# Keskuspuiston ammattiopisto: tietoturvakartoituksesta tietoturvan hallintajärjestelmään

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ylemmän ammattikorkeakoulututkinnon opinnäytetyö

TOSJO07

Visamäen yksikkö 20.05.2009

Charles Gustafsson

Koulutusohjelma
Visamäki
13100 Hämeenlinna

| | |
|---|---|
| Työn nimi | Keskuspuiston ammattiopisto: tietoturvakartoituksesta tietoturvan hallintajärjestelmään |
| Tekijä | Charles Gustafsson |
| Ohjaava opettaja | Jarmo Levonen |
| Hyväksytty | _____._____.20_____ |
| Hyväksyjä | |

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

VISAMÄKI
Koulutusohjelman nimi Teknologiaosaamisen johtamisen koulutusohjelma 2007

**Tekijä** Charles Gustafsson **Vuosi** 2009

**Työn nimi** KESKUSPUISTON AMMATTIOPISTO: TIETOTURVAKARTOITUKSESTA TIETOTURVAN HALLINTAJÄRJESTELMÄÄN

**Työn säilytyspaikka** HAMK, Visamäki

TIIVISTELMÄ

Opinnäytetyön tarkoituksena on ollut tutkia, kuinka koulun tietoturvan nykytila selvitetään ja kuinka tietoturvallisuuden hallintajärjestelmä suunnitellaan, toteutetaan ja kehitetään kouluorganisaatiossa käyttäen hyväksi standardissa ISO/IEC 27001:fi esitetty jä valvontatavoitteita ja turvamekanismeja. Tutkimusmenetelmänä on käytetty toimintatukimusta, jossa tietoturvan nykytilaa on verrattu standardin esittämään ihannetilaan. Vertailusta saadut tulokset esitetään ja ehdotus tietoturvan hallintajärjestelmän käyttöönotolle tehdään. Tutkimus tehtiin Keskuspuiston ammattiopistossa Helsingissä syksyllä 2008. Työn on tarkoitus toimia apuvälineenä myös toisille organisaatioille, jotka suunnittelevat tietoturvan hallintajärjestelmän käyttöönottoa ja/tai tietoturvan tilan kartoitusta. Tutkittavina aihealueina olivat tietoturvallisuuden hallintajärjestelmään liittyvät standardit ISO/IEC 27002 ja ISO/IEC 27001:fi sekä valtionhallinnon tietoturvallisuuteen liittyvä ohjeistus ja Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskuksen tietoturvallisuussuositukset. Muu tutkimuksen lähdemateriaali liittyy tietoturvallisuudesta kertovaan kirjallisuuteen ja sähköiseen lähdeaineistoon.

Toimintatutkimuksen avulla pyritään kehittämään Keskuspuiston ammattiopiston tietoturvaa vaikuttamalla organisaation toimintatapoihin. Vertailemalla nykytilannetta standardien esittämään tilaan laaditaan kehittämisohjelma. Tutkimus osoitti, että tietoturvallisuuden hallintajärjestelmän kehittäminen on jatkuva prosessi. Toistuvan syklin vaiheet ovat suunnittelu, toteutus, arviointi ja kehitys. Standardien avulla luodaan uskottava tietoturvallisuuden hallintajärjestelmä ja helpotetaan tietoturvan hallintajärjestelmän kehittämisprosessin dokumentointia. Tietoturvan hallintajärjestelmän asteittaista käyttöönottoa suositellaan Keskuspuiston ammattiopistolle. Sopivat etenemisaskelmat olisivat: johdon hyväksymän tietoturvapolitiikan laatiminen, riskikartoitus, suojattavan tiedon määritteleminen, työntekijöiden motivointi tietoturvatyöhön, tietoturvatietoisuuden lisääminen varsinkin rekrytointivaiheessa ja järjestelmätuen yhtenäiset kirjalliset toimintaohjeet

**Avainsanat** Tietoturvan hallintajärjestelmä, tietoturva, suojattava kohde, riski.
**Sivut** 32 s. + liitteet 53 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

ABSTRACT

VISAMÄKI
Name of degree programme Teknologiaosaamisen johtamisen koulutusohjelma 2007

