Kinnitanud: Aivo Aasa 04.08.2008a
AS Sivex International Pärnu kontor

ARVUTIKASUTAJA REEGLISTIK

I. Eesmärk

Käesolev arvutikasutaja eeskiri on osa AS Sivex International (edaspidi "ettevõtte") kvaliteetjuhtimissüsteemist ja infoturbe korraldusest. Arvutikasutaja reeglistik kehtestab elementaarsed sätted, mis aitavad vähendada ettevõtte infosüsteemi halduskulusid ning tõhustavad selle turvalisust ja efektiivsust.

Antud reeglistiku eesmärgiks on tekitada organisatsioonisisene turvateadlikkus ning saavutada infosüsteemi kasutajate individuaalset vastutust ja aktiivset osalust turvalisuse tagamisel.

II. Üldsätted

1. Ettevõtte infosüsteem – ettevõtte mitteavalik teave, arvutid ja nendega seonduvad tarkvara ning seadmed ja selle komponendid ning ressursid (kaasa arvatud Interneti ühendus) – on ettevõtte omand, mille kasutamisel tuleb alati lähtuda eelkõige ettevõtte huvidest.
2. Ettevõtte infosüsteemi kasutamisel tuleb juhinduda:
   - ettevõtte tegutsemise eesmärkidest, mis on määratud ettevõtte põhikirjaga;
   - antud reeglistikust;
   - headest tavadest.
3. Antud reeglistik sätestab infosüsteemi kasutajate õigused ning kohustused.
4. Antud reeglistik kehtib kõigis ettevõtte infosüsteemi lülitatud arvutisüsteemides (k.a. kaasaskantavates arvutites).
5. Ettevõtte infosüsteemi ning sellega seonduvate ruumide haldajad võivad ülaltoodud põhimõtetest ja seadmete sihtotstarbest lähtuvalt kehtestada täiendavaid reegleid, mis ei vähenda käesoleva reeglistiku nõudeid.
6. Kui ettevõtte infosüsteemi erinevad kasutusviisid satuvad konflikti, mille lahendamisel ei saa ühtselt lähtuda antud reeglistikust ega täiendavatest reeglistikest, tuleb lähtuda järgnevatest prioriteetidest:
   - ettevõtte põhitegevusega seotud tegevused;
   - muud ettevõtte tegevuse eesmärkidega otseselt seotud tegevused;
   - ettevõtte tegevuse eesmärkidega kaudselt seotud tegevused;
   - muud tegevused, mis ei häiri teiste infosüsteemi tööd.
7. Ettevõtte infosüsteemi haldajaks on ettevõtte juhtkond, mis kontrollib ka infosüsteemi hooldust kolmandate osapoolte poolt.
8. Infosüsteemi turvalisuse tagamise eest vastutab ettevõtte juht, kelle poolt määratud kontaktisikule tuleb teavitada kõikidest turvaintsidentidest.
9. Infosüsteemi kasutamise ja turvalisusega seonduvate intsidentide puhul tuleb pöörduda ettevõtte tugipersonali poole telefonil: 50 10 535(Taro Võsu), 4459932 (Urmas Reinart) 5096261(Aivo Aasa).

III. Kasutaja kohustused

1. Kasutaja on kohustatud täitma oma rolli infosüsteemi turvalisuse tagamiseks. Selleks peab ta:
   - hoidma saladuses kasutusõigusi tagavaid paroole vastavalt ettevõtte paroolide haldamise korrale; (vt. VIII ptk.)
   - mitte võimaldama või lubama teistel isikutel kasutada oma kasutajaõigusi;

- vältima oma valduses olevate andmete ja informatsiooni lekkimist kõrvalistele isikutele;
- teavitama vastutavat personali kõikidest infosüsteemi tõrgetest ja turvaintsidentidest.

