RSU Informācijas sistēmas elektronisko platformu drošības politikas saīsinātais variants

Dotais dokuments ir RSU Informācijas sistēmas elektronisko platformu drošības politikas saīsinātais variants, kas paredzēts lai iepazīstinātu RSU darbiniekus ar RSU Informācijas sistēmas elektronisko platformu drošības politikas pamatnostādnēm. Lūdzam Jūs iepazīties arī ar pilno RSU Informācijas sistēmas elektronisko platformu drošības politikas versiju.

RSU IS drošības pārvaldība balstās uz sekojošiem principiem[1]

- Likumība. RSU informācijas apstrāde tiks veikta tikai normatīvajos aktos noteikto funkciju izpildei un informācijas aprites process atbildīs likumos noteiktām drošības prasībām;
- Personas datu aizsardzība. Pieejas tiesības personas datiem ierobežojamas ar dažādiem scenārijiem, atkarībā no RSU Darbinieka statusa un veicamajiem pienākumiem;
- Tikai nepārprotami autentificētu personu piekļuve datiem. Jebkuras saistītās IS lietotājam, lai viņš varētu piekļūt tā vai cita veida datiem, nepieciešama nepārprotama un droša autentifikācija. Jebkurā saistītās IS pieprasījumā jābūt nepārprotami identificētam lietotājam, kurš pieprasījis datus un, nepieciešamības gadījumā – datu pieprasījuma pamatojumam, pretējā gadījumā šāds pieprasījums netiks apstrādāts;
- Atbildība. Katrai IS sastāvdaļai un informācijas aprites procedūrai ir noteikta atbildīgā persona;
- Samērojamība. Finanšu ieguldījumi informācijas aizsardzības pasākumiem nepārsniedz iespējamos tiešos un netiešos finansiālos zaudējumus drošības incidentu gadījumos. Šis princips nav attiecināms uz personas datu aizsardzību;
- Monitorējamība. IS jāparedz mehānismi, kuri identificē iespējami nepamatotus informācijas pieprasījumus un ir paredzēta šādu gadījumu izmeklēšana. Iespējami nepamatoto un aizdomīgo pieprasījumu analīzei un izvērtēšanai jānorisinās pietiekami kompetentā institūcijā;
- Neatkarība no ārējiem apstākļiem. Lai gan pilnībā drošu IS nav iespējams izveidot, jāparedz IS galveno tehnisko resursu dublēšana, izvietojot funkcionāli līdzvērtīgus tehniskos resursus dažādās, ģeogrāfiski nošķirtās vietās, lai ārēju apstākļu ietekme (piemēram, inženiertīklu avārija) neapturētu IS darbību.

[1] RSU Informācijas sistēmas elektronisko platformu drošības politika, 3.punkts

Konfidencialitāte[2]

Atkarībā no personu loka, kuras ir pilnvarotas informāciju saņemt, IS ir noteikti trīs informācijas konfidencialitātes līmeņi:

- Publiska (K1) Informācija ir brīvi pieejama visiem IS administratoriem un jebkurai organizācijai vai personai, kas šo informāciju ir pieprasījusi. Šīs informācijas izplatīšana neietekmē IS vai saistīto sistēmu pārziņu darbību negatīvā veidā.
  Par publiski pieejamu tiks uzskatīta sekojoša informācija:
  - IS lietošanas dokumentācija.

- Iekšējās lietošanas (konfidenciāla) (K2) Informācija tiek aizsargāta no publiskas piekļuves. Informācija ir pieejama IS un saistīto sistēmu lietotājiem, kuriem ir atbilstošs tiesību līmenis. Informācija nav pieejama trešajām personām un trešo personu informācijas sistēmām bez atbilstošas atļaujas. Informācijas nesankcionēta nokļūšana trešo personu rīcībā var radīt zaudējumus vai neērtības IS pārzinim, tomēr sekas nav kritiskas. Šis līmenis tiek piešķirts jebkurai informācijai, ja vien nav atklāti norādīts, ka tā ir publiska vai slepena.

- Slepena (K3) Informācija tiek aizsargāta no ārējās un iekšējās piekļūšanas. Pieeja pieļaujama IS un saistīto sistēmu lietotājiem, kuriem ir pilnvarojums piekļūt konkrētai informācijai. Ja informācija kļūst zināma trešajai personai, iespējams nopietns datu subjekta tiesību aizskārums vai ievērojami zaudējumi IS pārzinim vai saistīto sistēmu pārziņiem.
  Pie slepenas informācijas pieder:
  - Jebkura informācija par IS lietotāju identitāti un parolēm;
  - Jebkura informācija par datu subjekta personas datiem.
  - Iesniegumu uzskaite (reģistrēta Datu Valsts inspekcijā);
  - Reflektantu uzskaite (reģistrēta Datu Valsts inspekcijā);
  - Studējošo uzskaite (reģistrēta Datu Valsts inspekcijā);
  - Bibliotēkas lasītāju uzskaite (reģistrēta Datu Valsts inspekcijā).

