

		ISO 27002	ISKE
1		Skoop	ISKE rakendusjuhend ja kataloogid, Peatükk 1, BSI-Standard 100-2 Peatükk 1, Sissejuhatus
2		Terminid ja definitsioonid	ISKE rakendusjuhend, sõnastik
3		Standardi struktuur	ISKE rakendusjuhend ja kataloogid, Sissejuhatus
4		<b>Riskide kaalutlemine ja käsitus</b>	
	4,1	Turvariskide kaalutlemine	<b>M 2.195 Infoturbe kontseptsiooni koostamine</b>  BSI-Standard 100-2 peatükk 4.3 BSI-Standard 100-2 peatükk 4.6
	4,2	Turvariskide käsitus	<b>BSI-Standard 100-3 IT-etalonturbel põhinev riskianalüüs</b>  BSI-Standard 100-2 peatükk 4 M 2.339 Ressursside ökonomne kasutamine infoturbeks
5		<b>Turvapoliitika</b>	
	5,1	Infoturbepoliitika	
	5.1.1	Infoturbepoliitika dokument	<b>M 2.192 Infoturbepoliitika koostamine</b>  BSI-Standard 100-2, peatükk 3 I B 1.0 Infoturbe haldus M 2.335 Infoturbe eesmärkide ja strateegia kehtestamine
	5.1.2	Infoturbepoliitika läbivaatus	<b>BSI-Standard 100-2 peatükk 3.3.5 B 1.0 Infoturbe haldus</b> M 2.193 Infoturbeks sobiva organisatsioonilise struktuuri rajamine M 2.199 Infoturbe käigushoidmine M 2.200 Infoturbearuanded juhtkonnale ja hinnangud infoturbele
6		<b>Infoturbe korraldus</b>	
	6,1	Sisemine korraldus	<b>B 1.0 Infoturbe haldus</b>
	6.1.1	Juhtkonna kohustumus infoturbe alal	<b>BSI-Standard 100-2, peatükk 3.1</b>  B 1.0 Infoturbe haldus M 2.192 Infoturbepoliitika koostamine M 2.200 Infoturbearuanded juhtkonnale ja hinnangud infoturbele
	6.1.2	Infoturbe koordineerimine	<b>M 2.193 Infoturbeks sobiva organisatsioonilise struktuuri rajamine</b>

			BSI-Standard 100-2 peatükk 3 B 1.0 Infoturbe haldus B 1.13 Infoturbe teadlikkus ja - koolitus
6.1.3	Infoturbekohustuste jaotamine		<b>BSI-Standard 100-2, Peatükk 3.4.2</b> <b>M 2.193 Infoturbeks sobiva organisatsioonilise struktuuri rajamine</b> M 2.225 Teabe, rakenduste ja IT-komponentide alase vastutuste kinnitamine
6.1.4	Infotöötlusvahendite volitamise protsess		<b>B 1.9 Riist- ja tarkvara haldus</b> B 1.0 Infoturbe haldus M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld M 2.216 IT-komponentide kinnitamise protseduur
6.1.5	Konfidentsiaalsuslepped		<b>M 3.55 Konfidentsiaalsuslepingud</b> B 1.2 Personal M 2.226 Asutusevälise personali kasutamise protseduur M 3.2 Uute töötajate kohustamine eeskirju järgima
6.1.6	Kontakt ametivõimudega		<b>B 1.3 Hädaolukorraks valmisoleku kontseptsioon</b> <b>B 1.8 Turvaintsidentide käsitlemine</b> M 6.59 Turvaintsidentide käsitlemise eest vastutavate isikute määramine M 6.61 Turvaintsidentide käsitlemise laiendamisstrateegia M 6.65 Asjassepuutuvate isikute teavitamine turvaintsidentidest
6.1.7	Kontakt erihuvigruppidega		<b>M 2.35 Teabe hankimine turvaaukude kohta</b> M 2.199 Infoturbe käigushoidmine
6.1.8	Infoturbe sõltumatu läbivaatus		<b>M 2.199 Infoturbe käigushoidmine</b> BSI-Standard 100-2 Peatükk 6 B 1.0 Infoturbe haldus M 2.200 Infoturbearuanded juhtkonnale ja hinnangud infoturbele
6,2	Välised pooled		
6.2.1	Väliste pooltega kaasnevate riskide väljaselgitamine		<b>B 1.11 Väljastellimine</b> B 1.9 Riistvara ja tarkvara haldus B 4.4 Virtuaalne privaatvõrk (VPN) M 2.251 Väljastellimisprojektide turvanõuete spetsifitseerimine
6.2.2	Turvalisuse eest hoolitsemine klientidega tegelemine		<b>M 5.88 Leping andmevahetuse kohta kolmandate pooltega</b> M 5.87 Leping kolmandate poolte võrkudega ühendamise kohta
6.2.3	Turvalisuse eest		<b>B 1.11 Väljastellimine</b>

