Biedrība Privātā vidusskola
Ādažu Brīvā Valdorfa skola
Skolas ielā 21, Ādažos, Ādažu novadā, LV-2164
www.abvs.lv,
e-pasts skola@abvs.lv
Reģistrācijas Nr. 40008007030,

APSTIPRINĀTI

Apstiprināts
ar Biedrības Privātā vidusskola ĀBVS
valdes priekšsēdētāja
2023. gada 21.augustā, rīkojumu Nr. 38

NOTEIKUMI
Ādažos, Ādažu novadā

Biedrības Privātā vidusskola Ādažu Brīvā Valdorfa skolas informācijas sistēmu lietošanas noteikumi

Izdoti saskaņā ar Ministru kabineta 20.07.2015. noteikumu Nr. 442 „Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 8. un 11. punktu

I. Vispārīgie noteikumi

1. Šie noteikumi nosaka kārtību, kādā Biedrība Privātā vidusskola
2. Ādažu Brīvā Valdorfa skola (turpmāk – Pārzinis) veic informācijas sistēmu drošu lietošanu, kā arī kārtību, kādā tiek veikta sistēmu lietotāju pieejas tiesību piešķiršana, to izmaiņas un anulēšana.
3. Noteikumos lietotie termini:
   3.1. **par tehniskajiem resursiem atbildīgā persona** – Pārziņa atbildīgā persona, kurai ar amata aprakstu uzticēta atbildība par informācijas tehnoloģiju resursiem un to drošību (Informācijas tehnoloģiju administrators);
   3.2. **informācijas sistēma** (turpmāk - IS) – strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kas nodrošina Pārziņa funkciju izpildei nepieciešamās informācijas ierosināšanu, radīšanu, apkopošanu, uzkrāšanu, apstrādāšanu, izmantošanu un iznīcināšanu;
   3.3. **IS tehniskie resursi –** serveri, tīkla aparatūra, komunikāciju līnijas un citi tehniskie līdzekļi, ko izmanto informācijas uzglabāšanai un apritei;
   3.4. **IS informācijas resursi** – datu faili, datu bāzes, arhīvi, u.c. informācija;
   3.5. **IS lietotājs –** persona, kurai darba pienākumu veikšanai piešķirta datortehnika un piekļuves tiesības darbam Pārziņa IS;
   3.6. **IS ārējie lietotāji** – personas, kurām ir tiesisks pamats un nodrošinātas tehniskas iespējas piekļūt Pārziņa IS;

3.7. **drošības incidents** - jebkāds kaitīgs notikums vai nodarījums, kura rezultātā tiek vai var tikt ietekmēta IS integritāte, konfidencialitāte un pieejamība;

3.8. **risks** - varbūtība, ka īstenojoties drošības apdraudējumam, Pārziņa informācijas vai tehniskie resursi varētu mainīties, sabojāties, tikt iznīcināti vai nonākt tādu personu rīcībā, kuras nav tam pilnvarotas, vai piekļūšana informācijas resursiem varētu būt traucēta, vai neiespējama;

3.9. **integritāte** - nesankcionēta lietotāja veiktās informācijas izmaiņas nav iespējamas (vai vismaz ir atklātas), un autorizēto lietotāju veiktās izmaiņas tiek izsekotas;

3.10. **konfidencialitāte** - informāciju redz un izmanto tikai personas, kurām tas atļauts;

3.11. **auditācijas pieraksti** – analīzei pieejami pieraksti, kuros reģistrēti dati par konkrētiem IS notikumiem (piekļuve, datu ievade, maiņa, dzēšana, izvade, u.c.);

4. Noteikumi attiecas uz Pārziņa pārvaldībā esošiem informācijas un tehniskajiem resursiem, un ir saistoši visiem darbiniekiem, kuri ir tiesīgi izmantot šos resursus, kā arī tiem ārpakalpojumu sniedzējiem, kuri Pārzinim sniedz ar informācijas tehnoloģijām saistītus pakalpojumus.

II. IS lietotāju reģistrācijas un tās atcelšanas kārtība

5. IS resursu lietošanas tiesību pārvaldības mērķis ir nodrošināt informācijas resursu kontroli.

6. Institūciju vadītāji atbild par padotībā esošo darbinieku lietotāju pieejas tiesību piešķiršanu, izmaiņu veikšanu un anulēšanu.

7. Lai izveidotu lietotāju pieejas tiesības vai veiktu izmaiņas tajās, institūcijas vadītājs iesniedz pieprasījumu (1.pielikums) pašvaldības izpilddirektoram, pievienojot Lietotāja apliecinājumu darbiniekam, kuram nepieciešamas piekļuves tiesības (2.pielikums).