2. Kasutajad on kohustatud järgima infosüsteemi haldajate poolt kehtestatud piiranguid ja täitma haldajate poolt tehtud korraldusi.
3. Keelatud on kasutada teistele isikutele omistatud kasutajaõigusi (näiteks e-maili või kasutajakontot).
4. Keelatud on infosüsteemi tööd häiriv tegevus, mis häirib selle tööd või kasutust haldaja poolt määratud otstarbel või segab teisi kasutajaid nii otseselt kui ka kaudselt (näiteks ressursside tahtliku raiskamise teel või e-maili masspostitusega selleks konkreetset soovi mitte avaldanud isikutele).
5. Ettevõtte infosüsteemi ja selle kasutusõigust ei tohi kasutada isikliku või muu tulu saamise eesmärgil, mis ei lähtu ettevõtte põhikirjalisest tegevusest. Ettevõtte infosüsteemi maksuliseks kasutamiseks sõlmitakse vajadusel eraldi leping.
6. Arvutivõrku ühendatud arvutites on rangelt keelatud hoida, kasutada ja ettevõtte arvutivõrgus levitada:
   - illegaalselt omandatud või litsentseerimata tarkvara;
   - autorikaitse alla kuuluvat tarkvara või andmefaile vms. millede kohta ei ole ostutõendit;
   - sündsusetu sisuga faile.
7. Rangelt on keelatud mistahes tarkvara (litsentseeritud või litsentseerimata) omavoliline paigaldamine ettevõtte arvutitesse ja/või arvutivõrku.
8. Keelatud on infosüsteemi võimalike turvaaukude kasutamine täiendavate juurdepääsuõiguste ja privileegide saamiseks.
9. Kasutajal on kohustus turvaaukudest teadlikuks saamisel koheselt teavitada ettevõtte tugipersonali.
10. Keelatud on arvutite või seadmete omavoliline ühendamine arvutivõrku, nende ümberühendamine ja nendele mistahes perifeeriaseadmete ühendamine. Mistahes isikliku riistvara paigaldamine peab olema kooskõlastatud infosüsteemi haldajatega.
11. Kasutaja on kohustatud kontrollima enda poolt ettevõtte ruumidesse toodava tarkvara/andmefaile viirustõrje programmiga.
12. Kasutajale on rangelt keelatud peatada haldaja poolt paigaldatud viirusetõrje programmi.
13. Kõik kahtlused mis on seotud arvuti võimaliku nakatumisega viirustega peavad olema koheselt edastatud tugipersonalile.
14. Iga kasutaja vastutab isiklikult oma arvutis ja andmekandjatel olevate failide olemasolu eest ja töölised kellel on juurdepääs ettevõtte serverile vastutavad nende andmete säilimise eest.

IV. Kasutaja õigused

1. Kasutajaõiguse saanud isikutel on õigus kasutada infosüsteemi vastavalt antud reeglistikule tööalasel eesmärgil igal ajal, kui see ei ole vastuolus muude kehtestatud reeglitega.
2. Kasutajal on õigus saada teenindajatelt informatsiooni kõigist muudatustest ja sündmustest, mis mõjutavad oluliselt selle kasutamist või kasutajate privaatsust.
3. Kasutajal on õigus teha ettepanekuid ettevõtte infosüsteemi töö, teenuste ja halduse parema korraldamise osas.
4. Kasutajal on õigus infosüsteemi häiretest teatada selle teenindajatele.
5. Kui kasutajal on pretensioone infosüsteemi teenindajate suhtes, siis on kasutajal õigus need esitada ettevõtte juhtkonnale.

V. Infosüsteemi haldajate kohustused

1. Haldajate primaarseteks kohustusteks on tagada ning jälgida infosüsteemi turvalisust, ettenähtud toimimist ja teenuste kättesaadavust kasutajatele.
2. Haldajad peavad tegema kasutajatele kättesaadavaks infosüsteemi kasutamise vastavad juhised.
3. Haldajad on kohustatud kasutajatele andma eelteavet olulistest muudatustest infosüsteemis. Samuti on haldajad kohustatud teavitama sündmustest, mis võivad mõjutada kasutajate privaatsust.
4. Haldajad on kohustatud saladuses pidama oma töökohustuste täitmise käigus neile avalikuks saanud andmeid, mille kohta neil puudub andmete omaniku luba seda edasi anda, v.a. juhud, kui seadus kohustab informatsiooni teatavaks tegema. Antud reeglistiku rikkumisi puudutav informatsioon kuulub teatavaks tegemisele rikkumisi arutama volitatud isikutele.
5. Haldajad on vastavalt korraldustele kohustatud rutiinselt teostama andmebaaside ja failiressursside turvakopeerimist.
6. Rikkumise tuvastamisel on haldaja kohustatud koostama vastavasisulise aruande.