		hoolitsemine lepetes kolmanda poolega	M 5.87 Leping kolmandate poolte võrkudega ühendamise kohta M 5.88 Leping andmevahetuse kohta kolmandate pooltega
7		<b>Varade haldus</b>	
	7,1	Vastutus varade eest	
	7.1.1	Varade inventariloend	<b>BSI-Standard 100-2, peatükk 4.2</b> B 1.0 Infoturbe haldus B 1.1 Arhiveerimine M 2.139 Olemasoleva võrgukeskkonna läbivaatus M 2.195 Infoturbe kontseptsiooni koostamine M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus
	7.1.2	Varade omanikud	<b>M 2.225 Teabe, rakenduste ja IT-komponentide alaste vastutuste kinnistamine</b>
	7.1.3	Varade lubatav kasutamine	<b>M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus</b> M 1.33 Kaasaskantavate IT-süsteemide hoidmine reisil M 1.34 Kaasaskantavate IT-süsteemide hoidmine põhiasukohas M 2.455 Infoturbepoliitika kehtestamine rühmatarkvara jaoks M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid M 2.226 Asutusevälise personali kasutamise protseduurid M 2.235 Interneti-PC kasutamise suunised M 2.309 Mobiilse IT-kasutuse turvapoliitika ja eeskirjad M 5.88 Leping andmevahetuse kohta kolmandate pooltega
	7,2	Läbivaatuse lähteandmed	
	7.2.1	Liigitussuunised	<b>BSI-Standard 100-2, peatükk 4.3</b> B 1.0 Infoturbe haldus M 2.195 Infoturbe kontseptsiooni koostamine M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus
	7.2.2	Teabe märgistamine ja käitlus	<b>BSI-Standard 100-2, peatükk 4.3</b> B 1.0 Infoturbe haldus M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus
8		<b>Inimressursside turve</b>	
	8,1	Enne töösuhet	

8.1.1	Rollid ja kohustused	<b>M 2.1 Struktureeritud andmetalletus</b> B 1.1 Organisatsioon B 1.2 Personal M 2.5 Vastutuse ja ülesannete jaotamine M 2.193 Infoturbeks sobiva organisatsioonilise struktuuri rajamine M 2.198 Personali teadvustamine infoturbe küsimustes M 3.1 Uute töötajate esmane juhendamine ja väljaõpe M 3.26 Personali juhendamine IT-vahendite turvalise kasutamise alal
8.1.2	Taustakontroll	<b>M 3.33 Personali taustakontroll</b> B 1.2 Personal M 3.50 Personali valimine
8.1.3	Töölepingu sätted	<b>M 2.226 Asutusevälise personali kasutamise protseduurid</b> <b>M 3.2 Uute töötajate kohustamine eeskirju järgima</b> B 1.2 Personal M 3.1 Uute töötajate esmane juhendamine ja väljaõpe
8,2	Töösuhte ajal	
8.2.1	Juhtkonna kohustused	<b>M 2.198 Personali teadvustamine infoturbe küsimustes</b> B 1.13 Infoturbe teadlikkus ja -koolitus M 2.226 Asutusevälise personali kasutamise protseduurid M 3.5
8.2.2	Infoturbetaadlikkus, -haridus ja -koolitus	<b>B 1.13 Infoturbe teadlikkus ja -koolitus</b> M 2.312 Infoturbealase koolitus – ja teadvusetusprogrammi kavandamine M 3.5 IT-turvameetmete alane koolitus
8.2.3	Distsiplinaarprotsess	<b>M 2.39 Vastutus turvapoliitika rikkumise eest</b> B 1.8 Turvaintsidentide käsitlemine M 2.192 Infoturbepoliitika koostamine M 3.26 Personali juhendamine IT-vahendite turvalise kasutamise alal
8,3	Töösuhte lõpetamine või muutmine	
8.3.1	Lõpetamiskohustused	<b>M 3.6 Reguleeritud protseduur töösuhete lõpetamiseks</b> B 1.2 Personal M 2.226 Asutusevälise personali kasutamise protseduurid
8.3.2	Varade tagastamine	<b>M 3.6 Reguleeritud protseduur töösuhete</b>

			<b>lõpetamiseks</b> M 2.226 Asutusevälise personali kasutamise protseduur
	8.3.3	Pääsuõiguse äravõtmine	<b>M 3. 6 Reguleeritud protseduur töösuhte lõpetamiseks</b> M 2.30 kasutajate ja kasutajarühmade määramise protseduurid M 2.226 Asutusevälise personali kasutamise protseduurid
9		<b>Füüsiline ja keskkonnaturve</b>	
	9,1	Turvalised alad	
	9.1.1	Füüsiline turvameede	<b>M 1.55 Perimeetri kaitse</b> <b>M 2.17 Sisemised reeglid ja reguleerimine</b>  B 2.1 Hooned M 1.10 Turvauksed ja -aknad M 1.17 Pääsla M 1.19 Sissemurdmiskaitse M 1.50 Kaitse suitsu eest
	9.1.2	Füüsilise sissepääsu reguleerimise meetmed	<b>M 2.17 Sisenemise reeglid ja reguleerimine</b>  B 2.1 Hooned B 2.9 Arvutuskeskus M 1.49 Tehnilised ja organisatoorsed nõuded arvutuskeskusele M 1.58 Tehnilised ja organisatoorsed nõuded serveriruumidele M 2.6 Sissepääsuõiguste andmine
	9.1.3	Kabinettide, ruumide ja rajatiste turve	<b>Kataloogide alajaotus B2 infrastruktuur</b>  B 2.3 Bürooruum B 2.4 Serveriruum M 1.12 Kaitstavate hooneosade märgistamata jätmise M 1.13 kaitset vajavate ruumide paigutus M 1.15 Aknad ja uksed suletud M 1.18 valve- ja tuletõrjesignalisatsioon M 1.51 Tulekoormuse vähendamine M 1.58 Tehnilised ja organisatoorsed nõuded serveriruumidele
	9.1.4	Kaitse väliste ja keskkonnaohtude eest	<b>Kataloogide alajaotus B2 infrastruktuur</b> M 1.1 Vastavus normidele ja eeskirjadele M 1.6 Tuletõrje- eeskirjade täitmine M 1.13 Kaitset vajavate ruumide paigutus M 1.16 Hoone sobiv asukoht M 1.18 Valve – ja tuletõrjesignalisatsioon M 1.55 Perimeetri kaitse

