Asutuse andmesüsteemi turvareeglid

Üldsätted

1. Käesoleva eeskirjaga sätestatakse käitumisreeglid x-firma (edaspidi Ettevõtte) infosüsteemide ja IT-vahendite kasutamisel.
2. Asutuse andmesüsteemi turvareeglid on kohustuslikud kõikidele Ettevõtte töötajatele ja teistele isikutele, kes soovivad kasutada Ettevõtte IT vahendeid. Reeglid kehtivad ühtmoodi nii tavakasutajatele, juhtkonnale kui ka IT-personalile.
3. Tööandja ressursse (arvutid, telefonid, nutiseadmed, võrk ja välisühendus, tööaeg) kasutatakse üldjuhul töötegemiseks. Nimetatud ressursse on lubatud kasutada ka isiklikuks otstarbeks ulatuses, mis ei sega tööülesannete täitmist ning on kooskõlas käesoleva eeskirjaga ning muude kehtivate regulatsioonidega.
4. Tööalast informatsiooni kasutades ja säilitades peab töötaja lähtuma minimaalsuse ja eesmärgipärasuse põhimõtetest. Informatsiooni levitamisel tuleb arvestada sellele seatud ligipääsupiirangutega.

Arvutikasutaja õigused ja kohustused

5. Vastutus riistvara ja andmekandjate füüsilise julgeoleku eest lasub eelkõige selle vahetul kasutajal.
    1. Avalikus kohas ei tohi jätta sülearvutit, telefoni või nutiseadet järelvalveta.
    2. Mobiiltelefoni, muud nutiseadet või andmekandjat on keelatud anda kolmandatele isikutele, välja arvatud otsesest töökorraldusprotsessist tingitud juhtudel.
    3. Seadme kadumisest või vargusest tuleb viivitamatult teavitada turvajuhti.
    4. Konfidentsiaalsed ja asutusesiseseks kasutamiseks mõeldud andmed, mis lahkuvad mõnel andmekandjal asutuse ruumidest, peavad olema krüpteeritud.
    5. Sülearvutite kõvakettad peavad olema krüpteeritud.
6. Vastutus informatsiooni säilimise, tervikluse ning konfidentsiaalsuse eest lasub eelkõige selle vahetul kasutajal.
    1. Eelistatud koht informatsiooni säilitamiseks on kontori failiserver. Serveris olevate andmete säilimise tehniliste probleemide korral ja varundamise korraldab IT Haldusosakond.
    2. Sülearvutites ja irdkandjatel peaks hoidma minimaalse hulga asutusesiseseks kasutuseks mõeldud või konfidentsiaalseid andmeid. Laua- ja sülearvutites ning irdkandjatel asuva informatsiooni säilimise ja

konfidentsiaalsuse peab kasutaja tagama iseseisvalt, sh korraldama andmete varundamise.

3. Andmete transpordiks kasutatavad irdkandjad tuleb pärast kasutamist tühjendada või hävitada.
4. Andmete sünkroniseerimiseks seadmete vahel tuleb kasutada lahendusi, kus sünkroniseeritavad seadmed suhtlevad omavahel ilma kolmandate osapoolte (nt Google, Apple või Microsofti pilveteenus) vahenduseta.
5. Asutusesiseseks kasutamiseks või konfidentsiaalseid andmeid ei ole lubatud kopeerida seadmetesse, mis ei vasta käesoleva korra p. 14 ja 15 nõuetele.