8. Lietotāju pieejas tiesības piešķir atbilstoši darbiniekam individuāli noteiktajiem darba pienākumiem.

9. Izpilddirektors vīzē Lietotāja pieejas tiesību piešķiršanas pieprasījumu par tehniskajiem resursiem atbildīgā personai, kurš uzdot izpildi tam ITN speciālistam, kuram ir attiecīgās IS lietotāju administrēšanas tiesības.

10. Lietotāju pieejas tiesību piešķiršana Pārziņa informācijas resursiem personām, kas nav Pārziņa darbinieki, notiek tikai pēc pašvaldības izpilddirektora pieprasījuma (piemēram, pakalpojuma līguma gadījumā, kurā noteikti personas pienākumi, informācijas izmantošanas mērķi, konfidencialitātes prasības un atbildības).

11. ITN darbinieki atbild par lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, glabāšanu, kontroli un uzraudzību.

12. Lietotāju pieejas tiesības informācijas resursiem nekavējoties anulē:

12.1. darbiniekam, kurš pārtrauc darba tiesiskās attiecības ar pašvaldību, vai tiesības vairs nav nepieciešamas darba pienākumu veikšanai;

12.2. personai, kura ir izpildījusi līgumu ar Pārzini vai līguma izbeigšanās (pārtraukšanas) gadījumā.

13. Iestājoties 11. punkta gadījumam, institūcijas vadītājam, kura pakļautībā ir minētais darbinieks vai ārpakalpojuma veicējs, ir pienākums informēt par tehniskajiem resursiem atbildīgo personu, kas veic lietotāja tiesību bloķēšanu.

14. Lietotāju pieejas tiesības var anulēt arī par tehniskajiem resursiem atbildīgā persona, rakstiski informējot pašvaldības izpilddirektoru, ja lietotājs pieļāvis IS drošības politikas vai ar to saistītu dokumentu pārkāpumus.

15. ITN patstāvīgi veido, uztur un aktualizē lietotāju pieejas tiesību sarakstu.

16. ITN reizi gadā veic lietotāju pieejas tiesību kontroli, pārbaudot un salīdzinot piešķirto lietotāju pieejas tiesību atbilstību darbinieka amata pienākumiem, vai personas, kuras darbojas uz līguma pamata, spēkā esoša līguma noteikumiem.

III. Lietotāju tiesības, pienākumi, ierobežojumi un atbildība

17. Lietotājam ir tiesības:

    17.1. saņemt pieeju tiešo darba pienākumu veikšanai nepieciešamajiem IS tehniskajiem un informācijas resursiem;

    17.2. saņemt konsultācijas no par tehniskajiem resursiem atbildīgās personas vai ITN un IS tehnoloģisko resursu turētāja par IS darbību un drošības prasībām;

    17.3. izmantot piešķirtos IS informācijas resursus tikai darba pienākumu veikšanai.

18. Lietotājam nekavējoties jāziņo ITN, ja:

    18.1. radušās aizdomas, ka autentifikācijas rīku ir uzzinājusi vai ieguvusi cita persona;

    18.2. radušās aizdomas par novirzēm IS darbībā (piemēram, palēnināta interneta darbība, parādās sistēmai neraksturīgi paziņojumi);

    18.3. konstatēts datu zudums;

    18.4. nespēja autorizēties IS.

19. Lietotājam ir pienākums:

    19.1. pirms IS lietošanas, iepazīties ar jomas normatīvo aktu prasībām attiecībā uz IT lietošanu un apliecināt šo iepazīšanos rakstveidā;

    19.2. reizi gadā iziet apmācības par IT jomas normatīvo aktu prasībām;

    19.3. izlasīt gan par tehniskajiem resursiem atbildīgās personas vai ITN, gan IS tehnoloģisko resursu turētāja sūtītos ziņojumus un izpildīt tajos norādītās darbības;

    19.4. pārtraucot darba tiesiskās attiecības ar Pārzini, nekavējoties nodot ITN viņa rīcībā esošo aprīkojumu, informāciju, t.sk. datnes un dokumentus, kas tika saņemti, vai bija lietotāja paša radīti darba pienākumu izpildes laikā;

    19.5. neizpaust un neizmantot savu vai trešo personu interesēs ierobežotas pieejamības informāciju, kas saņemta no IS, kā arī ievērot tiesisko regulējumu informācijas atklātības un fizisko personu datu apstrādes jomā;

    19.6. saglabāt informācijas konfidencialitāti arī pēc darba (līguma izpildes) tiesisko attiecību izbeigšanās.

