STOPIŅU NOVADA DOME

ULBROKAS VIDUSSKOLA
Reģistrācijas Nr.2013901107
Vālodzes, Stopiņu novadā, LV- 2130, tālrunis: 67910372, 25144588,
fakss: 67910151, e-pasts: ulbrokas.skola@u-vsk.lv; www.ulbrokas-vsk.lv

APSTIPRINU
Ulbrokas vidusskolas direktors

N. Balabka

31.08.2018. Nr.88

Ulbrokas skolas iekšējie informācijas sistēmu drošības noteikumi

I Vispārīgie jautājumi

1. Iekšējie noteikumi nosaka Stopiņu Novada Domes Ulbrokas vidusskolas, turpmāk tekstā – "Skola" informācijas sistēmu drošības un datu apstrādes aizsardzības kartību. Informācijas sistēmas šo noteikumu izpratnē ir elektroniskas iekārtas, kas izveidotas, strādā un tiek uzturētas, lai radītu, apkopotu, uzkrātu, apstrādātu, uzglabātu un izmantotu informāciju. Informācijas sistēmas kopumu veido informācijas resursi un tehniskie resursi.
   Šo noteikumu izpratnē Skolas Informācijas sistēmas un tehnisko resursu turētājs ir Skola *(tiek norādīts IT pakalpojuma sniedzējs ārpakalpojuma gadījumā)* (turpmāk — TR turētājs).

II Informācijas sistēmu fiziska aizsardzība

2. Skola risku pārvaldīšanas ietvaros veic IS fiziskas aizsardzības pasākumus, kas aizsarga tās no nevēlamiem apkārtējas vides (ugunsgrēks, plūdi, temperatūras svārstības u. c.), tehniskajiem (neatbilstoša elektroenerģijas padeve u. c.) un cilvēkfaktoriem (tīši vai netīši bojājumi, zādzība u. c.)
3. Skola IS izvietotas uz TR turētāja serveriem/datorā. TR turētājs nodrošina serveru/datora fizisko aizsardzību:
   3.1. visas IS tiek ekspluatētas ierobežotas pieejamības, slēdzamās telpās, kuru fiziskā aizsardzība nodrošina tikai pilnvarotu personu piekļuvi, vai arī nodrošina serveru/datoru fizisko aizsardzību, lai tos nevarētu izslēgt, pārvietot, bojāt un nesankcionēti mainīt to konfigurāciju;
   3.2. nepiederošas personas, t. sk. ārējie pakalpojumi sniedzēji telpās, kurās atrodas datos / serveri drīkst uzturēties tikai pilnvarotu personu pavadībā;
   3.3. TR turētājs nodrošina pietiekamu serveru un serveru telpu aizsardzību pret

fiziskiem apdraudējumiem (t. sk. neatbilstošiem klimatiskajiem apstākļiem, ugunsgrēku, plūdiem elektroenerģijas padeves pārtraukumiem, tīšiem bojājumiem), nepieciešamības gadījumā ierīkojot ugunsdzēsības signalizāciju, uzstādot alternatīvās strāvas padeves iekārtas un gaisa dzesēšanas iekārtas.