7. Arvutikasutajal on õigus kasutada vaid litsentseeritud tarkvara ning andmeid. Tööks vajaliku tarkvara ning andmete litsentside hankimine ning arvestuse pidamine on IT haldusosakonna ülesanne. Litsentseerimata sisu hoidmine ja kasutamine on keelatud ka tööandjale kuuluvates seadmetes isiklikuks otstarbeks ning isiklikes seadmetes, mida kasutatakse tööülesannete täitmisel.
8. Arvutikasutajal on õigus ja kohustus arvutiga töötamisel esinevate tõrgete korral pöörduda IT Haldusosakonna töötaja poole abi saamiseks.
9. Arvutikasutajad on kohustatud võimalikest ja toimunud turvaintsidentidest viivitamatult teavitama turvajuhti.
10. Tööandja teeb oma parima, et austada töötajate privaatsust ning isiklike sõnumite või muu isikliku info puutumatust. Töötaja omalt poolt peab arvestama, et isiklike seadmete, info, failide ning meili-, kiirsuhtlus-, sotsiaalvõrgustiku või muude kontode kasutamist tööandja riistvaral või võrguressurssidel võidakse tööandja poolt nii üldise turvapoliitika raames kui ka rutiinsete IT-hooldustööde käigus monitoorida, kopeerida ning kas valikuliselt või täielikult tõkestada. Arvutikasutajal on kohustus võimaldada IT Haldusosakonna töötajale ligipääs enda kasutuses olevatele seadmetele eesmärgiga kontrollida nende seadmete ja seadistuste vastavus kehtivatele kordadele.
11. Asutuse sisevõrku tuleb kasutada moel, mis ei kahjusta teiste võrgu kasutajate huve:
    1. Kasutaja teeb kõik endast oleneva, et vältida pahavara levikut Ettevõtte sisevõrgus. Sellekohased soovitused leiab aadressilt www.arvutikaitse.ee. Pahavara avastamisel või kahtluse korral on arvutikasutajal on kohustus viivitamatult eraldada arvuti kõikidest andmesidevõrkudest ning teavitada leiust IT Haldusosakonna töötajaid ja turvajuhti, kellelt saab ka juhised edasiseks käitumiseks. Saadavad juhised on täitmiseks kohustuslikud.
    2. Keelatud on võrgu risustamine ebasobiva sisuga;
    3. keelatud on võrgu (sh välisühenduste) ülekoormamine või muul moel teistele kasutajatele teenuste tõkestamine;
    4. keelatud on kasutada kohtvõrku litsentseerimata sisu allalaadimiseks või hoiustamiseks;

5. keelatud on võrgust välja saata sõnumeid või infot, mis võivad tekitada tööandjale varalist või mainekahju;
6. keelatud on turvatestid ja võrguliikluse jälgimine ilma eelneva turvajuhi kooskõlastuseta.

12. E-posti, Skype ja muude sidevahenditega ei ole üldjuhul lubatud teha järgmist laadi toiminguid:
    1. Rämpsposti, reklaamide saatmine isikutele, kes ei ole seda palunud
    2. E-kirjade päiste, sotsiaalvõrgustike või kiirsuhtlusvahendite kasutajanimede võltsimine
    3. Avalikesse sisututesse diskussioonidesse laskumine moel, mis võimaldab töötajat seostada Ettevõttega ning tema seisukohti pidada Ettevõtte omadeks.
    4. Ettevõtte kontodele suunatud kirjade edasisuunamine isiklikele kontodele, samuti kiirsuhtlusvahendite kontode kasutamise arvutites, mis ei vasta punktide 14 ja 15 nõuetele.

Ligipääs infosüsteemidele

13. Juurdepääsuks asutuse andme- ja võrguressurssidele ning IT-teenustele (e-post, ärirakendused jms) tuleb kasutajal end identifitseerida. Kasutajaid identifitseeritakse infosüsteemides kasutajatunnuse või isikukoodi alusel. Kasutajatunnus on tavapäraselt kasutaja eesnimi, kattuvate nimede korral mõni muu sobiv nimi. Kasutajatunnused on ühekordseks kasutamiseks ning töösuhte lõppemisel konto suletakse, ent ei kustutata. Isikukoodi alusel tuvastatakse kasutajaid nendes süsteemides, kuhu toimub meldimine ID-kaardiga.
14. Kõigil töötajatel ning vastava lepingu alusel ka partnerite töötajatel on õigus kasutada kaugtöö vahendeid kontoris paiknevatele ressurssidele ligipääsuks järgmistel tingimustel:
    1. Arvutisse peab olema paigaldatud ajakohane tunnustatud viirusetõrje tarkvara ning see peab olema ühenduses keskse viirusetõrje haldusjaamaga;
    2. Arvuti kõvaketas peab olema krüpteeritud;
    3. Arvuti kuulub tööandjale või ligipääsu taotlevale isikule.
15. Töötajatel on õigus kasutada tööülesannete täitmiseks ka oma isiklikke mobiiltelefone või teisi nutiseadmeid. Nii isiklikele kui tööandja poolt kasutada antud mobiilsetele seadmetele kehtivad järgmised nõuded:
    1. Seadmel peab olema parooliga kaitstud ekraanilukk, mis rakendub automaatselt, kui seadet pole 5 minuti jooksul kasutatud. Peale 10. järjestikku valesti sisestatud parooli käivitatakse automaatselt seadme mälu kustutamise protseduur.
    2. Seadmele peab regulaarselt paigaldama seadme või operatsioonisüsteemi tootja poolt väljastatud tarkvara turvauuendusi.

3. Uusi rakendusi, sealhulgas personaalseks kasutuseks mõelduid, on lubatud paigaldada ainult usaldusväärsetest allikatest (näiteks seadme tootja enda tarkvaravaramust).