**Author** Charles Gustafsson **Year** 2009

**Subject of Master's thesis** KESKUSPUISTO VOCATIONAL COLLAGE: FROM INFORMATION SECURITY SURVEY TO ISMS

**Archives** HAMK University of Applied Sciences, Visamäki

ABSTRACT

The purpose of the thesis has been to find out the current status of the information security at Keskuspuisto Vocational Collage and the method for planning, executing, implementing and auditing an information security managing system (ISMS) in the commissioning vocational school. The modeling source is the standard ISO/IEC 27001and its control objectives and controls. Survey research has been used as the research method comparing the present state of information security with the ideal model of the standard. The results of the comparison are presented and a proposal for implementing ISMS is made. The research was made in Keskuspuisto Vocational Institute in Helsinki in the autumn of 2008. The purpose of the thesis is also to serve as a model and instrument for other organisations and schools who are investigating their possibilities to implement ISMS and/or examine the state of their information security. The researched fields have been the associated with ISMS standards ISO/IEC 27002 and ISO/IEC 27001, as well as the public administration information security guidelines and public administration information security references. The other background material was obtained from various information security and electronic literature.

The intention of the survey is to develop the information security of Keskuspuisto Vocational Collage by influencing the ways of its actions. A development plan is made by comparing the current status with that of the standard. The survey indicated that the development of ISMS is a continuous process. The repeating stages of the cycle are planning, implementing, evaluating and developing. A stepwise implementation of ISMS is recommended at Keskuspuisto Vocational Collage. Proper steps for the development are: an information security policy document approved by management, implementation of a risk treatment plan, definition of the asset management, motivation of employees into safe approach, increase of information security consciousness especially in the recruiting process and developing uniform written instructions for the system administrators.

**Keywords** ISMS Information Security Management System, information security, asset, risk.

**Pages** 32 p. + appendices 53 p.

SISÄLLYS

# 1 JOHDANTO

Tietoturvallisuuden hallint ajärjestelmä ja tietotu rvapolitiikka puuttuvat vielä m onelta pk-yritykseltä Suom essa. Valtionhallinto ja m onet konsulttiyritykset tarjoavat apua ongelm aan. Keväällä 2007 Oulun yliopisto ilmoitti ha lustaan auttaa pieniä org anisaatioita luom aan näm ä toim innot. Siitä kertova lehtiartikkeli Helsingin Sanom issa 10.4.2007 toim i innoittajana tämän selvityksen tekemiseen.

Tietoturvallisuuteen on olemassa kansainväliset standardoidut ohjeet, joita noudattamalla organisaatio voi laatia tietoturvallisuuden ha llintajärjestelmän. Standardinm ukaisella ser tifioinnilla organisaatio voi myös osoittaa sidosryhmille panostavansa tehokkaaseen ja valvottuun tiedon turvaam iseen.

Tämän opinnäytetyön tavoitteena on tehdä selvitys, joka tukisi m ahdollisimman hyvin toim eksiantajan, Kes kuspuiston amm attiopiston, tietoturvallisuuden hallintajärjestelmän suunnitteluprosessia ja kuvaisi tietoturvan nykyistä tasoa. Tutkimusongelmat painottuvat seuraaviin kysymyksiin:

1. Mikä on Keskuspuiston ammattiopiston tietoturvan taso tällä hetkellä?
2. Tarvitaanko Keskuspuiston ammattiopistossa tietoturvan hallintajärjestelmää?
3. Miten tieto turvaa vo itaisiin p arantaa Keskuspuiston amm attiopistossa yksinkertaisin toimenpitein.
4. Miten tässä työssä esitettyä m allia voisi hyödyntää toisessa kouluorganisaatiossa?