9.1.5	Töötamine turvalistel aladel	<b>Kataloogide alajaotus B2 infrastruktuur</b> M 1.49 Tehnilised ja organisatoorsed nõuded arvutuskeskusele M 1.58 Tehnilised ja organisatoorsed nõuded serveriruumidele M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld M 2.16 Välipersonali ja küllastajate valve ja saatmine M 2.17 Sisenemise reeglid ja reguleerimine M 2.18 Kontrollringkäigud	
9.1.6	Avalikud juurdepääsu-, tarne- ja laadimisalad	<b>M 2.17 Sisenemise reeglid ja reguleerimine</b> M 1.55 Perimeetri kaitse M 2.2 Ressursside haldamine M 2.6 Sissepääsuõiguste andmine M 2.16 Välipersonali ja küllastajate valve ja saatmine M 2.90 Kohaletoimetamise kontroll	
9,2	Seadmete turve		
9.2.1	Seadmete paigutus ja kaitse	<b>M 1.29 IT-süsteemide õige paigutus</b> M 1.28 Puhvertoiteallikas (UPS) M 1.45 Äridokumentide ja -andmekandjate sobiv talletus	
9.2.2	Tehnilised tugiteenused	<b>M 1.28 Puhvertoiteallikas</b>  Schicht 2 Infrastruktu M 1.56 Varutoite allikas	
9.2.3	Kaabelduse turve	<b>B 2.2 Elektrotehniline kaabeldus</b> <b>B 2.12 IT-kaabeldus</b> M 1.2 jaotusseadmete pääsueeskirjad M 1.22 Liinide õige dimensioneerimine M 5.4 Kaabelduse dokumenteerimine ja märgistus M 5.5 Minimaalselt ohtlikud kaablitrassid	
9.2.4	Seadmete hooldus	<b>M 2.4 Hooldus – ja remonditööde reeglid</b>	
9.2.5	Seadmete turve väljaspool territooriumi	<b>B 2.10 Riistvara ja tarkvara inventuur</b> B 3.203 Sülearvuti M 1.33 Kaasaskantavate IT-süsteemide hoidmine reisil M 1.61 Mobiilse töökoha sobiv valimine ja kasutamine M 2.309 Mobiilse IT-kasutuse turvapoliitika ja eeskirjad	

			M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid M 2.112 Kodutööjaamade ja asutuse vahelise failide ja andmekandjate transportimise reguleerimine M 4.29 Kaasaskantavatele IT-süsteemidele mõeldud krüpteerimistoote kasutamine
	9.2.6	Seadmete turvaline kõrvaldamine või taaskasutus	<b>B 1.15 Andmete kustutamine ja hävitamine</b> M 2.431 Korrakohased protseduurid informatsiooni kustutamiseks või hävitamiseks M 4.234 IT-süsteemide ja andmekandjate väljavahetamise kord
	9.2.7	Omandi väljaviimine	<b>M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid</b> M 2.36 Sülearvuti väljaandmise ja tagastamise reeglid
10		<b>Side ja käituse haldus</b>	
	10,1	Käitumisprotseduurid ja -kohustused	
	10.1.1	Dokumenteeritud käitumisprotseduurid	<b>M 2.219 Infotöötuse pidev dokumenteerimine</b> B 1.9 Riistvara ja tarkvara haldus B 4.2 Võrgu- ja süsteemihaldus M 2.1 IT-kasutajate vastutuse ja reeglite kehtestamine M 2.201 Infoturbe protsessi dokumenteerimine
	10.1.2	Muutusehaldus	<b>B 1.14 Turvapaikade ja muudatuste haldus</b>
	10.1.3	Kohustuste lahusus	<b>M 2.5 Vastutuse ja ülesannete jaotamine</b>
	10.1.4	Arendus-, testimis- ja töövahendite lahusus	<b>M 2.62 Parametriseering</b> M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld M 2.82 Tüüp tarkvara nõuete kataloogi koostamine M 4.95 Minimaalne operatsioonisüsteem
	10,2	Kolmanda poole teenusetarnete haldus	
	10.2.1	Teenusetarnimine	<b>B 1.11 Väljastellimine</b> M 2.250 Väljastellimise strateegia määramine M 2.251 Väljastellimisprojektide turvanõuete spetsifitseerimine M 2.252 Väljastellitava teenuse sobiva tarnija valimine