20. Lietotājam aizliegts:

    20.1. izmantot IS informācijas un tehnoloģiskos resursus, lai izplatītu vai uzglabātu ar darbu nesaistītu informāciju;

    20.2. veikt darbības, kas nepamatoti noslogo IS informācijas un tehnoloģiskos resursus;

    20.3. nesankcionēti nodot IS informācijas vai tehnoloģiskos resursus trešajai personai;

    20.4. nesankcionēti mainīt IS konfigurāciju;

    20.5. piekļūt tiem IS resursiem, kuriem viņam nav piešķirtas piekļuves tiesības;

    20.6. izpaust lietotājvārdu (identifikatoru) un paroles.

21. Lietotājs atbild par darbībām, kas veiktas, izmantojot viņa identifikatoru un autentifikācijas rīku, kā arī par zaudējumiem, kas radušies, neievērojot IS drošības prasības.

IV. IS lietošanas kārtība

22. **Datortehnika** jāizvieto tādā veidā, lai pie tās nevarētu piekļūt trešās personas, nodrošinoties pret jebkurām destruktīvajām darbībām, piemēram, inficētās zibatmiņas ievietošanas darbstacijā, barošanas vada izraušanas, utt. Izvades iekārtas (printeris, monitors) vēlams izvietot tā, lai trešās personas nevarētu nesankcionēti piekļūt tiem neparedzētai informācijai.
23. ITN izvērtē. vai lietotājam nepieciešams izsniegt lietošanā citu datortehniku.
24. ITN piešķir lietotājam datortehniku no institūcijām pieejamā datortehnikas inventāra. Ja nepieciešamā datortehnikas vienības konfigurācija nav pieejama, tad ITN organizē datortehnikas un programmatūras iegādi.
25. Sākotnējo datortehnikas konfigurēšanu veic ITN. Datortehnika tiek konfigurēta darba pienākumu veikšanai, ievērojot šādas minimālās prasības:
    25.1. katram lietotājam ir izveidots lietotājvārds un pieslēgšanās parole;
    25.2. ikdienas lietotājam nav piešķirtas datora administratora tiesības;
    25.3. tīmekļa pārlūkprogrammās (*Mozilla Firefox, Google Chrome,* u.c.) ir atslēgta automātiskā paroļu un lietotājvārdu saglabāšana, kā arī automātiskā autorizēšanās sistēmā;
    25.4. ieslēgta automātiskā darbstacijas bloķēšana pēc 10 minūtēm, ja tā netiek izmantota;
    25.5. operētājsistēmas atjauninājumi, antivīruss, ugunsmūris ir nepārtraukti aktīvi.
26. ITN veic programmatūras instalēšanu atbilstoši programmatūras instalēšanas posmam.
27. ITN nodod lietotājam datortehniku, sastādot datortehnikas izsniegšanas-pieņemšanas aktu par inventāra nodošanu materiāli atbildīgajai personai. ITN un lietotājs pārbauda datortehnikas darbību un pārliecinās par aprīkojuma atbilstību, t.sk. salīdzinot numurus aktā un uz datortehnikas. Pēc pārbaudes ITN un lietotājs paraksta aktu, kura viens eksemplārs glabājas pie lietotāja, otrs – Grāmatvedības nodaļā. Pēc nepieciešamības GRN nosūta grāmatvedības pārskatu par pamatlīdzekļu un mazvērtīgo inventāru izvietojumu materiāli atbildīgām personām.
28. Datortehniku nodod lietošanā lietotājam materiālā atbildībā. Lietotājs ir civiltiesiski atbildīgs par viņa lietošanā nodoto datortehniku un informācijas resursiem, kas tajā atrodas, kā arī to drošību un saglabāšanu.
29. Pašvaldības telpās aizliegts darba vajadzībām lietot personīgos datorus, kā arī pieslēgt tos iekšējam datortīklam. Nav atļauta nezināmas izcelsmes datu nesēju (piemēram, ārējie cietie diski, zibatmiņas, utt.) lietošana kopā ar Pārziņa un tā institūciju datoriem. Personīgie datu nesēji var tikt izmantoti tikai ar ITN atļauju, kā arī pirms to lietošanas obligāti jāveic pārbaude ar antivīrusa programmu.
30. Lietotājs lieto IS tehniskos resursus atbilstoši šādiem vispārīgiem nosacījumiem:
    30.1. izmanto tos tikai amata aprakstā noteikto pienākumu pildīšanai;
    30.2. lieto tos darba vietā, izņemot klēpjdatorus un citas mobilas iekārtas, kas darba pienākumu veikšanai var lietot ārpus darba vietas, saskaņojot ar darbinieka priekšnieku;
    30.3. neatstāj tos nepieskatītus publiski pieejamās vietās un redzamā vietā automašīnā. Klēpjdatoru, ja iespējams, uzglabā slēdzamos skapjos vai atvilktnēs aizvērtā veidā. Komandējumos vai darba braucienos klēpjdatoru pārvadā kā rokas bagāžu;
    30.4. pret IS tehniskajiem resursiem izturas saudzīgi;