VI. Infosüsteemi haldajate õigused

1. Haldajatel on oma kohustuste täitmiseks õigus ajutiselt piirata infosüsteemi kasutamist nii, et see võimalikult vähe häiriks infosüsteemi ja selle kasutajate tööd. Kõigist sellistest piirangutest on infosüsteemi haldajad kohustatud kasutajaid adekvaatselt teavitama (näiteks kasutaja ekraanile tekkiva eelneva hoiatussõnumiga).
2. Infosüsteemi häireolukorra kiireks selgitamiseks või kõrvaldamiseks on infosüsteemi haldajatel õigus lugeda/kustutada kasutajate faile. Niimoodi saadav info ei kuulu levitamisele v.a. juhud, kui seadus kohustab informatsiooni teatavaks tegema.
3. Haldajatel on õigus teostada auditit paroolide haldamise korra järgimise osas (näiteks paroolide murdmine). HOIATUS: tavalistele arvutikasutajatele on selline tegevus rangelt keelatud!
4. Haldajatel on õigus rakendada koheselt sanktsioone arvutikasutaja reeglite rikkumiste ilmnemisel või informatsiooni lekkimise vältimiseks (piirata kasutajaõigusi, eemaldada omavoliliselt installeeritud programme, kustutada sündsusetuid või piraatlusega seonduvaid ning ressursse raiskavaid (*.avi, *.mp3) faile).

VII. Kasutusõiguse saamise kord

1. Ettevõtte infosüsteemi kasutusõigus antakse kasutajakonto väljastamisega tema tööle asumisel otsese ülemuse või tugiisiku poolt:
   - ettevõtte töötajatele;
   - ettevõtte ajutistele töötajatele vastava allüksuse taotluse alusel;
   - ettevõttele IT teenuseid osutavatele isikutele, kes vajavad selleks kasutusõigust;
   - erandkorras võib anda kasutusõiguse teistele isikutele, kui esitatakse põhjendatud taotlus organisatsiooni poolt, millega see isik on seotud.
2. Ettevõtte töötajate kasutusõigust kehtib reeglina nende ettevõttes töötamise aja jooksul. Ajutistele kasutajatele ja lepingulistele hooldusisikutele antakse üldjuhul tähtajaline kasutusõigus, reeglina mitte pikemaks ajaks kui üks aasta.
3. Kasutusõigus on personaalne ja seda pole lubatud ühelt isikult teisele edasi anda (unikaalne kasutajatunnus identifitseerib kasutajat ja kõiki tema tegevusi, mida võetakse aluseks ka rikkumiste jälgimisel).
4. Iga kasutaja peab esmasel kasutusõiguse väljastamisel oma allkirjaga kinnitama, et on tutvunud ettevõtte arvutikasutaja reeglistikuga ning kohustub järgima neis kehtestatud nõudeid.

5. Kasutusõiguse saamisel omistatakse taotlejale kasutajakonto(d) unikaalse kasutajanime ja esmase parooliga. Esmane parool tuleb kasutajal endal vahetada koheselt peale esimest infosüsteemi sisenemist vastavalt ettevõtte paroolide haldamise korrale (vaata peatükk VIII, Paroolide Haldamine).
6. Koos kasutajaõigustega omistatakse kasutajale (vajadusel) ka tema e-posti aadress.
7. Kasutajaõigusi ei väljastata ega muudeta ilma kasutaja ülemuse või sponsori kirjaliku kinnituseta.