			M 2.53 Faksi desaktiveerimine õhtul M 2.254 Väljast tellitud projektide infoturbekontseptsiooni loomine M .6.83 Väljasttellimise avariipartii
10.2.2	Kolmanda poole teenuse seire ja läbivaatus		<b>M 2.256 Infoturbe planeerimine ja käigushoidmine väljasttellimise tegevuste ajal</b> B 1.11 Väljasttellimine
10.2.3	Kolmanda poole teenuste muutuste haldus		<b>B 1.14 Turvapaikade ja muudatuste haldus</b> M 2.34 IT-süsteemi muudatuste dokumenteerimine
10,3	Süsteemide plaanimine ja vastuvõtmine		
10.3.1	Suutvuse haldus		<b>M 2.214 IT-kasutuse kontseptsioon</b>
10.3.2	Süsteemide vastuvõtmine		<b>M 2.62 Tarkvara vastuvõtuprotseduurid</b> B 1.14 Turvapaikade ja muudatuste haldus M 2.85 Tüüp tarkvara kinnitamine M 2.216 IT-komponentide kinnitamise protseduur M 4.65 Uue riist- ja tarkvara testimine
10,4	Kaitse kahjur- ja mobiilkoodi eest		
10.4.1	Kahjurkoodi tõrje meetmed		<b>B 1.6 Viirusetõrje kontseptsioon</b> B 1.8 Turvaintsidentide käsitlus M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld M 2.10 riistvara ja tarkvara inventuur M 2.35 parametrisering M 2.154 viirusetõrje kontseptsiooni loomine M 6.23 Käitumisreeglid arvutiviiruste esinemisel
10.4.2	Mobiilikoodi tõrje meetmed		<b>M 5.69 Aktiivsisu tõrje</b> B 1.6 Viirusetõrje kontseptsioon M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld M 2.198 Personali teadvustamine infoturbe küsimustes M 4.23 Lokaalse paketi filtri rakendamine M 4.100 Turvalüüs ja aktiivsisu M 4.199 Ohtlike failivormingute vältimine
10,5	Varundamine		
10.5.1	Teabe varuandamine		<b>B 1.4 Andmevarunduspoliitika</b> M 6.20 Varukoopia andmekandjate õige ladustus M 6.32 Regulaarne andmevarundus

			M 6.41 Andmete taastamise harjutamine
10,6	Võrguturbe haldus		
10.6.1	Võrguturbe meetmed		<b>B 4.1 Heterogeensed võrgud</b> B 4.4 Virtuaalne privaatvõrk (VPN) M 2.38 Administraatorirollide jagamine M 2.169 süsteemihalduse strateegia väljatöötamine M 2.279 marsruuterite ja kommutaatorite turvapoliitika koostamine M 4.79 Kohapealse võrguhalduse turvalised pääsumehhanismid M 4.80 Kaug-võrguhalduse turvalised pääsumehhanismid M 4.81 Võrgutoimingute audit ja logimine M 4.82 Võrgu aktiivkomponentide turvaline konfigureerimine M 5.7 Võrguhaldus M 5.9 Serveri logi M 5.68 Krüpteerimisprotseduuride kasutamine võrgusuhtluses M 5.71 Sissetungi tuvastuse ja sellele reageerimise süsteemid
10.6.2	Võrguteenuste turve		<b>B 4.1 Heterogeensed võrgud</b> B 3.301 Turvalüüs (tulemüür) B 4.2 Võrgu- ja süsteemihaldus B 4.4 Virtuaalne privaatvõrk (VPN) B 4.5 IT-süsteemi kohtvõrguühendus ISDN kaudu M 4.133 Sobivate autentimismehhanismide valimine M 5.68krüpteerimisprotseduuride kasutamine võrgusuhtluses M 5.71 Sissetungi tuvastuse ja sellele reageerimise süsteemid
10,7	Infokandjate käitlus		
10.7.1	Ird-infokandjate haldus		<b>M 2.3 Andmekandjate haldus</b> B 5.14 Mobiilsed andmekandjad M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid
10.7.2	Infokandjate kõrvaldamine		<b>B 1.15 Andmete kustutamine ja hävitamine</b> M 2.431 Korrakohased protseduurid informatsiooni kustutamiseks või hävitamiseks M 4.234 IT-süsteemide ja andmekandjate väljavahetamise kord
10.7.3	Teabe käitluse protseduurid		M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus B 5.2 Andmekandjatel toimuv

			andmevahetus B 5.3 Rühmatarkvara M 2.7 Süsteemi ja võrgu pääsuõiguste andmine M 2.42 Võimalike suhtluspartnerite määramine M 4.34 Krüpteerimise, kontrollsummade ja digitaalallkirjad rakendamine
10.7.4	Süsteemi dokumentatsiooni turve		
10,8	Infovahetus		
10.8.1	Infovahetuse poliitikad ja protseduurid		<b>M 2.393 Infovahetuse reguleerimine</b> B 3.402 Faks B 3.403 automaatvastaja B 3.404 Mobiiltelefon B 5.2Andmekandjatel toimuv andmevahetus B 5.3 Rühmatarkvara B 5.14 Mobiilsed andmekandjad B 5.19 Interneti kasutamine M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus M 2.398 printerite, koopiamasinate ja multifunktsionaalsete seadmete soetamise ning väljavalimise kriteeriumid M 5.88 Leping andmevahetuse kohta kolmandate pooltega
10.8.2	Infovahetuslepped		<b>M 5.88 Leping andmevahetuse kohta kolmandate pooltega</b> M 2.45 Andmekandjate üleandmine M 2.455 Infoturbepoliitika kehtestamine rühmatarkvara jaoks
10.8.3	Füüsiliste infokandjate transport		<b>M 5.23 Andmekandjate sobivate edastusviiside valimine</b> M 2.3 Andmekandjate haldus M 2.4 Hooldus- ja remonditööde reeglid M 2.44 Andmekandjate pakkimine edasiandmiseks M 2.45 Andmekandjate üleandmine M 2.112 Kodutööjaamade ja asutuse vahelise failide ja andmekandjate transportimise reguleerimine M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid
10.8.4	Elektrooniline sõnumivahetus		<b>B 5.3 Rühmatarkvara</b> B 5.19 Interneti kasutamine M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus M 5.54 Meili ülekoormuse ja spämmi tõrje