30.5. izvairās no datortehnikas pārkaršanas, pārliecinās, ka nav aizsegti datortehnikas ventilatori;

30.6. datortehniku novieto uz līdzenām un stabilām darba virsmām;

30.7. klēpjdatorus pārnēsā tikai atbilstošā somā;

30.8. nenovieto priekšmetus uz datortehnikas;

30.9. patvaļīgi neskrūvē datortehnikas korpusa skrūves un neveic remontu, kā arī nebojā vai nenoņem uzlīmes ar programmatūras autentifikācijas numuru un inventāra numuru, kā arī neaplīmēt datortehniku ar uzlīmēm un magnētiem;

30.10. nepakļaut datortehniku tiešai saules gaismas, lietus un mitruma, postošu ķimikāliju vai citu šķidru vielu iedarbībai. Ja datortehnikā iekļuvis šķidrums, tehniku nekavējoties atvieno no elektrotīkla un paziņo ITN;

30.11. nelieto sildītājus vai citus karstuma vai uguns avotus datortehnikas tiešā tuvumā;

30.12. nepieslēdz citas elektroiekārtas datortehnikai paredzētajās elektrības rozetēs;

30.13. izmanto tikai savu IS lietotāja kontu. Ieejot sistēmā, izmanto savu paroli. Datortehnikas lietošanas laikā neveic sākotnējās konfigurācijas maiņu, izņemot ar ITN atļauju. Sākotnējās konfigurācijas maiņu var veikt tikai uz noteiktu laiku vai uz īpašu darba uzdevumu pildīšanas brīdi, pēc tam atjaunojot sākotnējos uzstādījumus;

30.14. ikdienas darba pienākumu veikšanas laikā sekot drošības sistēmas (antivīruss, operētājsistēmas atjauninājumi un ugunsmūris) paziņojumiem, nekavējoties informē par tiem ITN. Ja ir aizdomas, ka dators ir inficēts, vai var būt inficēts ar ļaunatūru, par to nekavējoties paziņo ITN;

30.15. prombūtnes (arī īslaicīgas prombūtnes) laikā ieslēgt ar paroli aizsargātu ekrānsaudzētāju, vai arī nobloķēt datoru, nospiežot pogu Ctrl-Alt-Del kombināciju, un izvēloties iespēju „Lock Computer” vai nospiežot pogu kombināciju ⊞ + L;

30.16. darba dienas beigās, vai, beidzot darbu, datortehniku izslēgt, izmantojot funkciju „Shut down” vai „Install updates and shut down”, izņemot, ja darba pienākumu veikšanai nepieciešams pie datora pieslēgties attālināti;

30.17. klēpjdatora nozaudēšanas, zādzības vai pilnīgas iznīcināšanas gadījumā, nekavējoties informē policiju, tiešo vadītāju, par tehniskajiem resursiem atbildīgo personu un ITN.

31. Galda datora vai klēpjdatora profilaksi, remontu un tehniskā aprīkojuma nomaiņu veic ITN. Profilakses veic:

31.1. ja klēpjdatoram ir tehniskas problēmas vai tas ir inficēts ar datorvīrusiem;

31.2. materiālo vērtību inventarizācijas laikā;

31.3. pēc ITN pieprasījuma, lai veiktu programmatūras licenču atjaunošanu un papildu konfigurāciju.

32. **Elektroniskā pasta lietošana** notiek šādā kārtībā:

32.1. institūcijas vadītājs informē ITN par jaunu darbinieku stāšanos amatā, darbinieku pārcelšanu, darbinieka amata maiņu vai darbinieka vārda vai uzvārda maiņu;

32.2. ja darbiniekam, uzsākot darba tiesiskās attiecības, nepieciešama elektroniskā pastkaste, institūcijas vadītājs informē ITN, kas veic elektroniskās pastkastes izveidi vai izmaiņas, ievērojot šādus nosacījumus:

32.2.1. piešķir lietotājam pieejas tiesības elektroniskā pasta sistēmai;

32.2.2. uzstāda elektronisko pastkasti uz lietotāja darba datora elektroniskā pasta programmas, kā arī veic elektroniskās pastkastes pāruzstādīšanu un iestatīšanu, ja nepieciešams;

32.2.3. veic elektronisko pastkastu uzskaiti un kontroli;

32.2.4. lietotāja elektroniskā pasta adrese satur informāciju par sūtītāju un adresi veido pēc šāda principa:

32.2.4.1. lietotājam ar vienu vārdu un uzvārdu elektroniskā pasta adrese ir *Vards.Uzvards@[domena adrese].lv*;

32.2.4.2. lietotājam ar diviem uzvārdiem elektroniskā pasta adrese ir *Vards.Uzvards1@[domens].lv*;