4. Andmevahetuseks on eelistatuim viis mobiilsideoperaatori andmeside teenus. WiFi võrke, eriti avalikke, on lubatud kasutada ainult äärmise vajaduse korral.

5. Seadme WiFi, Bluetooth ja infrapunaliidesed on soovitav välja lülitatda, kui neid parasjagu ei kasutata.

16. Punktide 14 ja 15 nõuetele mittevastavad arvutid tuleb ühendada külalistele ette nähtud võrku. IT haldusosakonnal on õigus ja kohustus rakendada tehnilisi piiranguid nõuetele mittevastavate seadmete kohtvõrguga liitumise takistamiseks.

Paroolipoliitika

17. Iga arvutikasutaja valib endale ligipääsuks vajaliku(d) parooli(d) iseseisvalt. Parool peab olema vähemalt 12 tähemärki pikk. Märkide valikul tuleb silmas pidada, et kõik märgid ei pruugi igas keskkonnas (näiteks US paigutusega klaviatuuril või RDP/VNC protokolliga kaugtöölauda kasutades) ühtviisi kättesaadavad olla. Arvutikasutajal on soovitatav kasutada erinevates süsteemides erinevaid paroole, kui tehnilised vahendid seda lubavad. Mobiiltelefoni käivitamiseks ja ekraaniluku avamiseks kasutatav PIN-kood peab olema vähemalt 4 numbrit.

18. Arvutikasutajal on keelatud oma isikliku konto parooli kellelegi avaldada.

19. Arvutikasutajal on kohustus töökohalt eemal viibides kasutada parooli või muu ligipääsupiiranguga kaitstud ekraanisäästjat. Sülearvutitel ja muudel kaasaskantavatel seadmetel peab olema ligipääsupiirang ka uinunud olekus.

20. Arvutikasutajal on kohustus muuta enda valduses olevaid paroole vähemalt üks kord aastas. Juhul, kui muudetav parool on kuhugi talletatud ühiskasutuseks, tuleb ka kõik vastavad koopiad värskendada.

21. Arvutikasutaja on kohustatud talletama Ettevõttele kuuluvate arvutite peakasutaja (root või administrator) parooli, BIOS parooli ning muud võimalikud arvuti käivitumist takistavad paroolid kinnises ümbrikus ITH administraatori seifis – vajalik on minimaalne kogus infot, et arvuti rikke korral või töötajaga kontakti puudumisel oleks Ettevõttele tagatud ligipääs arvutis olevatele andmetele. Mobiiltelefonide PIN-koode täiendavalt hoiustama ei pea.

22. Punktides 17, 20 ja 21 nõuded ei ole kohustuslikud keskkondades, mis on loetletud Lisas 1.

Blogimine, foorumites ja sotsiaalvõrgustikes osalemine

23. Blogimisel, foorumites ja sotsiaalvõrgustikes osalemisel peab Ettevõtte töötaja olema viisakas ja vastutustundlik, hoiduma vastuoludest seaduste, kehtivate kordade ja Ettevõtte huvidega. Blogimist, foorumites ja sotsiaalvõrgustikes osalemist Ettevõtte sisevõrgust võidakse sarnaselt muu võrguliiklusega vajadusel monitoorida.

24. Blogides ja kommentaarides ei ole lubatud esineda ebaviisakate, solvavate ega diskrimineerivate seisukohtadega, samuti esitada autoriõiguste valdaja loata või ligipääsupiiranguga kaitstud materjali. Kogu vastutus sõnavõttude sisu eest langeb töötajale.

25. Blogides ja kommentaarides peavad isiklikud seisukohad olema selgelt esitatud isiklikena, mitte ettevõtte omadena. Ettevõtte seisukohti on lubatud esitada vaid vastavate kokkulepete alusel.

26. Keelatud on blogimine, kommenteerimine või sotsiaalvõrgustikes osalemine võõra nime all või võõrast kontot kasutades.

Rakendussätted

27. Andmesüsteemi turvareeglite kaasajastamise ning täitmise kontrolli eest vastutab turvajuht.

28. Ettevõtte tagab töötajale võimaluse igal ajal tutvuda eeskirjaga, mille üks eksemplar asub sekretäri juures; elektrooniliselt on dokument kättesaadav kõigile Ettevõtte töötajatele sisemise arvutivõrgu vahendusel dokumendi päises määratud aadressil.

29. Ettevõtte-sse tööleasumisel või reeglite jõustumisel võetakse Ettevõtte töötajalt ja Ettevõtte vahenditega tööd tegevatelt partneritelt allkiri, millega kinnitatakse turvareeglitega tutvumist ja kohustust neid järgida.