Tässä työss ä tieto turvallisuuden hallinta järjestelmän käsittely ra jataan koskemaan toisen asteen ammatillis en amm attioppilaitoksen yleisiä opetustoimintaprosesseja. A ihetta e i kä sitellä ta rkemmin yksittäisten liike toiminta-alueiden kannalta tai yksittä isen tie tojärjestelmän kannalta va an noudatetaan ISO/IEC tietoturvastandardin 27001:fi ja ISO/ICE 27002 mukaista käsittelytapaa ja jaotte lua. Työ tehdään niin avoim esti, ettei m itään osia tarvitsisi julistaa salaisiksi. Tämä edellyttää, ettei työssä ilmaista yksityiskohtaista tieto a organisaation su ojatuista tiedoista,. Silloin m ahdollistuu työn k äyttö kokeilu mallina kouluissa, jo tka suunnittelevat tieto turvan hallintajärjestelmän käyttöön o ttoa. Suoraa kop ioimista, täs tä m allista ei suositella, koska jokaisella organisaatiolla on o mat toim intatapansa ja toimintakriteeristönsä.

## 1.1 Asiayhteys

Keskuspuiston ammattiopisto on Orton Invalidisäätiön ylläpitämä toisen asteen ammatillinen erityisoppilaitos ja erityisopetuksen kehittämiskeskus. Se tarjoaa monipuolisia opetus-, kehittämis-, ja asiantuntijapalveluja opiskelijoille, toisille oppilaitoksille ja muille yhteistyötahoille. Keskuspuistolla ja Invalidisäätiöllä on yhteinen missio ja visio. Monet toimintastrategiat ovat myös yhteisiä.

Keskuspuiston ammattiopiston perustana on elämän ja ihmisarvon kunnioittaminen. Opisto panostaa yksilölliseen palveluun ja tukee opiskelijoittensa kuntoutumista, oppimista, ja omaehtoista elämänhallintaa. Yksilölliset ja joustavat opiskelusuunnitelmat sekä pienet opintoryhmät luovat hyvän lähtökohdan opiskelulle (Laatukäsikirja 2003).

Tavoitteena on, että Keskuspuiston ammattiopistosta valmistuneilla opiskelijoilla on hyvä yksilöllisesti mitoitettu ammattitaito, elinikäinen halu oppia uusia asioita ja mahdollisuus sijoittua yhteiskuntaan sen täysivaltaisina jäseninä (Laatukäsikirja 2003).

Koulu on osallistunut ammatillisen koulutuksen laatupalkintokilpailuihin ja menestynyt niissä kohtuullisesti. Aluksi koululla oli puutteita dokumentoitujen toimintaohjeiden, standardien ja prosessikuvausten kanssa. Näitä dokumentteja on vuosien mittaan tuotettu ja uusittu ahkerasti. Tietoturvan ja tietosuojan puolelta ei kirjallista kuvausta ole toistaiseksi olemassa. Tämän työn tarkoituksena on korjata kyseistä puutetta ja edesauttaa systemaattisen tietoturvallisuuden hallintajärjestelmän luomisessa. Hallintajärjestelmä muodostuu itseään toistavan prosessin avulla ja tarvitsee useamman päivityskierroksen. Luonnollinen aloituskohta on vallitsevan tilanteen kartoitus.

## 1.2 Strategia

Keskuspuiston ammattiopiston arvot, missio, visio ja strategiat on esitetty organisaation laatukäsikirjassa (Laatukäsikirja 2003). Sen avulla on löydettävissä seuraavassa esitettävät perustelut tietoturvapolitiikan luomiselle.

Arvojen joukossa todetaan, että henkilökunnan ammatilliseen osaamiseen kuuluu: jatkuva oppiminen, kehittyminen, yhteistyökyky ja innovatiivisuus. Tämä näkyy laadukkaana, luotettavana ja tuloksellisena työnä.

Visiossa mainitaan, että tietotekniikkaa sovelletaan laajasti ja korkeatasoisesti osana kokonaisvaltaista oppimisen suunnittelua ja toteutusta verkostoyhteistyössä oppilaiden ja muiden palvelu- ja tutkimusorganisaatioiden kanssa. Tämä edellyttää tietoteknistä luotettavuutta ja turvallisuutta kaikissa toiminnoissa. Vision toteuttaminen edellyttää siten laajaa ja korkeatasoista tietotekniikan osaamista ja verkkopedagogiikan kehittämistä. Tietokoneiden ja tietoverkkojen käyttö puolestaan edellyttää tuntemusta tietoturvasta, joka saavutetaan toteuttamalla toimivaa tietoturvapolitiikkaa.