4. Skola nodrošina pārziņā esošo tīklu infrastruktūrai (t. sk. komunikāciju tīklu aparatūrai, kabeļu tīklam) pietiekamu fizisko aizsardzību, to izvietojot tādējādi, lai tai nevarētu nesankcionēti un nemanīti piekļūt, pieslēgties vai bojāt ar Skolu nesaistītas personas, kā arī, lai tai nevarētu nesankcionēti piekļūt, pieslēgties un bojāt, vai nejauši aiz neuzmanības bojāt Skolas darbinieki vai apmeklētāji.
5. Skola nodrošina, ka darbstacijas lieto atbilstoši ražotāja noteiktām prasībām un lieto elektroenerģijas nepārtrauktas padeves iekārtas, ja atklājas, ka elektroenerģijas padeves traucējumu risks ir nepieņemami liels.
6. Portatīvo iekārtu fiziskā aizsardzība:
   6.1. portatīvos datorus lieto atbilstoši ražotāja noteiktajām prasībām;
   6.2. Skola veic portatīvo iekārtu aprites reģistrēšanu, lai noteiktu, kura persona lieto attiecīgo iekārtu.
7. Datu nesēju fiziskā aizsardzība:
   7.1. Skola veic nepieciešamos drošības pasākumus datu nesēju fiziskai aizsardzībai neatkarīgi no veida (t. sk. demontētas disku iekārtas, papīra izdrukas, faksa izdrukas, USB zibatmiņas, optiskie diski u. tml.);
   7.2. Skolas IS resursi, kurus nav nepieciešams lietot vai pārvietot, tiek glabāti Skolas telpās tam paredzētās vietās. Ja ir nepieciešams iznīcināt datu nesējus, to iznīcināšanu uzrauga vai nodrošina TR turētājs;
   7.3. Skola nodrošina datu ievades un izvades iekārtu fizisko aizsardzību, novēršot nesankcionētu lietošanu;
   7.4. datu nesējus ar klasificētiem informācijas resursiem aizliegts atstāt nedrošās (piemēram, publiski pieejamās) vietās;
   7.5. ja datu nesēju, kas satur klasificētus informācijas resursus, ir paredzēts iznīcināt, tad to izdara tādā veidā, lai nebūtu iespējams veikt uz tā esošo datu atjaunošanu.
8. Nepieciešamības gadījumā Skola veic papildu fiziskās aizsardzības pasākumus atkarība no IS resursu klasifikācijas līmeņa. IS fiziskās aizsardzības pasākumus veic sistemātiski, nepieļaujot situāciju, ka Informācijas sistēmas resursi atrastos ārpus ierobežotas pieejamības telpām bez Skolas pilnvarotu darbinieku uzraudzības. Skola regulāri veic fiziskās aizsardzības pasākumu pārbaudi.

III Piekļuves kontrole

9. Katram informācijas resursu (IR) lietotājam tiek piešķirts ID lietotājvārds(i) (identifikators(i)) un parole, kā arī noteiktas piekļuves tiesības. IS lietotājs ir atbildīgs par piešķirtā lietotājvārda (identifikatora) un paroles lietošanu, saglabāšanu un neizpaušanu.
10. Piekļuves tiesības apstiprina attiecīgo IR turētājs. Balstoties uz IR turētāja pieprasījumu, TR turētājs izveido lietotājam piekļuvi visās apstiprinājumā norādītajās informācijas sistēmās.
11. IR turētājam ir jāinformē TR turētājs par tiem darbiniekiem, kuri pārtrauc darba attiecības Skolā. TR pēc šīs informācijas saņemšanas nekavējoties anulē visas attiecīgā darbinieka piekļuves tiesības Skolas informācijas sistēmas resursiem.
12. IS lietotājs ir atbildīgs par darbībām, kas tiek veiktas, izmantojot viņa lietotājvārdu (identifikatoru). IS lietotāja autentiskumu nosaka, lai pārliecinātos, ka lietotājvārda (identifikatora) izmantotājs ir sankcionētais tā turētājs. Autentiskuma noteikšanai tiek izmantotas paroles. Pēc lietotājvārda (identifikatora) un paroles ievadīšanas IS lietotājs var izmantot informācijas sistēmas resursu atbilstoši noteiktajām piekļuves tiesībām.

Parole sastāv no burtu un ciparu kombinācijas, kur jābūt vismaz vienam ciparam un vienam lielajam burtam, un tās garums nedrīkst būt īsāks par deviņiem simboliem. Parole nedrīkst saturēt garumzīmes un mīkstinājuma zīmes. Nedrīkst par paroli izmantot personu identificējošos datus (piemēram, personas datus, lietotājvārdu (identifikatoru) vai tā daļu, automašīnas numuru, radu vārdus vai uzvārdus, vārdus, kas saistīti ar darbavietu vai kas bieži tiek tajā lietoti).