VIII. Paroolide haldamine

Paroolide koostamise nõuded:

1.Parool peab:

- olema vähemalt 8 kirjamärki pikk;
- sisaldama vähemalt üht igast märgitüübist: **väike täht, suur täht, number, erimärk** (näiteks&?,!).

2. Parool ei tohi:

- olla liiga äraarvatav (sarnaneda sõnaraamatu sõnaga, olla kasutaja lemmikfraas, jne.)
- sisaldada kasutajanime või kasutaja isikuga seonduvat informatsiooni (ära kasuta parooli koostamisel oma enda, sugulaste või näiteks lemmiklooma nime, mõnda olulist kuupäeva, auto registrinumbrit, isikukoodi, lemmikfraasi vms.)
- sisaldada rohkem kui kahte järjestikust sama kirjamärki
- sarnaneda varemkasutatud paroolide või teistele kasutaja paroolidele (rangelt on keelatud isiklikke paroole kasutada tööga seotud paroolidena).

Paroolide hoidmise nõuded:

1. Paroole tuleb hoida konfidentsiaalsena (talletada mällu, mitte paberile või faili)
2. Parooli ega viiteid selle sisule ei tohi anda teada teistele isikutele.
3. Kasutajaõigustega kaasnev esmane parool tuleb ära vahetada kohe peale selle esimest kasutamist infosüsteemi sisenemisel.
4. Kasutajad on kohustatud oma paroole vahetama perioodiliselt (iga 60 päeva tagant kui ei ole sätestatud teisiti) ning koheselt kui on tekkinud kahtlusi parooli või kasutusõiguste lekkimises teistele isikutele.

IX. Töökoha ja tööjaama (terminali) turvalisus

1. Kasutaja peab järgnevalt vältima tema kasutajakonto kasutamist teiste isikute poolt.
   - Töökohalt ajutiselt (näiteks kõrvalkabinetti või lõunale) lahkudes tuleb arvuti ALATI lukustada (vajuta klahvikombinatsiooni CTR+ALT+DEL ja seejärel "Lock computer";
   - Töökohalt pikemaks ajaks lahkudes tuleb arvutist välja logida.
2. Kasutaja on kohustatud vältima tema käsutuses olevaid olulist informatsiooni sisaldavate andmekandjate ja andmete sattumist kõrvaliste isikute kätte:
   - ei tohi jätta andmekandjaid (floppy, CD, ZIP, magnetlint jms.) kergesti nähtavate või ligipääsetavatesse kohtadesse või jätta neid arvuti vastavasse seadmesse.
   - Võimalusel on soovitav kasutaja eemalolekul hoida andmekandjaid lukustatavas sahtlis või kapis (see kehtib ka lukustatavate kabinettide puhul kui sellele omab normaalset juurdepääsu rohkem kui üks inimene)

X. Interneti kasutamine

1. Interneti kasutamine töö ajal on lubatud eelkõige ainult tööülesannete täitmiseks.

2. Ettevõtte juhtkonnal on õigus inspekteerida ja jälgida kõikvõimalikke Interneti ühendusi üldvõrgu kaudu ning suunata kogu liiklust läbi vastavate kontrollmehhanismide.
3. Salastatud ja konfidentsiaalse informatsiooni edastamine interneti kaudu krüpteerimata kujul on rangelt keelatud.
4. Keelatud on Interneti kasutamine isikliku tulu saamiseks, ebasündsaks käitumiseks, ebasündsate failide vaatamiseks või allalaadimiseks, Interneti ühenduse või ettevõtte arvutiressursside raiskamist põhjustades või muul moel, mis ei ole ettevõtte huvides.
5. Keelatud on internetist tundmatute failide käivitamine või allalaadimine (vältimaks nakatumist viirusega või rünnakut pahatahtliku tarkvara läbi)

XI. E-posti kasutamine

1. Kasutajale antud e-posti kasutusõigus ja e-posti aadress on ette nähtud tööülesannetega seotud kirjavahetuse jaoks.
2. Kasutaja ei tohi avalikustada ettevõtte e-posti aadresse kõrvalistele isikutele väljaspool selleks ettenähtud protseduure.
3. E-posti saatmisel tuleb erilist tähelepanu pöörata sellele, et kiri ei satuks valele aadressile.
4. Keelatud on avada e-postiga saadetud kahtlasi või tundmatuid faile tundmatutelt isikutelt. Kahtluse tekkimisel tuleb konsulteerida tugipersonaliga.
5. Keelatud on edastada e-posti vahendusel krüpteerimata konfidentsiaalset informatsiooni või muud eriti sensitiivset teavet (k.a. paroolid).
6. Keelatud on e-posti ressursseraiskav, ebaviisakas või sündsusetu kasutamine.