Šajā sadaļā noteiktie konfidencialitātes noteikumi neattiecas uz normatīvajos aktos noteiktajā kārtībā saņemtajiem tiesībsargājošo iestāžu informācijas pieprasījumiem.

Informācijas resursa vērtība [3]

Informācijas resursa vērtība tiek raksturota ar vērtības pakāpēm, kuras var būt sekojošas – augsta riska, vidēja riska vai zema riska.

- Augsta riska pakāpe (R3) piešķirama informācijai, ja ar šo informāciju saistīts drošības incidents var apdraudēt IS darbības turpināšanu vai radīt nopietnu ar likumā noteiktu trešo personu tiesību aizskārumu, vai radīt tiešus draudus personas dzīvībai.
  Augsta riska pakāpe ir piešķirama:

[2] RSU Informācijas sistēmas elektronisko platformu drošības politika, 4.1.punkts
[3] RSU Informācijas sistēmas elektronisko platformu drošības politika, 4.2.punkts

- Sensitīviem personas datiem;
- IS servisu programmatūrai;
- Lietotāju identifikācijas informācijai.

Uzskaitījums papildināms Sistēmas projektēšanas un izstrādes stadijās.

- Vidēja riska pakāpe (R2) piešķirama informācijai, ja ar šo informāciju saistīts drošības incidents var nopietni traucēt darbību vai radīt nopietnus zaudējumus. Vidēja riska pakāpe piešķirama:
  - Sistēmas audita pierakstiem (ciktāl tas neskar sensitīvu informāciju);

  Uzskaitījums papildināms Sistēmas projektēšanas un izstrādes stadijās.

- Zema riska pakāpe (R1) tiek piešķirta informācijai, kuras pazaudēšana vai nonākšana personu rīcībā, kas tam nav pilnvarotas, nerada nopietnus zaudējumus vai darbības nopietnus traucējumus un nerada trešo personu tiesību aizskārumu.
  Zema riska pakāpe piešķirama:
  - Informācijai, kura klasificēta kā publiski pieejama;

IS lietotāji[4] – RSU darbinieki vai studenti, vai ar RSU saistīti datu subjekti. IS lietotāju tiesības un pienākumi: IS lietotājam saņemot lietotājvārdu un paroli piekļuvei IS, ir ar savu parakstu jāapliecina iepazīšanās ar IS drošības dokumentāciju. IS lietotāji, atbilstoši savam piekļuves līmenim vai darba uzdevumu vajadzībām, drīkst piekļūt tiem IS apgabaliem, kurus viņi ir tiesīgi izmantot. IS lietotājam nekavējoties jāpaziņo IS administratoram (-iem) par IS drošības incidentiem vai/un darbības traucējumiem.

Informācijas sistēmas darbināšanas vispārējie nosacījumi, kas attiecināmi uz RSU darbiniekiem[5]

- Visos līmeņos ir skaidri noteikta atbildība par informācijas drošības nodrošināšanu. Katram informācijas un tehniskajam resursam ir noteikts atbildīgais darbinieks. Katrai informācijas drošības procedūrai ir noteikts darbinieks, kurš ir atbildīgs par šīs procedūras darbības nodrošināšanu;
- Personāla loma un pienākumi drošības nodrošināšanā (atbilstoši informācijas drošības politikai) ir noteikti amata aprakstos, darba līgumos vai citos iekšējos tiesību aktos;
- Darbiniekiem, kurus pieņem pastāvīgā darbā, tiek noslēgta vienošanās par konfidencialitātes ievērošanu. Vienošanās ietver atbildības noteikumus par nepubliskojamas informācijas izpaušanu. Vienošanās pārkāpums var izsaukt IS pārziņa tiesības vērsties pret profesionālās darbības apdrošināšanu ar prasību par zaudējumu piedziņu;
- Parakstot darbu līgumu darbinieks tiek iepazīstināts ar informāciju, kas nosaka darbinieka atbildību par informācijas drošību;
- Par drošības incidentiem tiek nekavējoties ziņots IS pārziņa vadībai atbilstoši paredzētajai kārtībai;

[4] RSU Informācijas sistēmas elektronisko platformu drošības politika, 5.punkts
[5] RSU Informācijas sistēmas elektronisko platformu drošības politika, 6.punkts