32.2.4.3. lietotājam ar diviem vārdiem elektroniskā pasta adrese ir *Vards1.Uzvards@[domens].lv*;

32.2.4.4. ja divu darbinieku vārdi un uzvārdi ir identiski, otra darbinieka elektroniskā pasta adrese tiek izveidota kā *Uzvards.Vards@*[domens]*.lv*;

32.2.5. lietotāja e-pastu var veidot *@[domens].lv* vietā lietojot institūcijas IT e-pastu resursa nosaukumu, piem., *@adazuvidusskola.lv*, u.c.;

32.2.6. ja lietotājam mainās vārds vai uzvārds, ITN veic izmaiņas elektroniskā pasta adresē un nodrošina elektroniskā pasta saņemšanu uz iepriekšējās elektroniskās pasta adresi ne ilgāk, kā vienu mēnesi;

32.3. lietotājam izbeidzot darba tiesiskās attiecības, anulē pieejas tiesības elektroniskajai pastkastei šādā kārtībā:

32.3.1. institūcijas vadītājs e-pastā informē ITN par darba tiesisko attiecību izbeigšanas datumu ar darbinieku;

32.3.2. ITN reģistrē pieprasījumu un liedz darbiniekam pieeju elektroniskajai pastkastei no darba tiesisko attiecību izbeigšanas brīža;

32.3.3. darbinieka tiešais vadītājs telefoniski vai e-pastā var pieprasīt, lai ilgstošā prombūtnē esošā lietotāja elektroniskais pasts tiek pāradresēts uz tiešā vadītāja vai cita darbinieka elektronisko pastu, kurš pārņem lietotāja darba pienākumus;

32.4. lietotājs uzsāk darbu ar elektronisko pasta sistēmu, ievērojot, ka:

32.4.1. lietotājam ir tiesības lietot elektronisko pastkasti atbilstoši piešķirtajām pieejas tiesībām;

32.4.2. elektroniskā pasta nosūtīšanai vai saņemšanai, kalendāra organizēšanai, uzdevumu veidošanai vai apstrādei, kontaktpersonu un piezīmju vienumu uzkrāšanai lietotājs izmanto tikai šim mērķim paredzēto programmatūru;

32.4.3. lietotājs ir atbildīgs par elektroniskā pasta izmantošanu tikai darba vajadzībām;

32.5. lietotājam aizliegts:

32.5.1. nodot savu lietotāja vārdu un paroli citām personām;

32.5.2. izplatīt izplatīšanai neparedzētu darba informāciju ārpus institūcijām;

32.5.3. veikt nesankcionētas darbības, izmantojot piešķirto elektronisko pastkasti;

32.5.4. pieļaut citu personu piekļūšanu elektroniskajai pastkastei un tās izmantošanu;

32.5.5. izplatīt pornogrāfiska, vardarbību propagandējoša vai naidu kurinoša satura materiālus;

32.5.6. sūtīt ziņojumus, par kuru nokļūšanu līdz adresātam sūtītājam ir šaubas;

32.5.7. vērt vaļā pielikumus no apšaubāmu adresātu sūtītiem e-pastiem;

32.5.8. sūtīt vienā elektroniskā pasta sūtījumā informāciju vairāk 30 MB apjomā;

32.5.9. uzstādīt citu klienta programmatūru;

32.5.10. darba e-pastu izmantot kā kontaktinformāciju personām un iestādēm, kas nav saistīts ar darba pienākumu veikšanu (personīgai preču un pakalpojumu iegādei, komunālajiem maksājumiem un kreditoriem);

32.6. lietotājs sagatavo, nosūta un saņem e-pastu, ievērojot, ka:

32.6.1. sagatavojot e-pastu nosūtīšanai vairākiem institūciju darbiniekiem:

32.6.1.1. laukā „Kam" ("To" – angļu val.) norāda adresāta e-pasta adresi. Ja adresāti ir vairāki, e-pasta adreses atdala ar simbolu ";";

32.6.1.2. laukā „Tēma" ("Subject" – angļu val.) ar latīņu alfabēta burtiem raksta īsu informāciju par vēstules saturu;

32.6.1.3. e-pasta teksta laukā nepieciešamības gadījumā ieraksta papildu informāciju, kas atvieglo adresātam domātās informācijas identificēšanu un atsauci par datu drošību un datu aizsardzību;

32.6.2. sagatavojot e-pasta nosūtīšanai ārējiem adresātiem (piem.. klientiem, sadarbības partneriem, u.tml.):

32.6.2.1. lai neizpaustu e-pasta adreses kā personas datus, lietotājs laukā „Kam" ("To" – angļu val.) norāda viena adresāta e-pasta adresi. Ja adresāti ir vairāki, adresātu e-pasta adreses norāda ailē "Bcc", atdalot ar simbolu ";";