Missiossa todetaan, että Keskuspuiston ammattiopistossa erityisenä koulutustehtävänä on huolehtia erityisopetuksen järjestämisestä, sen yhteydessä vammaisille annettavasta valmentavasta ja kuntouttavasta opetuksesta sekä ohjauksesta mukaan lukien maahanmuuttajien koulutus. Tehtävä vaatii erityistä huomiota tietokoneiden ja tietoverkojen turvallisessa käytössä.

Organisaation toimintaa kuvaavat tapahtumaketjut eli prosessit joiden kuvaukset osoittavat miten ne kulkevat eri työvaiheiden kautta ja määrittävät toimintavastuut. Vision toteuttaminen edellyttää tässä työssä esitetystä näkökulmasta katsottuna, että koko henkilöstö soveltaa laajaa ja korkeatasoista tietotekniikan osaamista, verkkopedagogiikan kehittämistä ja oppimista tukevien uusia menetelmiä, materiaaleja, välineitä ja ympäristöjen suunnittelua sekä niiden kokeilua ja käyttöä. Tietotekniikka on oleellinen osa näitä alueita ja tietoturva on oleellinen osa tietotekniikkaa.

Strategiat vyörytetään prosessien kautta tiimeihin, jolloin koko henkilökunta joutuu vastuuseen omasta osuudestaan noudattaa yhteisesti hyväksyttyjä strategioita. Siten se on myös vastuussa tietoturvasta, joka on osa organisaation käytössä olevia strategioita.

Keskuspuiston ammattiopistossa on meneillään organisaationmuutos. Valtionhallinto lopettaa omat valtion erityisoppilaitokset. Tämän seurauksena Arla-instituutti Espoosta sulautetaan Keskuspuiston ammattiopistoon 1.1.2009. Lisäksi Helsingin Metsälään on syntymässä uusi kohtuullisen suuri koulun toimipaikkakeskittymä. Aiemman yhden keskittyneen tietojärjestelmän hallintopaikan sijaan tulevaisuudessa niitä tulee olemaan ainakin kolme ja tietohallinnolle nimitetään tietohallintopäällikkö. Tämä asettaa uudenlaiset vaatimukset tietohallinnon tietoturvamenettelyille ja sen myötä vaatimukset tiedon ja menettelytapojen dokumentoinnille kasvavat oleellisesti.

Organisaatio muuttuu suuremmaksi ja opiskelijamäärä kasvaa 880:een ja henkilökunnan määrä 460:een. Näin suuri joukko ja sen käyttämät tietotekniikkajärjestelmät ja -laitteet tarvitsevat yhtenäisiä käytäntöjä toimintaansa. Tällaista järjestelmää kutsutaan tietohallinnon hallintajärjestelmäksi, jonka käyttöön otolla alkaa olla kiire. Järjestelmä on laaja, eikä se synny ilman resursointia.

# 2 TIETOTURVATILANNE KESKISUURISSA ORGANISAATIOISSA

Tietoturvan hallintajärjestelmä on monessa keskisuuressa ja pienessä organisaatiossa heikosti tiedostettu osa tietoturvaa sen kehittämistyö tarjoaa oikotien kommunikoinnille tietoturvasta kiinnostuneille osapuolille Keskuspuiston ammattiopistossa ja samalla muillekin asiasta kiinnostuneille kouluorganisaatioille. Liiteosassa esitetty tietoturvan tilaa kartoittava kysymyssarja on pyritty esittämään niin avoimesti kuin mahdollista, vaarantamatta omaa tietoturvaa, jotta tietojen käytettävyys toisessa organisaatiossa olisi mahdollisimman yksiselitteistä. Tietoturvan hallintajärjestelmän toteuttaminen voi pikaisella silmäyksellä näyttää yksinkertaiselta toimenpiteeltä, kun taas syvällisempi tarkastelu voi luoda mielikuvan ylivoimaisesta tehtävästä. Teoreettisen tarkastelutavan tarkoitus on tuoda esille ongelman monimutkaisuus, mutta samalla sen hallittavuus käyttäen hyväksi valmiina olevia standardeja ISO/IEC 27001 ja 27002. Yhteiset neuvottelut organisaatiossa eri osapuolten välillä ovat luoneet ja luovat tulevaisuudessa uusia ideoita asioiden ratkaisemiseksi ja parantamiseksi. Laatujärjestelmä ja tietoturvallisuuden hallintajärjestelmän näennäinen erilaisuus osoittautuvat lähemmässä tarkastelussa läheiseksi ja toiminnoiltaan hyvin samankaltaisiksi. Tämä teoreettinen tieto helpottaa arkipäivän toiminnoissa ja kehitysprojektin läpiviennissä.