13. IS lietotājam paroli jāmaina vismaz reizi trijos mēnešos. TR turētājam ir jānodrošina:
    13.1. automātisku paroles maiņas pieprasījumu, lietotājam pirmo reizi reģistrējoties tīklā;
    13.2. automātisku paroles maiņas pieprasījumu ik pēc trim mēnešiem;
    13.3. sistēmas bloķēšanu uz laiku līdz _____ *(laika periods)*, ja lietotājs piecas reizes pēc kārtas ir ievadījis nepareizu paroli vai lietotājvārdu.
14. IS lietotājam parole ir jāiegaumē. Rakstiskā veidā paroles atļauts glabāt tikai aizslēgtā seifā.
15. Ja radušās aizdomas, ka paroli uzzinājusi cita persona, IS lietotājs to nekavējoties nomaina un par incidentu ziņo atbildīgajam pat IS drošību.
16. Aizliegts mēģināt uzzināt citu lietotāju paroles, izņemot gadījumus, kad tas ir nepieciešams IS administratoram viņa tiešo pienākumu veikšanai. Pēc minēto darbu pabeigšanas IS lietotājs paroli nomaina.
17. Uz datora ir jābūt uzstādītam ekrāna saudzētājam ar aktivizācijas paroli. Tam ir automātiski jāaktivizējas, ja 15 minūšu laikā lietotājs nav veicis nekādas darbības.
18. TR turētājam pēc IR pieprasījuma ir tiesības veikt lietotāju darbības auditus. Šādi auditi var ietvert lietotāja darbību auditācijas veikšanu (tai skaitā apmeklētos interneta resursus), analizēšanu un papildus informācijas pieprasīšanu par veiktajām darbībām.
19. Datu apstrāde Skolas informācijas sistēmās notiek Skolas telpās: c. Vālodzes, Stopiņu novads.
20. Sistēmu darbības nodrošināšanas un kontroles nolūkos TR turētājs drīkst nodrošināt attālinātu piekļuvi Skolas informācijas sistēmām. Šādu darbību veikšanai nepieciešama Skolas vadītāja atļauja.

IV Rezerves datu kopēšana

21. TR turētājs veic svarīgāko informācijas resursu un programmatūru rezerves datu kopēšanu. Rezerves datu kopēšanu nodrošina TR turētājs, un to biežums un apjoms tiek saskaņots ar IR turētāju.
22. Rezerves datu kopijas tiek uzglabātas tā, lai to drošību neietekmē vieni un tie paši draudi. Rezerves datu kopijām ir jābūt pieejamām jebkurā laikā.
23. Rezerves kopēšana tiek organizēta tā, lai būtu iespējams atjaunot datus. Organizējot rezerves datu kopēšanu, tiek ņemtas vērā normatīvajos aktos noteiktās prasības.
24. Rezerves kopiju integritāte tiek pārbaudīta vismaz vienu reizi gadā.
25. Ne retāk kā reizi gadā, TR turētājs sadarbībā ar IR turētāju, veic pārbaudes, lai pārliecinātos, ka rezerves datu kopijas tiek sagatavotas kvalitatīvi un no tām ir iespējams atjaunot IS darbību.

V Informācijas sistēmas resursu loģiskā aizsardzība

26. Skola risku pārvaldīšanas ietvaros veic informācijas sistēmu loģiskās aizsardzības pasākumus. Skola dokumentē un veic informācijas sistēmu lietotāju reģistrācijas, tiesības piešķiršanas un anulēšanas procedūras:
    26.1. katram lietotājam, IR turētājam piešķir unikālu lietotāja kodu. Jauna lietotāja reģistrāciju veic saskaņā ar IT drošības politiku un iekšējiem sistēmas drošības noteikumiem. Informācijas sistēmu lietotāju, IR turētāju darba pienākumu maiņas

vai darba attiecību izbeigšanas gadījumā tiek nekavējoties mainīti vai anulēti piešķirtie lietotāja kodi un pieejas tiesības informācijas sistēmām;

26.2. informācijas pārvaldnieku informācijas sistēmu pieejas kodus kopā ar parolēm glabā drošā ierobežotas pieejas vietā, seifā.