			M 5.56 Meiliserveri turvaline kasutamine M 5.108 Rühmatarkvara või meilisüsteemi krüptograafiline kaitse
10.8.5	Talitusinfosüsteemid		<b>M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus</b> M 2.1 IT-kasutajate vastutuse ja reeglite kehtestamine M 2.7 Süsteemi ja võrgu pääsuõiguste andmine M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine M 2.220 Pääsu reguleerimise suunised M 2.338 Sihtrühmakohase infoturbepoliitika koostamine
10,9	Elektronkaubanduse teenused		
10.9.1	Elektronkaubandus		<b>B 5.4 Veebiserver</b> M 2.162 Krüptoprotseduuride ja -toodete vajaduse määramine M 2.164 Sobiva krüptoprotseduuri valimine M 2.172 Veebilehe kasutamise kontseptsiooni väljatöötamine M 2.220 Pääsu reguleerimise suunised M 4.176 Autentimismeetodite valimine veebisaitide jaoks M 5.87 Leping kolmandate poolte võrkudega ühendamise kohta M 5.88 Leping andmevahetuse kohta kolmandate pooltega
10.9.2	Tehingud võrgu kaudu		<b>B 1.7 Krüptokontseptsioon</b> M 2.162 Krüptoprotseduuride ja -toodete vajaduse määramine M 2.164 Sobiva krüptoprotseduuri valimine M 4.176 Autentimismeetodite valimine veebisaitide jaoks M 5,88 Leping andmevahetuse kohta kolmandate pooltega
10.9.3	Avalik teave		<b>B 5.4 Veebiserver</b> B 5.19 Interneti kasutamine M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus M 2.272 Veebitoimetajate meeskonna loomine M 4.93 Regulaarne tervikluse kontroll M 4.94 Veebiserveri failide turve
10,1	<b>Seire</b>		
10.10.1	Revisjonlogimine		<b>M 2.64 Logifailide kontroll</b> M 2.110 Andmeprivaatsuse suunised logimisprotseduuridele M 4.81 Võrgutoimingute audit ja logimine

			M 5.9 Serveri logi
10.10.2	Süsteemide kasutamise seire		<b>M 2.64 Logifailide kontroll</b> M 2.133 Andmebaasisüsteemi logifailide kontroll M 4,81 Võrgutoimingute audit ja logimine M 5.9 Serveri logi
10.10.3	Logiteabe kaitse		<b>M 2.220 Pääsu reguleerimise suunised</b> M 2.110 Andmeprivaatsuse suunised M 4.34 Krüpteerimise, kontrollsummade ja digitaalallkirjade rakendamine M 4.93 Regulaarne tervikluse kontroll M 4.135 Süsteemifailide pääsuõiguste andmise kitsendused
10.10.4	Administraatori- ja operatori logid		<b>M 2.64 Logifailide kontroll</b> M 2.110 Andmeprivaatsuse suunised M 2.133 Andmebaasisüsteemi logifailide kontroll M 4.5 Kodukeskjaama (PBX) haldustööde logi M 4.25 Logimine Unix-süsteemis
10.10.5	Tõrgete logimine		<b>M 2.215 Tõrkekäsitlus</b> M 4.81 Võrgutoimingute audit ja logimine
10.10.6	Kellade sünkroniseerimine		<b>M 4.227 Lokaalse NTP-serveri rakendamine aja sünkroniseerimiseks</b>
11		<b>Pääsu reguleerimine</b>	
11,1	Tööalane vajadus pääsu reguleerida		
11.1.1	Pääsu reguleerimise poliitika		<b>M 2.220 Pääsu reguleerimise suunised</b> B 5.15 Üldine kataloogiteenus M 2.5 Vastutuse ja ülesannete jaotamine M 2.7 Süsteemi ja võrgu pääsuõiguste andmine M 2.8 IT-rakendustele ja andmetele pääsuõiguste andmine M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid
11,2	Kasutajate pääsu haldus		
11.2.1	Kasutajate registreerimine		<b>M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid</b> M 2.31 Volitatud kasutajate ja õiguseprofiilide dokumenteerimine M 2.63 Parametriseering M 3.2 Uute töötajate kohustamine eeskirju järgima M 3.6 Reguleeritud protseduur töösuhete lõpetamiseks M 4.13 Identifikaatorite hoolikas jaotamine M 2.402 Paroolide uuendamine