## 2.1 Aikaisemmat tutkimukset

Valtionhallinto panostaa voimakkaasti tietoturvan hallintajärjestelmien käyttöönottoon, arviointiin ja parantamiseen. Tietoa siitä jaetaan VAHTI -järjestelmän kautta valtionvarainministeriön www- sivuilla. Sivut sisältyvät jokaisen tietoturvan hallintajärjestelmää käsittelevään tutkimukseen. Ammattikorkeakouluissa ja yliopistoissa on tehty tutkimuksia aiheesta. Työt ammattikorkeakouluissa ja teknisissä yliopistoissa ovat puolestaan yleensä tehty toimeksiannosta, jolloin osa tutkimuksesta on salaista. Näistä töistä saa hyvää teoreettista tietoa ja lähdeviitteitä omaan työhönsä. Käytännön esimerkit ja toteutukset jäävät ylleensä pimentoon. Tiedeyliopistojen puolelta tulevat tutkimukset ovat teoriapainotteisia ja työläitä siirtää käytännön työhön.

Turvallisuuskulttuurin edistäminen on monella organisaatiolla noussut kehityskohteiden kärkijoukkoon, mutta kovin monessa organisaatiossa tietoisuus kehitystarpeesta ei näytä vielä kanavoituneen toiminnaksi. Panostukset tälle alueelle tulevat kasvamaan selvästi lähivuosina. Tietoturvan tilaa luotaavia kansainvälisiä tutkimuksia julkaistaan useita vuodessa, mutta vastaavia tutkimuksia ei ole aiemmin toteutettu puhtaasti Suomessa toimiviin organisaatioihin keskittyen. Vaikka monet tietoturvan ilmiöt ja trendit ovat globaaleja, eroavat paikallinen toimintakulttuuri ja lainsäädäntö eri puolilla maailmaa toisistaan (Nixu 2008).

Suomalaisten organisaatioiden yleisin haaste tietoturvan toteuttamiselle on riittämättömät resurssit. Se ei ole kuitenkaan yllättävää, kun vastuuhenkilöiden ajasta leijonanosa menee vähemmän tärkeisiin aiheisiin, tietoturvan hyötyjä ei osata mitata, eikä tietoturvan budjetointia ja investointien perus-

telua pidetä kovin tärkeänä . Organisaatioissa, joissa ei ole nim ettyä tietoturvapäällikköä tai tieto turvan ohja usryhmää, painottuu vastauksissa useammin tietoturvan tekninen puoli. R iittävän m onipuolisesti organisaatiota edustava ohjausryhmä näyttää olevan paras tapa ohjata tekemistä sellaisiin oleellisiin asioihin, kuin tietoturvatietoisuuden kehittäminen ja henkilöstön sitouttaminen sovittujen periaatteid en m ukaiseen toim intaan. Turva llisuuskulttuurin edistäm inen on m onessa organisaatiossa noussut kehityskohteiden kärkijoukkoon, m utta kovin m onessa organisaatiossa tietoisuus kehitystarpeesta ei näytä vielä kanavoituneen toiminnaksi. Panostukset tälle alueelle tulevat kasvamaan selvästi lähivuosina (Nixu 2008).

