Biedrība "VECMĀMIŅAS.lv"
Informācijas tehnoloģiju drošības politika

I Vispārējie noteikumi

Biedrības 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 *biedrībā* attiecībā uz informācijas sistēmām, kādas tiek uzturētas *biedrības* darbības nodrošināšanas vajadzībām.

IT drošības politika attiecas uz visām *biedrībā* izmantotajām vai lietotajām informācijas sistēmām (informācijas tehnoloģiju un datu bāzu kopumu, kuru lietojot, tiek nodrošināta *biedrības* 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 *biedrības* darbiniekiem; atsevišķas IT drošības politikas prasības ir saistošas IS ārējiem lietotājiem, saskaņā ar noslēgtajiem līgumiem.
IT drošības politikas mērķi ir:
• nodrošināt *biedrībā* lietoto informācijas resursu un IS drošību, respektējot apstākli, ka informācijas drošība nav sinonīms lietoto tehnisko resursu drošībai;
• panākt vienveidīgu un sistemātisku pieeju IT drošības jautājumu risināšanā, t.sk. atbilstošu noteikumu izstrādē.

IT drošības politikas pamatprincipi ir:
a) vispārējās līdzdalības princips - par IT drošību savu darba pienākumu izpildes ietvaros atbildīgs ir ikviens *biedrības* 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 *biedrības valde*, kuras locekļu 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

<u>Apdraudējumi (iemesli, kuri samazina lietoto IS drošību)</u>
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 tās noteiktajiem drošības aspektiem vai ierobežojumiem.

Apdraudējumu novēršana:

a) *biedrības valdes* pienākums ir regulāri īstenot vai organizēt IT jomas risku analīzi, pamatojoties uz kuru, tiek plānoti un realizēti nepieciešamie pasākumi risku samazināšanai;
b) *biedrība* nodrošina līgumiski apstiprinātas sadarbības attiecības ar sertificētu privāto kompāniju par IT drošības apdraudējumu agrās brīdināšanas sistēmas izveidi un ekspluatāciju, kā arī faktiskās situācijas objektīvu novērtēšanu.

IT drošības pamatnostādnes:

a) *biedrībā* IT drošības politika tiek realizēta atbilstoši Latvijā spēkā esošo tiesību aktu normām;
b) IT jomas drošības prasību ievērošana ir *biedrības* darbinieku ikdienas pienākums, ko nosaka spēkā esošais iekšējais regulējums;
c) IT jomas drošības nodrošināšanai nepieciešamo atbalstu, palīdzību un konsultācijas koordinē un realizē *biedrības valde*.

III IT jomas resursu ekspluatācija

a) *biedrība* nodrošina IS lietotājiem tikai legālas izcelsmes un darba pienākumu veikšanai nepieciešamo programmatūra;
b) *biedrības valde* 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 *biedrības valdei*, t.i., IS lietotājiem ir liegtas tiesības patstāvīgi veikt jebkādas izcelsmes programmproduktu vai to atjauninājumu instalāciju lietošanai nodotajos tehniskajos resursos;
d) *biedrības* darbības nodrošināšanai nepieciešamā programmatūra, tās versiju atjauninājumi un izstrādātāju atbalsts tiek iegādāti atbilstoši *biedrības* budžetam.

Tehnisko resursu drošība:

a) koplietošanas datu apstrādes un pārraides iekārtas u.tml. *biedrības* kritiskās infrastruktūras komponentes fiziski ir novietotas ierobežotas piekļuves telpās;
b) tiešraižu un ierakstu datu apstrādes un pārraides iekārtu izmantošana, kuru fizisko novietojumu tehnoloģiskie procesi limitē tiešā *biedrības* telpu tuvumā, tiek speciāli administrēta;
c) *biedrības* tehnisko resursu apkalpošanu veic atbilstoši kvalificēts IT personāls (ārpakalpojuma līgums).

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 apstiprina *biedrības valde*;
c) individuālās pieejas paroles tiek veidotas ar atbilstošu garumu un atbilstošiem simboliem;
d) paroles ir jāmaina lietotājiem paredzētā laika periodā, un ieteicams, ka jaunās paroles nav līdzīgas iepriekšējām parolēm;
e) jebkuras darbības biedrības 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

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

Datu pārraides tīklu aizsardzība

Piekļuve informācijai par datu pārraides tīkla topoloģiju un tā aparatūras konfigurāciju ir ierobežota, pieslēgumi ārējiem tīkliem tiek aizsargāti, datu pārraides tīkla plūsmas anomālijas tiek novērstas (*biedrības valde*, piesaistītais IT personāls).

Datu rezerves kopiju veidošana

Biedrības datiem var tikt veidotas rezerves kopijas, kas tiek uzglabātas speciālā USB diskā ne mazāk kā 3 gadus; pieeja tām ir nodrošināta *biedrības valdei*.

IS lietotāju kvalifikācija:
a) atbildīga par *biedrības* darbinieku pamatzināšanu IT jomas resursu lietošanā atbilstību lietoto IS prasībām un iekšējo normatīvo aktu izpildei ir *biedrības valde*;
b) pirms IS lietotāja tiesību piešķiršanas darbiniekam *biedrības valdes* pienākums ir iepazīstināt ar spēkā esošo iekšējo normatīvo aktu prasībām, IT jomas resursu lietošanas kārtību *biedrībā* un informēt par iespējamiem drošības riskiem un atbilstošām sekām to pārkāpšanas gadījumā.

Informācijas tehnoloģiju drošības nostādnes apstiprinātas biedrības „Vecmāmiņas.lv ” valdes sēdē 2024. gada 1. februārī.

INĀRA PUČUKA,
biedrības “VECMĀMIŅAS.lv ” valdes priekšsēdētāja

Rīgā, 2024. gada 1. februārī