11.2.2	Privileegide haldus	<p><b>M 2.220 Pääsu reguleerimise suunised</b>  M 2.20 Liinide kontroll  M 2.38 Administraatorirollide jagamine  M 4.312 Kataloogiteenuste monitooring</p>
11.2.3	Kasutajate paroolide haldus	<p><b>M 2.11 Paroolide kasutamise reeglid</b>  M 2.22 Paroolide deponeerimine  M 4.7 Algparoolide muutmine  M 4.133 Sobivate autentimismehhanismide valimine  M 5.34 Ühekordsed paroolid</p>
11.2.4	Kasutajate pääsuõiguste läbivaatus	<p><b>M 2.31 Volitatud kasutajate ja õiguseprofiilide dokumenteerimine</b>  M 2.199 Infoturbe käigushoidmine</p>
11,3	Kasutaja kohustused	
11.3.1	Paroolide kasutamine	<p><b>M 2.11 Paroolide kasutamise reeglid</b>  M 2.22 Paroolide deponeerimine  M 3.5 IT-turvameetmete alane koolitus  M 3.26 Personali juhendamine IT-vahendite turvalise kasutamise alal  M 4.7 Algparoolide muutmine</p>
11.3.2	Järelvalveta kasutajaseadmed	<p><b>M 4.2 Ekraanilukk</b>  M 1.45 Äridokumentide ja -andmekandjate sobiv talletus  M 1.46 Vargustõrjevahendid  M 2.37 Korrastatud töölaud  M 3.26 Personali juhendamine IT-vahendite turvalise kasutamise alal</p>
11.3.3	Tühja laua ja tühja ekraani poliitika	<p><b>M 2.37 Korrastatud töölaud</b>  B 3.406 Printerid, koopiamasinad ja multifunktsionaalsed seadmed  M 4.1 Parametriseering  M 4.2 Parametriseering</p>
11,4	Võrkpääsu reguleerimine	
11.4.1	Võrguteenuste kasutamise poliitika	<p><b>M 2.220 Pääsu reguleerimise suunised</b>  B 4.4 Virtuaalne privaatvõrk (VPN)  M 2.71 Turvalüüsi (turvamüüri) turvapoliitika  M 2.169 Süsteemihalduse strateegia väljatöötamine  M 2.457 Interneti turvalise kasutamise kontseptsioon  M 2.214 IT-kasutuse kontseptsioon</p>
11.4.2	Kasutajate autentimine välisühendustes	<p><b>B 4.4 Virtuaalne privaatvõrk (VPN)</b>  B 4.5 IT-süsteemi kohtvõrguühendus ISDN kaudu  M 2.7 Süsteemi ja võrgu pääsuõiguste andmine  M 2.220 Pääsu reguleerimise suunised</p>

11.4.3	Seadmete identifitseerimine võrkudes	<b>M 4.82 Võrgu aktiivkomponentide turvaline konfigureerimine</b> M 4.133 Sobivate autentimismehhanismide valimine
11.4.4	Kaugdiagnostika ja -konfigureerimise portide kaitse	<b>B 4.4 Virtuaalne privaatvõrk (VPN)</b> M 4.80 Kaug-võrguhalduse turvalised pääsumehhanismid
11.4.5	Eraldamine võrkudes	<b>M 5.77 Alamvõrkude rajamine</b> M 5.61 Sobiv füüsiline segmenteerimine M 5.62 Sobiv loogiline segmenteerimine
11.4.6	Võrguühenduse reguleerimine	<b>B 3.301 Turvalüüs (turvamüür)</b> B 4.4 Virtuaalne privaatvõrk (VPN) M 4.238 Lokaalse paketi filtri rakendamine M 5.13 Võrgu ühendusaparatuuri õige kasutamine
11.4.7	Võrgu marsruutimise reguleerimine	<b>B 3.301 Turvalüüs (tulemüür)</b> B 3.302 Ruuter ja kommutaatorid M 4.82 Võrgu aktiivkomponentide turvaline konfigureerimine M 5.61 Sobiv füüsiline segmenteerimine M 5.70 Aadressi tõlkimine – Network Address Translation (NAT)
11,5	Operatsioonisüsteemi pääsu reguleerimine	M 4.15 Turvaline sisselogimine M 2.220 Pääsu reguleerimise suunised M 2.321 Klient-server-võrgu kasutuselevõtu planeerimine M 2.322 Klient-server-võrgu turvapoliitika kehtestamine M 4.133 Sobivate autentimismehhanismide valimine
11.5.1	Turvaline sisselogimisprotseduur	<b>M 4.15 Turvaline sisselogimine</b> M 2.220 Pääsu reguleerimise suunised M 2.321 Klient-server-võrgu kasutuselevõtu planeerimine M 2.322 Klient-server-võrgu turvapoliitika kehtestamine M 4.133 Sobivate autentimismehhanismide valimine
11.5.2	Kasutajate identifitseerimine ja autentimine	<b>M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid</b> M 2.220 Pääsu reguleerimise suunised
11.5.3	Paroolihalduse süsteem	<b>M 2.11 Paroolide kasutamise reeglid</b> M 4.133 Parametriseering
11.5.4	Süsteemiutiliitide kasutamine	<b>M 4.135 Süsteemifailide pääsuõiguste andmise kitsendused</b>
11.5.5	Seansi kontrolllaeg	<b>M 3.18 PC kasutajate väljalogimiskohustus</b> M 4.2 Ekraanilukk