32.6.2.2. e-pasta teksta laukā obligāti ieraksta papildu informāciju, kas atvieglo adresātam paredzētās informācijas identificēšanu un atsauci par datu drošību un datu aizsardzību;

32.7. lietotājs izvērtē vai uz laiku atradīsies prombūtnē (atvaļinājums, komandējums, darba brauciens, kā arī citos prombūtnes gadījumos). Ja lietotājs atrodas prombūtnē, viņš savā elektroniskajā pastkastē aktivizē automātiskās atbildēšanas iespēju, kas nosūta katram e-pasta sūtītājam atbildi par lietotāja prombūtni. Lietotājs atbild par datuma, e-pasta un telefona numura aktualizāciju automātiskās atbildes tekstā atbilstoši situācijai. Atgriežoties no prombūtnes, lietotājs deaktivizē automātiskās atbildēšanas iespēju;

32.8. ja lietotājs koplieto pastkasti ar citiem lietotājiem, viņš savā pastkastē norāda attiecīgos citus lietotājus un to piekļuves tiesību līmeni elektroniskai pastkastei. Par piekļuves nodrošināšanu lietotājs informē citus darbiniekus, kuri izmantojot e-pasta programmatūru, pievieno koplietoto pastkasti;

32.9. ja elektroniskās pastkastes piekļuves paroli ir uzzinājis kāds cits vai ir aizdomas, ka to ir uzzinājis kāds cits lietotājs, nekavējoties informē ITN, kas noskaidro cēloni un uz nenoteiktu laiku deaktivizē lietotāja kontu, vai nomaina paroli. Paroli nav atļauts sūtīt pa e-pastu;

32.10. ja pamanīti nesankcionēti piekļuves gadījumi elektroniskajai pastkastei, lietotājs mutiski par to informē ITN, kas veic pārbaudi un pasākumus, lai novērstu šādus gadījumus;

32.11. ja nepieciešams automātiski dzēst saņemtos liekpastus un mēstules, lietotājs e-pastā informē ITN, kas veic e-pasta sistēmas konfigurēšanu un nodrošina automātisku liekpastu un mēstuļu dzēšanu;

32.12. ja lietotājs izbeidz darba tiesiskās attiecības vai atrodas ilgstošā prombūtnē, tiešais priekšnieks izvērtē un mutiski informē IT nodaļu, kāda informācija lietotāja pastkastē ir nepieciešama turpmākajam darbam un to nepieciešams saglabāt, kā arī norāda jaunu lietotāju, kuram jānodrošina piekļuve šai informācijai. ITN nodrošina attiecīgās informācijas saglabāšanu un piekļuvi jaunajam lietotājiem;

32.13. e-pasta kontakti tik lietoti, ievērojot, ka:

32.13.1. institūciju lietotāju un lietotāju grupu e-pasta adreses glabā kopējā adrešu grāmatā uz e-pasta servera;

32.13.2. lietotājs var veidot savu personālo adrešu grāmatu, kurā glabā darba vajadzībām nepieciešamo kontaktpersonu e-pasta adreses un citu informāciju par šīm kontaktpersonām un nodrošina savas personālās adrešu grāmatas uzturēšanu;

32.13.3. institūciju lietotāju un lietotāju grupu e-pasta adrešu grāmatas uzturēšanu un informācijas aktualizēšanu uz e-pasta servera nodrošina ITN;

32.14. ITN reizi nedēļā sagatavo IS lietotāju elektronisko pastkastu rezerves kopijas;

32.15. katrs lietotājs ir disciplināri, administratīvi, civiltiesiski un krimināltiesiski atbildīgs par darbībām, kuras veiktas ar e-pastu, izmantojot viņa lietotāja vārdu vai paroli. Lietotājs uzņemas civiltiesisko atbildību par sekām, kas var rasties ikvienas nesankcionētās darbības rezultātā saistībā ar e-pastu.

33. **Informācijas sistēmas** lietotājam jāievēro šādi noteikumi:

33.1. lietotājs no IS saņemto informāciju drīkst izmantot tikai tiešo darba pienākumu veikšanai. Informāciju nedrīkst izmantot komerciāliem vai citādiem mērķiem;

33.2. lietotājs nedrīkst nodot citiem darbiniekiem un trešajām personām savus rekvizītus (lietotāja vārdu, paroli). Lietotājam regulāri (konkrētā IS noteiktā laika posmā) jāmaina lietošanas parole;

33.3. lietotājs nedrīkst veikt darbības, kas vērstas pret IS drošību, izmantojot neparedzētas pieslēgšanās iespējas. Beidzot (pārtraucot) darbu, lietotājam jāaizver pārlūkprogramma. Lietotājs nedrīkst saglabāt lietošanas paroli, izmantojot pārlūkprogrammas iespējas;