Jokaisesta työstä löytää jonkun helm en, joka vie om aa asiaa eteenpäin, siksi tutkimuksen nopea läpikäynti ja oikean asian löytäminen on hyvä avu hyödynnettäessä olem assa olevia tutkim uksia. Tiedettäessä m itä etsitään läpikäynti voi olla hyvinkin nopeata sähköisissä dokum enteissa, joita Internetistä löytyy yllättävän paljon. Työt ovat tallennettuina hyvin erilaisiin paikkoihin, joten löydetyn dokumentin aitous kannattaa aina tarkistaa.

## 2.2 Teoriat ja hyvät käytännöt

Tietoturvan hallinta järjestelmän keh itystyö tehdään usein standardien perusteella. Niiden läpikäynti on työläs prosessi. Toisaalta standardi vaatii jokaista organisaatiota käym ään läpi om an järjestelm änsä, koska on kuitenkin oletettavaa, että kahdesta samantyyppistä koulusta löytyy m onta yhdistävää tekijää ja osa kä ytänteistä voi olla jopa hyvinkin sa manlaisia, jouduttaa mallin katsom inen valmiiksi tehdystä työstä tietoturvan hallintajärjestelmän toteutusta. Suora kopioim inen ei johda hyvään tulokseen. Kehittämisprosessi luo om an näköisen jä rjestelmän aikanaan. Aloitta minen voi kuitenkin olla liian iso haaste jossakin organisaatiossa. Mainitulla mallilla vo isi m adaltaa kynnystä. Tätä työ tä s aa käyttää apukeinona jos sen sellaiseksi mieltää.

# 3 MENETELMÄT

Tutkimusmenetelmän malliksi valittiin standardit ISO/IEC 27001:fi Informaatioteknologia, turvallisuus, tietoturvallisuuden hallintajärjestelmät, vaatimukset ja ISO/IEC 27002 Information technology- Security techniques- Code of practice for information security management. Menetelmäksi valittiin toimintatutkimus. Toimintatutkimuksen avulla pyritään kehittämään Keskuspuiston ammattiopiston tietoturvaa vaikuttamalla organisaation toimintatapoihin. Standardien avulla kuvaillaan minkä lainen tietoturvallisuuden hallintajärjestelmä tulisi olla, kun se halutaan sertifioida ja mikä on tietoturvallisuuden tila tällä hetkellä Keskuspuiston ammattiopistossa. Vertailemalla saatuja tuloksia kuvataan tietoturvan taso organisaatiossa ja esitetään tilanteeseen sopivat toimenpiteet kappaleessa 5 yhteenveto. Tutkimuksen aluksi kartoitetaan nykytilanne ja selvitetään siihen vaikuttavia lähtökohtia. Toiminnan aikana pyritään tekemään interventioita eli vaikuttavia toimenpiteitä ja seurataan ja havainnoidaan niiden vaikutuksia.

ISO/IEC 27001:fi määrittää mallin tietoturvallisuuden hallintajärjestelmän (ISMS; Information Security Management System) kehittämiselle. Tietoturvallisuuden hallintajärjestelmän käyttöönotto on organisaation strateginen päätös. Tämän työn tarkoituksena on helpottaa Keskuspuiston ammattiopiston johtoa tekemään päätöksen tietoturvallisuuden hallintajärjestelmän tarpeellisuudesta ja tarjota standardin mukainen kartoitus tietoturvan nykytilasta organisaatiossa.

Kartoitus tietoturvan nykytilasta tehtiin osallistumalla jokapäiväiseen työntekoon ja havainnoimalla järjestelmien toimintaa. Lisäksi haastateltiin järjestelmätuen edustajia, ohjelmistojen pääkäyttäjiä ja tavallisia käyttäjiä eteenkin asioissa, joista oli vähän tai ei ollenkaan tietoa. Tietoa kerättiin paloittain ja yhdistettiin standardin ISO/IEC 27001:fi liitteessä A esitettyjen valvontavelvoitteiden ja turvamekanismien mukaisessa järjestyksessä. Tulokset havainnoinneista ja haastatteluista on esitetty opinnäytetyön liiteosassa. Epätäydellisten vastauksien kohdalla haettiin lisäselvityksiä toisilta asiantuntijoilta ja käyttäjiltä ja uudistettiin kysely alkuperäiselle vastaajalle kunnes saavutettiin yhtenevät vastaukset. Tällä menetelmällä pyrittiin lisäämään vastausten validiteettia.