XII. Mobiilsed kasutajad

1. Kaasaskantava arvuti kasutamisele kehtivad samad miinimumreeglid nagu statsionaarsetele tööjaamadele.
2. Kõik reeglid kehtivad kaasaskantava arvuti kasutamisel nii ettevõttes kui ka ettevõttest väljaspool.
3. Et tegemist on mobiilse IT vahendiga, mida kasutatakse ka väljaspool ettevõtte infosüsteemi ja selle turvakeskkonda, siis kehtivad kaasaskantavale arvuti kasutamisele ka järgnevad lisareeglid:

3.1. Kaasaskantavat arvutit on rangelt keelatud jätta üldkäidavates kohtades ilma järelvalveta (k.a. pargitud sõiduautodes).
3.2. Kaasaskantaval arvutil ei tohi töödelda sensitiivseid andmeid avalikus kohas või kohtades, kus töödeldavaid andmeid võivad näha kõrvalised isikud.
3.3. Kaasaskantava arvuti kasutusvõimalust on keelatud edasi anda isikutele, kellel puudub selleks ettevõtte poolt antud spetsiaalne kasutusõigus koos vastava kasutajakontoga (k.a. kasutaja pereliikmetele).
3.4. Kaasaskantav arvuti peab olema lisaks kasutaja paroolile kaitstud ka haldaja poolt seatud BIOSi parooliga.
3.5. Kaasaskantaval arvutil asuvate oluliste failide tagavarakoopiate olemasolu eest ettevõtte failiserveris vastutab kaasakantava arvuti kasutaja ise. Teenindajad vastutavad ainult failiserveris olevate andmete turvakoopiate ja taastamise eest.
3.6. Kaasaskantava arvuti ühendamisel Internetti või mistahes võrku väljaspool ettevõtte sisevõrku tuleb kasutada personaalset tulemüüri, mis on konfigureeritud vastavalt ettevõtte nõuetele.
3.7. Vastavalt vajadusele võib ettevõte kehtestada kaasaskantava arvuti kõvaketta või selle osa krüpteerimise nõude spetsiaalse tarkvara abil (kehtib pideva sensitiivsete andmete töötlemise puhul).

XIII. Sanktsioonid

1. Antud reeglistiku mittetundmine ei vabasta rikkumistega kaasnevast vastutusest.
2. Antud reeglistiku rikkumise kahtluse korral võib ettevõtte juhtkond peatada kasutusõiguse kuni asjaolude väljaselgitamiseni.
3. Reeglite rikkumises kahtlustataval on õigus esitada omapoolne selgitus.
4. Antud reeglistiku rikkumist käsitletakse kui ettevõtte huvide otsest ja sihilikku kahjustamist.
5. Antud reeglistiku rikkumisel on ettevõtte juhtkonnal õigus rikkujat karistada distsiplinaarkorras.
6. Antud reeglite korduva või tahtliku rikkumise puhul võib ettevõtte juhtkond kitsendada kasutaja õigusi ettevõtte huvisid silmas pidades vastavalt oma äranägemisele.
7. Kasutajatelt, kes antud reeglistiku rikkumisega kahjustavad ettevõtte vara või tekitavad lisakulutusi (teenindajate lisatöö aeg, väljakutsed väljaspool põhitöö aega, vms.) võib ettevõte nõuda tekitatud kahju hüvitamist ettevõttele poolte kokkuleppel. Kokkuleppe mittesaavutamisel toimub kahju hüvituse sissenõudmine seadusega ettenähtud korras.