33.4. lietotājs nedrīkst veikt nelegālu datu, sistēmas vai tās daļu kopēšanu (par nelegālām uzskata visas darbības, kuru izpildei netiek izmantotas atļautās, uz ekrāna redzamās komandas, vai kuras tiek izpildītas automātiski, bez cilvēka līdzdalības informācijas pieprasījumu formēšanas procesā, neatkarīgi no šo darbību mērķa);

33.5. saņemto informāciju lietotājs nedrīkst pārveidot, publicēt, pārvadīt, piedalīties tās nodošanā vai pārdošanā, reproducējot kopumā vai tās daļas. Jebkuras ar datiem veiktas apstrādes darbības, ieskaitot datu vākšanu, reģistrēšanu, ievadīšanu, glabāšanu, sakārtošanu, pārveidošanu, izmantošanu, nodošanu, pārraidīšanu un izpaušanu, bloķēšanu vai dzēšanu drīkst veikt tikai likumdošanā vai Pārziņa iekšējos normatīvajos aktos noteiktajā kārtībā;

33.6. lietotājs nedrīkst no IS saņemto informāciju glabāt publiski pieejamās vietās.

34. Visas IS lietotāja darbības tiek uzraudzītas IS ietvaros un iegūto informāciju var izmantot drošības incidentu izmeklēšanā un iespējamo draudu laicīgai novēršanai.

35. **Drukas iekārtu** lietošanā jāievēro šādi noteikumi:

35.1. darbinieki ir tiesīgi izmantot drukas iekārtas tikai tiešo darba pienākumu veikšanai;

35.2. dokumentu kopēšana un izdruka trešajām personām, vai darbinieku vajadzībām, kas nav saistītas ar tiešo pienākumu veikšanu, tiek veikta speciāli tam paredzētās vietās, saskaņā ar noteikto attiecīgā pakalpojuma cenrādi;

35.3. koplietošanas drukas iekārtās aizliegts atstāt personu datus un konfidenciālu saturu saturošus dokumentus;

35.4. veicot izdrukas uz koplietošanas drukas iekārtu, kas satur sensitīvus vai konfidenciāla rakstura datus, jānodrošina šo dokumentu fiziskā aizsardzība;

35.5. nepareizi vai nekvalitatīvi veiktās izdrukas nekavējoties likvidējamas dokumentu smalcinātājā.

36. Izmantojot privāto **mobilo telefonu** darbam, vai **darba telefonu**, jāievēro:

36.1. visas ierīces jāaizsargā ar paroli. To veidošanā jālieto burti, cipari un simboli, kā arī regulāri tās jāmaina. Vēlams izmantot vairāku līmeņu aizsardzību – ne tikai pašai ierīcei, piemēram, PIN kodu, pirkstu nospiedumu lasītāju, figūras zīmējumu, u.c., bet atšķirīgas paroles arī saturam – darba e-pastam, aplikācijām, u.tml. Caur mobilo telefonu lietojot Pārziņa IS, tajā skaitā e-pastu, aizliegts izmantot funkciju, kas ļauj automātiski atcerēties pieejas paroles;

36.2. darba un privātās dzīves dalījums ir drošāka metode mobilo ierīču drošības risinājums, piemēram, *KNOX*, kur atsevišķā "konteinerā" nodalīti darba dati ir aizsargāti pret datu noplūdi, vīrusiem, ļaunprogrammatūrām, hakeru uzbrukumiem un gadījumos, kad mobilās ierīces tiek nozagtas, vai pazaudētas;

36.3. datu dublēšanai ir vēlama informācijas uzglabāšanu arī kādā citā vietā – "datu mākonī" vai datorā ar šifrētu pieeju, lai varētu tos droši atjaunot vai pārnest uz citu ierīci;

36.4. attālinātai kontrolei jānodrošina ierīce ar aizsardzības risinājumiem gadījumiem, ja tā nonākusi nelabvēļu rokās. Ar tādu aplikāciju palīdzību kā *Find My Mobile i*espējams atrast telefonu un to attālināti bloķēt;

36.5. drošam bezvadu tīklam jāizvēlas uzticams interneta pieslēgums. Pieslēdzoties publiskam bezmaksas bezvadu tīklam, jāizvairās no īpaši konfidenciālām aktivitātēm, piemēram, paroļu ievadīšanas internetbankā vai naudas operācijām. Lietojot publisku bezmaksas bezvadu tīklu, aizliegts izmantot Pārziņa IS;