## 3.1 Tiedonhaun puitteet

Tietoturvan nykytilan kartoittamista varten tutkija on toimintatutkimuksessa käytetyn tavan mukaisesti osallistunut arkipäivän toimintaan ja havainnoinut toimintatapoja ja merkinnyt ne muistiin. Lisäksi avainhenkilöitä on haastateltu lisäinformaation saamiseksi ja saadun informaation oikeudellisuuden varmistamiseksi.

Työtä varten on haettu tietoa tietoturvallisuuden hallintajärjestelmän toteuttamiseksi toisen asteen kouluorganisaatiossa. Yliopistot näyttävät edis-

tyneen pitkälle tässä pros essissa samoin isot yrit ykset ja valtionhallinto. Perinteiset keskisuuret ja pienet yrit ykset ovat aloittaneet työt hitaasti, mutta suuri joukko varsinkin tietojärjestelmiä tehokkaasti hyödyntäviä uusia yrityksiä, on havainnut tietotu rvallisuuden h allintajärjestelmän välttämättömyyden. Pienet ja keskisuuret or ganisaatiot ovat vasta tulossa m ukaan. Keskuspuiston ammattiopisto on keskisuuri organisaatio.

Yllä mainitut standardit 27001 ja 27002 ovat runkona tiedonhaulle. Standardeissa tie to on hyv in pelkistettyä, joten pe lkästään niide n varas sa toimiminen on puutteellista. Valtionha llinnon VAHTI- sivut tarjoavat m onipuolista neuvontaa tietoturva-asioissa . Ne on suunnattu etupäässä valtion toimintoihin, mutta antavat monissa asioissa asiantuntevaa apua ja neuvoja mille organisaatiolle tah ansa, jop a ta valliselle k otitietokoneen käyttäjälle. Tuoreita yritysmaailman tarpeisiin s uunnattuja kirjoja on saatavilla: Laaksonen et al ja Hakala et al ne uvovat käytännönläheisesti m onien ongelmien ratkaisu issa. Heitä o n käytetty useassa yhtey dessä tässä työssä. STA - KES julkais ut käs ittelevät sos iaalialan ja te rveydenhoitoon liittyv iä tie toturva-asioita. Nämä ohjeet ja käyttäyt ymissäännöt ovat sovellettavissa erityisoppilaitoksen toimintoihin. Lisäksi eri oppilaitoksiin tehtyjen, tietoturvaan liittyvien, opinnäytetöiden lähdelue ttelot antavat oivia vihjeitä hyville lisätiedon hakupaikoille.

Tietoturvan hallintajärjestelmän toimintatavat ovat hyvin sam anlaiset kuin laatukäsikirjan toimintatavat. Laatukäsikirjan toimintaa on te hty tunnetuksi Keskuspuiston ammattiopistossa pitkään. Tätä tuttuusaspektia on tarkoitus hyödyntää tässä työ ssä ja sen esittelyss ä Keskuspuis ton a mmattiopistossa.

Tietoturvan nykytilan kartoitus on suoritettu stand ardin ISO/IEC 27001:ssa ja sen liitteessä A esitettyjen valvontatavoitteiden ja tietoturvamekanismien avulla. N äiden ohjeiden jäädessä vaillinaisiksi on lisäapua haettu standardi ISO/IE C 27002 toteut uksen ohjeistuksista. Varsinainen kartoitus on esitetty liitte essä 1 ja siitä vedetyt johtopäätökset kappaleessa yhteenveto. Liiteo sassa käsiteltävä kartoitus Ke skuspuiston ammattiopiston tietoturvan nykytilasta ja vallitsev ista käytännöistä on vaatinut suuren joukon haastatteluja eri avainhenkilöiltä organisaatiossa. Oikean tiedon esille saam inen on usein edelly ttänyt useamm alta taholta tapahtuvaa tiedonhakua. Haastattelut eivät kuitenkaan ole mitään tutkimusmenetelmällisiä haastatteluja. Ne ovat ainoastaan vallitsevien käytäntöjen selvittelyä.