			M 4.41 Sobivate IT-süsteemide turvatoodete valimine
	11.5.6	Ühendusaja piiramine	<b>M 4.16 Konto- ja/või terminalipääsu piirangud</b> M 4.133 Parametriseering
	11,6	Rakenduste ja teabe pääsu reguleerimine	
	11.6.1	Teabepääsu kitsendamine	<b>M 2.8 IT-rakendustele ja andmetele pääsuõiguse andmine</b> M 2.30 Kasutajate ja kasutajarühmade määramise protseduurid M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus M 2.220 Pääsu reguleerimise suunised
	11.6.2	Tundlike süsteemide isoleerimine	<b>M 5.77 Alamvõrkude jagamine</b> M 5.61 Sobiv füüsiline segmenteerimine M 5.62 Sobiv loogiline segmenteerimine
	11,7	Mobiil- ja kaugtöö	
	11.7.1	Mobiiltöötlus ja -side	<b>B 2.10 Mobiilne töökoht</b> B 3.203 Sülearvuti B 3.404 Mobiiltelefon B 3.405 Pihuarvuti (PDA) M 1.33 Kaasaskantavate IT-süsteemide hoidmine reisil M 2.309 Mobiilse IT-kasutuse turvapoliitika ja eeskirjad M 2.218 Andmekandjate ja IT-komponentide kaasavõtmise protseduurid
	11.7.2	Kaugtöö	<b>B 5.8 Kaugtöö</b>
12		<b>Infosüsteemide hankimine, väljatöötamine ja hooldus</b>	
	12,1	Infosüsteemide turvanõuded	
	12.1.1	Turvanõuete analüüs ja spetsifitseerimine	<b>M 2.80 Tüüparkvara nõuete kataloogi koostamine</b> B 1.10 Tüüparkvara B 1.9 Riistvara ja tarkvara haldus M 2.62 Parametriseering M 2.66 Sertifikaatidega arvestamine IT soetamisel M 2.83 Tüüparkvara testimine
	12,2	Õige töötlus rakendustes	
	12.2.1	Sisendandmete valideerimine	<b>M 2.83 Tüüparkvara testimine</b> M 2,363 SQL-injektsiooni kaitse
	12.2.2	Sisemise töötluse kontroll	<b>M 2.378 Süsteemiarendus</b> M 2.82 Tüüparkvara testimisplaani väljatöötamine M 2,83 Tüüparkvara testimine

12.2.3	Sõnumite terviklus	<b>M 4.34 Krüpteerimine, kontrollsummade ja digitaalallkirjade rakendamine</b> B 1.7 Krüptokontseptsioon
12.2.4	Väljundandmete valideerimine	<b>M 2.83 Tüüp tarkvara testimine</b>
12,3	Krüptograafilised turvameetmed	
12.3.1	Krüptograafiliste turvameetmete kasutamise poliitika	<b>B 1.7 Krüptokontseptsioon</b> M 2.161 parametrisering
12.3.2	Võtmehaldus	<b>B 1.7 Krüptokontseptsioon</b> M 2.46 Krüpteerimise õige korraldus M 2.164 Sobiva krüptoprotseduuri valimine
12,4	Süsteemifailide turve	
12.4.1	Töötarkvara ohje	<b>B 1.9 Riist- ja tarkvara haldus</b> B 1.10 Tüüp tarkvara M 2.62 Tarkvara vastuvõtuprotseduurid M 2.85 Tüüp tarkvara kinnitamine M 2.87 Tüüp tarkvara installeerimine ja konfigureerimine M 2.88 Tüüp tarkvara litsentsi- ja versioonihaldus
12.4.2	Süsteemi testandmete kaitse	<b>M 2.83 Tüüp tarkvara testimine</b>
12.4.3	Programmide lähtekoodi pääsu reguleerimine	<b>M 2.378 Süsteemiarendus</b> M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld M 2.62 Tarkvara vastuvõtuprotseduurid M 4.135 Süsteemifailide pääsuõiguste andmise kitsendused
12,5	Turve arendus- ja tugiprotsessides	
12.5.1	Muutuseohje protseduurid	<b>B 1.14 Turvapaikade ja muudatuste haldus</b> M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld M 2.34 IT-süsteemi muutuste dokumenteerimine M 2.62 Tarkvara vastuvõtuprotseduurid
12.5.2	Rakenduste tehniline läbivaatus pärast operatsioonisüsteemi muudatusi	<b>M 4.78 Konfiguratsioonimuudatuste hoolikas teostamine</b> B 1.14 Turvapaikade ja muudatuste haldus M 2.62 Tarkvara vastuvõtuprotseduurid
12.5.3	Tarkvarakomplektide muudatuste kitsendused	<b>M 2.9 Aktsepteerimata riist- ja tarkvara kasutuse keeld</b>
12.5.4	Infolekkes	<b>M 2.224 Trooja hobuste tõrje</b> M 2.66 Sertifikaatidega arvestamine IT soetamisel

			<p>M 2.87 Tüüptarkvara installeerimine ja konfigureerimine</p> <p>M 2.214 IT-kasutuse kontseptsioon</p> <p>M 3.10 Usaldusväärse administraatori ja tema asetäitja valimine</p> <p>M 4.35 Saatmisele eelnev andmete kontroll</p>
12.5.5	Väljastellitud tarkvaraarendus	<p><b>B 1.1 Organisatsioon</b></p> <p>M 2.250 Väljastellimise strateegia</p> <p>M 2.251 Väljastellimisprojektide turvanõuete spetsifitseerimine</p> <p>M 2.252 Väljastellitava teenuse sobiva tarnija valimine</p> <p>M 2.253 Välise teenusepakkujaga sõlmitava lepingu koostamine</p> <p>M 2.254 Väljast tellitud projektile infoturbekontseptsiooni loomine</p> <p>M 2.255 Turvaline üleviimine väljast tellitud projektides</p> <p>M 2.256 Infoturbe planeerimine ja käigushoidmine väljastellimise tegevuste ajal</p>	
12,6	Tehniliste nõrkuste haldus		
12.6.1	Tehniliste nõrkuste ohje	<p><b>M 2.35 Teabe hankimine turvaaukude kohta</b></p> <p>M 2.273 Turvalisust mõjutavate paikade ja värskenduste kiire paigaldamine</p>	
13	<b>Infoturbeintsidentide haldus</b>		
13,1	Teatamine infoturbesündmustest ja -nõrkustest		
13.1.1	Teatamine infoturbesündmustest		
13.1.2	Teatamine turvanõrkustest	<p><b>B 1.8 Turvaintsidentide käsitlemine</b></p> <p>M 2.35 Teabe hankimine turvaaukude kohta</p> <p>M 6.60 Turvaintsidentide käsitlemisprotseduurid ja teavitamiskanalid</p>	
13,2	Infoturbeintsidentide ja -täiustuste haldus		
13.2.1	Kohustused ja protseduurid	<p><b>B 1.8 Turvaintsidentide käsitlemine</b></p> <p>M 6.58 Turvaintsidentide käsitlemise haldussüsteemi rajamine</p> <p>M 6.59 Turvaintsidentide käsitlemise eest vastutavate isikute määramine</p>	
13.2.2	Infoturbeintsidentidest õppimine	<p><b>B 1.8 Turvaintsidentide käsitlemine</b></p> <p>M 6.66 Turvaintsidentide järelhindamine</p> <p>M 6.68 Turvaintsidentide käsitlemise süsteemi tõhususe testimine</p>	