27. Lietotāju autentiskuma noteikšanas ietvaros:

27.1. TR turētājs pārliecinās, ka attiecīgās informācijas sistēmas lieto pilnvarotais lietotāja koda turētājs, izmantojot dažādus, pietiekamus drošības autentifikācijas līdzekļus, kas var tikt pilnveidoti, mainīti un attīstīti;

27.2. Autentifikācijas līdzekļus lietošanas veidus un kārtību nosaka Skola, bet tehniski nodrošina TR turētājs;

27.3. Kā paroli izvēlas pietiekami sarežģītu simbolu kombināciju. Ievadot paroli, tā nedrīkst būt salasāma uz datora ekrāna. TR turētājs bloķē pieeju lietotājam visām IS, ja lietotāja pieejas parole varētu būt vai kļuvusi zināma citai personai.

28. Informācijas sistēmu lietošanas pārraudzības ietvaros:

28.1. TR turētājs nodrošina, ka Auditācijas pieraksti tiek veidoti par Informācijas sistēmām, kas satur klasificētus Informācijas resursus. Auditācijas pierakstos iekļauj visu veiksmīgas un neveiksmīgas pieslēgšanās gadījumu datumu un laiku. Kā arī lietotāja (TR turētāja) kodu vai citu autentifikācijas līdzekļi;

28.2. TR turētājs nodrošina Auditācijas pierakstu integritāti un regulāri veido Auditācijas datu rezerves kopijas saskaņā ar šīs kārtības III daļas noteikumiem;

28.3. TR turētājs regulāri pārrauga visu Informācijas sistēmu darbību, taču īpašu uzmanību pievērsto Informācijas sistēmu darbības pārraudzībai, kas satur klasificētus Informācijas resursus. Šim nolūkam TR turētājs pēc izvēles lieto speciālas pārraudzības programmas vai datoru iebrukumu noteikšanas sistēmas;

28.4. TR turētājs pārrauga vismaz šādus gadījumus:

28.4.1. atkārtota neveiksmīga pieslēgšanās Informācijas sistēmai;

28.4.2. mēģinājumi piekļūt Informācijas resursiem, kuriem lietotājs nav pilnvarots piekļūt;

28.4.3. Informācijas sistēmas lietošana neparastā laikā, piemēram, ārpus darba laika;

28.4.4. atkārtoti mēģinājumi lietot lietotāja kodus, kuri jau ir atcelti;

28.4.5. priviliģēto lietotāja kodu piešķiršana un lietošana (piemēram, tehnisko resursu pārvaldnieka kodi);

28.4.6. nesankcionētas programmatūras konfigurācijas maiņas un neatļautas programmatūras uzstādīšana.

29. Vīrusu kontrole Informācijas sistēmas resursos:

29.1. TR turētājs kārtību un veic pasākumus datoru vīrusu darbības novēršanai informācijas sistēmās;

29.2. vīrusu darbības novēršanai lieto speciāli šīm nolūkam paredzētu programmatūru. Vīrusu definīciju failus atjauno automātiski vismaz reizi dienā;

29.3. TR turētājs regulāri veic antivīrusu programmas pārraudzību, lai pārliecinātos par tās darbību, drošības incidentiem un jaunāko vīrusu definīciju failu esamību.

30. Personālo un portatīvo datoru aizsardzība:

30.1. portatīvajos datoros, kuri tiek lietoti ārpus Skolas darba telpām, glabā tikai to informāciju, kas nepieciešami noteiktajā laikā noteiktajam datora lietotājam;

30.2. personālajā datorā uzstāda un lieto tikai to programmatūru un tādā konfigurācijā, ko ir noteicis TR turētājs. Personālā datora funkcionalitāti ierobežo līdz darba vajadzībām nepieciešamo funkciju līmenim;

30.3. personālo datoru, atstājot bez lietotāja uzraudzības, slēdz, lietojot ekrānsaudzētāju ar paroli, speciālu slēgšanas funkciju vai citu metodi, kas ļauj turpināt darbu ar personālo datoru vienīgi tad, ja ir veikta lietotāja autentifikācija.