- IS lietotājiem ir noteikta procedūra, kas reglamentē drošības nepilnību reģistrēšanu un ziņošanu drošības pārvaldniekam;
- Darbinieki, kuri pārkāpj vai neievēro informācijas drošības politikas vai procedūras, tiek sodīti atbilstoši ārējiem normatīvajiem aktiem un RSU iekšējai darba kārtībai;
- Visiem IS lietotājiem tiek izmantoti unikāli identifikatori, kas piešķirti tikai viņiem personīgi, lai katra lietotāja aktivitātes varētu tikt viennozīmīgi identificētas un būtu izsekojamas;
- Paroļu veidošana un nomaiņa ir tiek kontrolēta automātiski, izmantojot IS iebūvētos līdzekļus;
- Vajadzības gadījumā datu autentiskuma un integritātes pārbaudē tiek izmantoti digitālie paraksti, atbilstoši esošajai kārtībai RSU;

Elektroniskā pasta (e-pasta) politika[6]

Elektroniskā pasta (e-pasta) politika nosaka galvenos nosacījumus attiecībā uz e-pasta autorizētu izmantošanu un drošības pasākumu ievērošanu. Šī politika ietver e-pasta sūtījumu saņemšanas un izsūtīšanas procedūras, kuras tiek veiktas izmantojot serveru, darba staciju vai mobilo iekārtu tehniskos resursus, kuri atrodas RSU rīcībā.

1. Darbinieku pienākumi

Visiem Rīgas Stradiņa universitātes darbiniekiem ir pienākums aktivizēt lietotāju kontus RSU e-pasta sistēmā un pārbaudīt savus universitātes e-pasta kontus vismaz vienu reizi dienā, ja darbinieks neatrodas atvaļinājumā, komandējumā vai jebkādā citā attaisnotā prombūtnē no savas darba vietas. Ja objektīvu un pamatotu apsvērumu dēļ darbiniekam nav iespēju pārbaudīt savu universitātes e-pasta kontu vismaz vienu reizi dienā, darbiniekam ir pienākums minēto e-pasta kontu pārbaudīt tiklīdz šāda iespēja ir radusies.RSU e-pasta sistēmā var nereģistrēties RSU Saimnieciskā atbalsta nodaļas vadītāja vai RSU Tehniskā servisa nodrošinājuma nodaļas vadītāja norādītie attiecīgās nodaļas tehniskā un saimnieciskā personāla pārstāvji, kā arī RSU akadēmisko struktūrvienību vadītāju norādītie attiecīgās akadēmiskās struktūrvienības mācību palīgpersonāla, tehniskā un saimnieciskā personāla pārstāvji.

2. Īpašuma tiesības

Visi e-pasta sūtījumi un pati sistēma kopumā, ieskaitot visus nosūtītos e-pasta vienumus, un citādi izmantotos e-pasta vienumus, kā arī e-pasta vienumu rezerves kopijas ir RSU īpašums.

3. Uzraudzība

Autorizētās personas ir atbildīgas par e-pasta sistēmas darbības uzraudzību, lai nodrošinātu e-pasta sistēmas pieejamību un nepārtrauktību. Lai nodrošinātu sistēmas drošību, problēmu novēršanu, un nepieciešamības gadījumā veiktu noteiktas izmeklēšanas procedūras, RSU ir tiesības veikt e-pasta sūtījumu uzraudzību un pārbaudi bez iepriekšēja brīdinājuma.

[6] RSU Informācijas sistēmas elektronisko platformu drošības politika, 7.punkts

4. Atbildība

Darbinieku atbildībā ietilpst e-pasta pieejas paroļu glabāšana un to informācijas neizpaušanas nodrošināšana trešajām pusēm. Gadījumos, kad ir nepieciešams nosūtīt ierobežotas pieejamības informāciju ārpus organizācijas, darbiniekam ir jāsaņem rakstisks apliecinājums no informācijas drošības pārvaldnieka. E-pasta politikas pārkāpšanas gadījumā pret darbinieku var tikt vērstas sankcijas, piemēram.: disciplinārlieta vai aizliegums izmantot e-pastu.

5. Ētiska uzvedība un atbildīga izmantošana

Personālam e-pasts ir jāizmanto tikai darba vajadzībām un organizācijas funkciju izpildes nodrošināšanai. Zemāk ir minēti piemēri atbildīgai un bezatbildīgai e-pasta sistēmas izmantošanai:

1. Ētiska un atbilstoša izmantošana:

1.1. Komunikācija izmantojot e-pastu tiek veikta balstoties uz darba pienākumiem un atbilstoši noteiktajām darba funkcijām;

1.2. Atbildi uz saņemto dienesta e-pasta sūtījumu nosūtot ne vēlāk kā 24 stundu laikā (neskaitot brīvdienas un svētku dienas) no vēstules saņemšanas. Izņēmums no šā punkta pieļaujams, ja no e-pasta sūtījuma satura izriet, ka atbilde uz to nav nepieciešama;