	13.2.3	Asitõendite kogumine	<b>B 1.8 Turvaintsidentide käsitus</b> M 6.127 Tõendite varundusmeetmete kindlaksmääramine seoses turvaintsidentidega
14		<b>Jätkusuutlikkuse haldus</b>	
	14,1	Jätkusuutlikkuse halduse infoturbeaspektid	
	14.1.1	Infoturbe lülitamine jätkusuutlikkuse halduse protsessi	<b>B 1.3 Hädaolukorraks valmisoleku kontseptsioon</b> BSI-Standard 100-2, peatükk 3 BSI-Standard 100-3 IT-etalon turbel põhinev riskianalüüs BSI-Standard 100-4 Hädaolukordade haldus B 1.8 Turvaintsidentide käsitus
	14.1.2	Jätkusuutlikkus ja riski kaalutlemine	<b>B 1.3 Hädaolukorraks valmisoleku kontseptsioon</b> BSI-Standard 100-3 IT-etalon turbel põhinev riskianalüüs BSI-Standard 100-4 Hädaolukordade haldus B 1.8 Turvaintsidentide käsitus
	14.1.3	Infoturvet hõlmavate jätkusuutlikkuse plaanide koostamine ja teostegemine	<b>B 1.3 Hädaolukorraks valmisoleku kontseptsioon</b> BSI-Standard 100-4 Hädaolukordade haldus B 1.8 Turvaintsidentide käsitus
	14.1.4	Jätkusuutlikkuse plaanimise raamstruktuur	<b>B 1.3 Hädaolukorraks valmisoleku kontseptsioon</b> BSI-Standard 100-4 Hädaolukordade haldus B 1.8 Turvaintsidentide käsitus
	14.1.5	Jätkusuutlikkuse plaanide testimine, hooldus ja ümberhindamine	<b>B 1.3 Hädaolukorraks valmisoleku kontseptsioon</b> BSI-Standard 100-4 Hädaolukordade haldus B 1.8 Turvaintsidentide käsitus
15		<b>Vastavus</b>	
	15,1	Vastavus õigusaktide nõuetele	
	15.1.1	Kohaldatavate õigusaktide väljaselgitamine	<b>B 1.16 Nõuete haldus</b> M 2.340 Õiguslike raamtingimuste järgimine M 3.2 Uute töötajate kohustamine eeskirju järgima
	15.1.2	Intellektuaalse omandi kaitse	<b>B 1.16 Nõuete haldus</b> M 2.217 Teabe, rakenduste ja süsteemide hoolikas liigitamine ja käitlus M 2.10 Riistvara ja tarkvara inventuur M 4.99 Kaitse info muutmise eest pärast üleandmist
	15.1.3	Organisatsiooni andmestike	<b>M 2.217 Teabe, rakenduste ja süsteemide</b>

		kaitse	hoolikas liigitamine ja käitlus
15.1.4	Andmekaitse ja isikuteabe privaatsus		<b>B 1.16 Nõuete haldus</b> B 1.5 Andmekaitse M 3.2 uute töötajate kohustamine eeskirju järgima M 2.10 Riistvara ja tarkvara inventuur M 2.205 Isikuandmete edastus ja kättesaadavus
15.1.5	Infotöötlusvahendite väärkasutuse vältimine		<b>B 1.16 nõuete haldus</b> M 2.380 Erandite kooskõlastamine B 1.13 Infoturbe teadlikkus ja -koolitus M 3.26 Personali juhendamine IT-vahendite turvalise kasutuse alal
15.1.6	Krüptograafiliste turvameetmete reguleerimine		<b>B 1.16 Nõuete haldus</b> M 2.163 Krüptoprotseduure ja -tooteid mõjutavate tegurite määramine
15,2	Vastavus turvapoliitikatele ja -normidele ja tehniline vastavus		
15.2.1	Vastavus turvapoliitikatele ja -normidele		<b>B 1.16 Nõuete haldus</b> M 2.199 Infoturbe käigushoidmine BSI-Standard 100-2, peatükk 3
15.2.2	Tehnilise vastavuse kontroll		<b>M 2.199 Infoturbe käigushoidmine</b>
15,3	Infosüsteemide auditi kaalutlusi		
15.3.1	Infosüsteemide auditi turvameetmed		<b>B 1.16 Nõuete haldus</b> M 2.199 Infoturbe käigushoidmine M 2.64 Logifailide kontroll M4.81 Võrgutoimingute audit ja logimine
15.3.2	Infosüsteemide auditi instrumentide kaitse		<b>M 2.199 Infoturbe käigushoidmine</b>