30.4. Informācijas resursu turētājs nosaka kārtību, kādā darba vajadzībām darbinieki

lieto viņiem piederošus IT ierīces (datorus) un kādā lieto Skolas datorus ārpus darba telpām. Šī kārtība nedrīkst samazināt noteikto informācijas resursu aizsardzības līmeni.

31. Datortīklu aizsardzība:
    31.1. TR turētājs izstrādā un uztur datortīkla shēmu, kurā parādīta datortīklā savienotā aparatūra un nodrošinātie pakalpojumi;
    31.2. datu plūsmā starp lokālo datortīklu un ārējo datortīklu atļauj tikai tos pakalpojumus, kas ir nepieciešami Skolas funkciju izpildei šim nolūkam lieto ugunsmūra sistēmas;
    31.3. TR turētājs regulāri pārbauda visu ārējo savienojumu eksistenci un pārliecinās, ka pastāv tikai tie savienojumi, kuri atbilst Skolas darbības vajadzībām un ka darbojas rezerves savienojumi;
    31.4. pieslēgšanos Skolas informācijas sistēmām no loģiski attālas vietas aizsargā, lietojot kriptogrāfijas līdzekļus kopā ar lietotāja paroli tā, lai droši noteiktu lietotāja autentiskumu. Pieslēgšanos attālinātiem servisiem nosaka attiecīgās IS lietošanas instrukcijā.
32. Skola pēc nepieciešamības veic papildu loģiskas aizsardzības pasākumus atkarībā no Informācijas sistēmas resursu klasifikācijas līmeņa.
33. Skola veic līdzvērtīgus loģiskās aizsardzības pasākumus klasificētiem Informācijas resursiem neatkarīgi no datu glabāšanas veida (t. sk. disketes, papīra dokumenti, audiokasetes u. tml.).
34. Skola sadarbībā ar ārējiem informācijas tehnoloģiju pakalpojumu sniedzējiem:
    34.1. nosaka prasības iesaistīto personu atbildībai, pagaidu lietotāju kontu piešķiršanai, pārmaiņu pārvaldīšanai un citas Informācijas sistēmas drošības prasības;
    34.2. saskaņojot ar IR turētajiem, piešķir pieejas tiesības Informācijas sistēmas resursiem ārējiem informācijas tehnoloģiju pakalpojumu sniedzējiem tikai to pienākumu veikšanai nepieciešamajā apjomā;
    34.3. nosaka informācijas izpaušanas ierobežojumus.
35. Skola izvēlas Informācijas sistēmas uzturēšanu uzticēt ārējam pakalpojumu sniedzējam, tam jānodrošina Informācijas sistēmas drošības līmenis, kas nav zemāks par šajā kārtība noteikto. Skola iepazīstina ārējo pakalpojumu sniedzēju ar šajā kārtība noteiktajām Informācijas sistēmas drošības prasībām.

VI Informācijas sistēmu izstrāde, iegāde un pārmaiņu pārvaldīšana

36. Veicot Informācijas sistēmas izstrādes, iegādes, ieviešanas un pārmaiņu pārvaldīšanas procesu, Skola ievēro un atbild par Informācijas sistēmas drošības prasību ievērošanu neatkarīgi no tā, vai šos procesus veic pats Skola vai ārējais izstrādātājs un piegādātājs. Tas pats jāievēro arī, veicot būtiskas izmaiņas datortīkla ārējo pieslēgumu konfigurācijā.
37. Informācijas sistēmas izstrādes uzsākšana:
    37.1. Skola nosaka par Informācijas sistēmas projektu atbildīgās personas, t. sk. arī saskaņā ar šiem noteikumiem nosaka izstrādājamās Informācijas sistēmas IR turētāju un TR turētāju;
    37.2. atbildīgās personas veic Informācijas sistēmas projekta un to Informācijas sistēmu, kuru darbību var ietekmēt jaunā Informācijas sistēma, risku analīzi, kā arī nosaka Informācijas sistēmas drošības prasības un risku ierobežošanas pasākumus;
    37.3. izstrādājamās Informācijas sistēmas IR turētājs un TR turētājs veic drošības prasību noteikšanu šai Informācijas sistēmai.
38. Informācijas sistēmas izstrāde:
    38.1. informācijas sistēmas izstrādes videi ir jāatbilst drošības prasībām, un to nodala

lietošanas vides;