36.6. bezvadu savienojumu lietošanai pēc nepieciešamības atslēdz visu, ko nelieto. Ja konkrētajā brīdī nav nepieciešams datu pieslēgums, atrašanās vietas noteikšana, Wi-Fi pieslēgums, Bluetooth vai citi pakalpojumi, tos nepieciešams atvienot, samazinot iespēju, ka telefons pieslēdzas nevēlamam Wi-Fi tīklam;

36.7. nav atļauta IS lietotāja tiesību maiņa, lai uzstādītu ierīcē apšaubāmas izcelsmes un ražotāja neatbalstītu programmatūru. Mobilās ierīces drošības līmenis būs ievērojami augstāks, saglabājot ražotāja uzstādīto aizsardzību un oficiālus programmatūras avotus. Operētājsistēma un aplikācijas regulāri jāatjaunina;

36.8. aizliegts glabāt paroles ierīcē vai e-pastā, nodot paroles citiem cilvēkiem. Jāievēro piesardzība interneta vietņu pārlūkošanā un izmantojot nejauši atrastus QR kodus.

Nepazīstamu aplikāciju uzstādīšanu veic nesteidzīgi, vispirms izlasot noteikumus, atsauksmes un visus piekrišanas nosacījumus;

36.9. nekavējoties ziņo savam mobilajam operatoram un ITN par nozaudētu ierīci vai aizdomīgām darbībām, kas saistīta ar datiem, parolēm vai ierīci.

V. IS lietotāju atbalsta kārtība

37. Par atklātajām IS ievainojamībām, vai ja notikusi ļaunprātīga ielaušanās sistēmā, iejaukšanās vai nesankcionēta piekļuve personas datiem, lietotājs nekavējoties informē par tehniskajiem resursiem atbildīgo personu vai ITN.

38. Darba laikā lietotājam ir tiesības lūgt ITN atbalstu IS un ar to saistītu resursu lietošanā. Ja atbalsts vajadzīgs nekavējoties un ārpus darba laika, lietotājs nosūta jautājumu SMS vai e-pastā. Izvērtējot iespējamos riskus IS drošībai, par tehniskajiem resursiem atbildīgā persona vai ITN lemj par nekavējošu atbildes reakciju, vai nākamajā darba dienā, informējot par to lietotāju.

39. Par tehniskajiem resursiem atbildīgā persona vai ITN nodaļa, izvērtē notikumu un gadījumos, ja noticis drošības incidents, kas apdraud IT integritāti, pieejamību vai konfidencialitāti, nekavējoties informē CERT (Informācijas tehnoloģiju drošības incidentu novēršanas institūciju) t. 67085888 (ziņojumu pieņemšana 24 x 7, CERT.LV darba laiks - darba dienās) cert@cert.lv, cert@cert.gov.lv.

40. Ja risks skar personu datus, nekavējoties jāinformē Datu aizsardzības speciālists pašvaldības oficiālajā e-pastā, ar norādi *"Personas datu aizsardzības speciālistam"*.

VI. Noslēguma jautājumi

41. Šo noteikumu neievērošana, un IS lietošanas tiesību iegūšana, izmantojot trešo personu pieejas paroles un trešo personu vārdā, tiek uzskatīta par sistēmas integritātes apzinātu bojājumu, kas klasificējams kā krimināls pārkāpums.

42. Šos noteikumus pārskata un aktualizē vismaz reizi gadā.

Valdes priekšsēdētāja K. Dāvidsone

1.pielikums
Biedrības Privātā vidusskola ĀBVS
.2023. noteikumiem Nr. ….

Biedrības Privātā vidusskola ĀBVS Valdes priekšsēdētājai

Iesniegums tehnisko resursu un IS lietotāja tiesību piešķiršanai

Lūdzu piešķirt

Vārds, Uzvārds_____

Amats_____

Telefona numurs_____

tehniskos resursus:

_____

_____

_____

_____

_____

_____

e-pasta adresi, pieeju un IS lietotāja tiesības šādām informācijas sistēmām:

_____

_____

_____

_____

_____

Paraksts:_____

Ādažu novadā, 202__.gada _____._____

2.pielikums
Biedrības Privātā vidusskola ĀBVS……...
noteikumiem Nr. ……

Apliecinājums par Biedrības Privātā vidusskola ĀBVS informācijas sistēmu lietošanas noteikumu ievērošanu

Parakstot šo apliecinājumu, es:

Vārds, Uzvārds_____

Amats_____

Telefona numurs_____

apliecinu, ka esmu iepazinies ar Biedrības Privātā vidusskola ĀBVS Informācijas sistēmu lietošanas noteikumiem, Informācijas sistēmu drošības politiku un Informācijas sistēmu drošības iekšējiem noteikumiem, tajā skaitā, pārzinu rīcību ar IS drošību saistītās ārkārtas situācijās un savu atbildību.

Paraksts_____

Ādažu novadā, 202__.gada _____._____