomā, kāds nepieciešams konkrētā lietotāja tiešo darba pienākumu izpildei; tiesību apjomu ierosina darbinieka tiešais vadītājs, apstiprinājumu realizācijai uzņēmuma vadība deleģē ITD;

c) individuālās pieejas paroles tiek veidotas ar garumu, ne īsāku par astoņiem simboliem, iekļaujot lielos un mazos burtus, skaitļu simbolus un speciālos simbolus (!@#$%&*)(?/);

d) paroles ir jāmaina lietotājiem, ne retāk kā reizi 180 dienās un jaunās paroles nedrīkst būt līdzīgas iepriekšējām trim pēdējām parolēm.

e) jebkuras darbības uzņēmuma IS, izmantojot cita lietotāja vārdu un paroli, ir aizliegtas - katrs lietotājs ir pilnā mērā atbildīgs par darbībām, kādas IS tiek veiktas, izmantojot viņa individuālos identifikatorus.

Pieeja publiskajam interneta tīklam:

a) Latvijas Radio izmanto vismaz divus, fiziski savstarpēji nesaistītus, platjoslas interneta pieslēgumus (tiešraidēm un ierakstiem izmantotās sakaru līnijas tiek dublētas ar funkcionāli līdzvērtīgu, uz bezvadu datu pārraidi balstītu, risinājumu);

b) IS lietotājiem ir aizliegts veikt uz publiskā interneta tīkla darbības traucēšanu vērstas darbības, izmantojot to tikai tiešo darba pienākumu izpildei.

Datu pārraides tīklu aizsardzība:

a) piekļuve informācijai par datu pārraides tīkla topoloģiju un tā aparatūras konfigurāciju ir ierobežota (ITD, uzņēmuma vadība, IT drošības speciālists);

b) pieslēgumi ārējiem tīkliem ir aizsargāti izmantojot „ugunsmūra" funkcijas iekārtas, kuru konfigurācijas parametri tiek regulāri pārbaudīti;

c) sadarbībā ar CERT.LV, tiek uzturēta Latvijas Radio IT drošības apdraudējumu agrās brīdināšanas sistēma, kura nodrošina datu pārraides tīkla plūsmas anomāliju analīzi, ļaunprogrammatūras parakstu atpazīšanu un regulāru atjaunošanu.

Datu rezerves kopiju veidošana:

a) visiem uzņēmuma datiem regulāri tiek veidotas rezerves kopijas; pirmajai rezerves kopijai ir identiskas pieejas tiesības kā oriģinālam;

b) pieejas tiesības centralizētajai datu rezerves kopijai ir tikai ITD;

c) visu datu, izņemot skaņas ierakstu arhīva, kopijas tiek veidotas ne retāk kā reizi diennaktī un uzglabātas neierobežotu laika periodu;

d) skaņas ierakstu arhīva kopijas tiek veidotas uz fiziskiem datu nesējiem un uzglabātas neierobežotu laika periodu.

IS lietotāju kvalifikācija:

a) atbildīgs, par uzņēmuma darbinieka pamatzināšanu IT jomas resursu lietošanā atbilstību lietoto IS prasībām un iekšējo normatīvo aktu izpildei, ir darbinieka tiešais vadītājs;

b) pirms IS lietotāja tiesību piešķiršanas darbiniekam, ITD pienākums ir iepazīstināt ar spēkā esošo iekšējo normatīvo aktu prasībām, IT jomas resursu lietošanas kārtību uzņēmumā un informēt par iespējamiem drošības riskiem un atbilstošajām sekām, to pārkāpšanas gadījumā.