38.2. pieejas tiesības Informācijas sistēmas izstrādes videi nosaka atbilstoši projektā iesaistīto personu pienākumiem;

38.3. katrai Informācijas sistēmai ir jābūt dokumentētai. Dokumentāciju glabā un lieto atbilstoši šīs dokumentācijas klasifikācijas līmenim. Dokumentācijai nodrošina rezerves kopijas, kuras glabā pēc līdzīgiem nosacījumiem kā citu datu rezerves kopijas;

38.4. dokumentācija iekļauj nepieciešamo informācijas apjomu, lai varētu kvalitatīvi veikt Informācijas sistēmas lietošanu, uzturēšanu un pārmaiņu pārvaldīšanu.

39. Informācijas sistēmas testēšana - pirms Informācijas sistēmas ieviešanas Skola veic Informācijas sistēmas darbības funkcionalitātes un drošības atbilstības noteiktajām prasībām pārbaudi;

40. Informācijas sistēmas ieviešana:

40.1. pirms Informācijas sistēmas ieviešanas ir jāsaņem to informācijas resursu turētāju atļauja, kuru Informācijas sistēmas tiks ietekmētas, lietojot jaunu Informācijas sistēmu;

40.2. pirms Informācijas sistēmas nodošanas lietošanai Skola veic darbinieku apmācību un citus pasākumus, lai nodrošinātu darbinieku izpratni par Informācijas sistēmas lietošanu, aizsardzības pasākumiem un to nozīmīgumu.

41. Informācijas sistēmas pārmaiņu pārvaldīšana:

41.1. Informācijas sistēmas pārmaiņas tiek veiktas tikai ar informācijas resursu turētāja atļauju;

41.2. Informācijas sistēmas pārmaiņas izdara, ievērojot šīs kārtības prasības attiecībā uz ieviešanu;

41.3. Skola identificē visus informācijas resursus un tehnoloģiskos resursus, kurus ietekmē pārmaiņas;

41.4. Skola analizē, kā pārmaiņas ietekmes esošos informācijas sistēmas drošības pasākumus un vai pārmaiņu rezultātā nesamazināsies informācijas sistēmas drošības līmenis;

41.5. Skolas veic informācijas sistēmas dokumentācijas papildināšanu;

41.6. pirms pārmaiņu ieviešanas Skola pārliecinās, vai informācijas sistēmas pārmaiņu rezultātā ir saglabāta datu integritāte un informācijas sistēmas drošības līmenis.

42. Informācijas sistēmas lietošanas izbeigšana:

42.1. likvidējot informācijas sistēmu, nodot to citai personai, t. sk. gadījumos, kad Skola pārtrauc kādu darbības veidu, kuru nodrošina šī Informācijas sistēma, jāveic nepieciešamos drošības pasākumus;

42.2. likvidējot informācijas sistēmu, Skola veic risku analīzi, kurā izvērtē iespējamo apdraudējumu citām Informācijas sistēmām kopumā;

42.3. Skola, ja nepieciešams, pieņem lēmumu par informācijas sistēmas lietošanas izbeigšanu, nosakot turpmākās darbības ar informācijas sistēmu — pilnīga likvidēšana vai glabāšana arhīvā;

42.4. ja informācijas sistēmu pilnībā likvidē, Skola nodrošina informācijas sistēmā ietilpstošo informācijas resursu likvidēšanu saskaņā ar šīs kārtības 8.2. punktu.