1.3. Aizpildot aili „Temats" („Subject"), pēc iespējas precīzi un īsi atspoguļojot e-pasta vēstules saturu;

1.4. Respektējot savu un e-pasta vēstules saņēmēja (saņēmēju) laiku – sūtot e-pasta vēstules tikai tad, kad nosūtīšana ir nepieciešama;

1.5. Gadījumos, kad e-pasts tiek izmantots, lai nosūtītu informāciju par jaunākajām normatīvo aktu prasībām, procedūrām, procesiem vai citiem iekšējiem dokumentiem;

1.6. Gadījumos, kad tiem nosūtīti paziņojumi personālam par noteiktiem pasākumiem – apmācībām, jubilejām u.tml.;

1.7. Respektējot visu trešo personu īpašumtiesību un licenču turētāju tiesības;

1.8. Nodrošinot nevajadzīgo un veco e-pasta sūtījumu izdzēšanu;

1.9. Ievērojot tādu pašu respekta līmeni, kā veicot komunikāciju verbālā formā;

1.10. Veicot gramatikas pārbaudi un kļūdu novēršanu pirms e-pasta sūtījuma nosūtīšanas;

1.11. E-pasta sūtījuma nobeigumā norādot vismaz sūtītāja vārdu un uzvārdu, amatu un dienesta tālruņa numuru;

1.12. Komandējuma, atvaļinājuma vai cita veida ilgstošas prombūtnes gadījumā e-pasta kontā ievietojot automātisko atbildes vēstījumu, norādot:

- no kura līdz kuram datumam darbinieks nebūs pieejams;
- aizvietotāju (vārds, uzvārds, e-pasts un telefons), kurš darbinieka prombūtnes laikā atbild par viņa kompetences jautājumiem.

2. Neētiska un neatbilstoša izmantošana:

2.1. Pārkāpjot noteiktus organizācijas iekšējos noteikumus (ieskaitot jebkāda veida apvainošanu, rasismu vai cita veida diskriminācijas);

2.2. Nosūtot informāciju, kas ietver neprecīzu vai apmelojošu informāciju, ieskaitot pornogrāfiskus, rasistiskus un personas aizskarošus materiālus;

2.3. Nosūtot noteiktas personas privāto informāciju, vai pārkāpjot citu personu tiesības uz brīvību, neatļauti izmantojot informāciju par šo personu, kas atrodas organizācijas rīcībā;

2.4. Izmantojot e-pastu noteiktu privāto darbību veikšanai, ar mērķi gūt individuālu labumu;

2.5. Nosūtot izklaidējošu un citu ar darba pienākumu izpildi nesaistītu informāciju;

2.6. Iekļaujot ikdienas lietišķajā sarakstē lieku elementus – krāsainus e-pasta vēstuļu fonus, nevajadzīgus skaistuma elementus, liekus rotājumus un tmldz.,

2.7. Pievienojot e-pasta sūtījumiem, kādu ļaunprātīgu programmnodrošinājumu ;

2.8. Nosūtot reklāmas vai spam sūtījumus.

„RSU IS autorizācijas paroļu sarežģītības noteikumi".[7]

Lietotāji paši ir atbildīgi par savu paroļu drošu glabāšanu.

Darbiniekam saņemot jaunu lietotājvārdu un paroli, pirmo reizi autorizējoties sistēmās, parole ir jānomaina.

Par paroli jāizvēlas pietiekami sarežģītu simbolu kombināciju. Paroles garumam jābūt vismaz 8 (astoņiem) simboliem un ne vairāk kā 16 (sešpadsmit) simboliem.

Parole ir jāmaina ne retāk kā katras 192 dienas, kā arī jaunā parole nedrīkst būt vienāda ar 24 iepriekšējām parolēm.

Pie nepareizas paroles ievadīšanas 5 reizes, lietotājvārda un paroles pāris tiek izslēgts (*lockout*) no sistēmas uz 30 minūtēm, lietotājs par to nekavējoties ziņo RSU IS administratoram vai sistēmas pārvaldniekam.

Lietotājam ir aizliegts izpaust jebkuru piešķirto paroli, kā arī citu konfidenciālu informāciju, kas saistīta ar RSU IS izmantošanu. Par katru darbību, kas veikta datoru tīklā, datu bāzēs, kā arī citās informatīvās sistēmās, ir atbildīgs izmantotā lietotāja vārda un paroles īpašnieks.

Ja lietotājs konstatē, ka kāds cits ir izmantojis viņa tiesības, lietotājs par to nekavējoties ziņo RSU IS administratoram vai sistēmas pārvaldniekam.

[7] RSU Informācijas sistēmas elektronisko platformu drošības politika, 1.pielikums

Lietotāju paroles uz serveriem var glabāt tikai šifrētā veidā.