## 3.2 Käsittelytavat

Kerättyä tietoa on seulottu ja jatkok äsittelyyn sopiva aineistoon on tutustuttu lähemmin. Joukosta on valittu aiheeseen sopivat osat ja hyödynnetty löydettyjä tietoja sopivilta osilta. Mene telmä on ollut osin perinteistä kirjallisuustutkimusta ja osin pohjatie don hankkim ista haastatteluja varten voimassa olevien tietoturvakäytäntöje n selvittäm iseksi. Hava itut puu tteet tietoturvassa on raportoitu eteenp äin organisaatiossa. Sam alla on kerrottu tietoturvan hallintajärjestelmän käyttöönoton eduista.

## 3.3 Raportointitavat

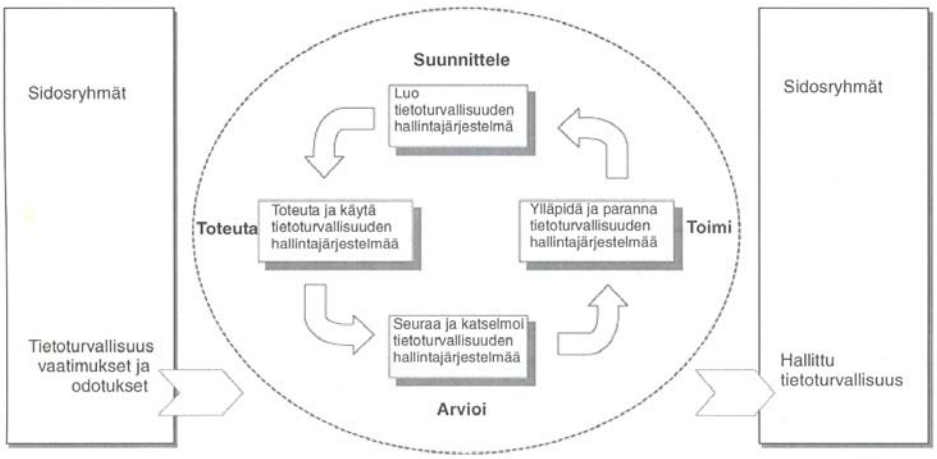
Työn pääraportoin titapa on täm ä ki rjallinen opinnäytetyö. Tutkittavass a organisaatiossa asianomaisia henkilöitä on ra portoitu käytyjen keskustelujen, haastattelujen ja työn välivaiheiden selvittämisen yhteydessä. Työ asetetaan saataville kaikille halukkaille ja annetaan m yös sähköisessä m uodossa.

# 4 TIETOTURVASTANDARDIN TOIMINTAMALLI

Tietoturvallisuutta koskevi en risk ien hallinta o n osa organisaation kokonaisriskienhallintaa ja johtam ista. Riskienhallinnan integroitum inen johtamisjärjestelmiin parantaa olennaisesti organisaation kykyä vastata erilaisiin tietoturva- ja m uihin uhkiin. Ri skejä hallittaessa lä htökohtina ovat organisaation toim innan tavoitteet ja st rategia, kehittäm inen, palveluprosessien varm istaminen sekä henkilöstön osaam inen ja johtam inen. Riskienhallinnan periaatteisiin kuuluu politiikka, hallintaj ärjestelmän käyttöönotto, ylläp itäminen ja päivittäm inen. Politiikan a vulla m ääritellään risk ienhallinnan ta voitteet, org anisointi ja vastuut. Hallintajä rjestelmä toteuttaa organisaation strategiaa ja kattaa k oko tietoturvallisuuden. Tietoturvallisuus tulee sisällyttää osaksi organis aation to imintaprosesseja, jotta se toteutuisi käytännön toiminnassa (Sundberg 2008).

## 4.1 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintaj ärjestelmä on se osa yl eistä toim intajärjestelmää, joka liiketoim intariskien arviointiin perustuen luodaan ja toteu tetaan ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan tavoitteena hyvä tietotu rvallisuus. Hallin tojärjestelmä sisältää organisaatiorakenteen, politiikat, suunnittelutoi menpiteet, vastuut, m enettelytavat, menetelmät, prosessit ja resurss it. Hallin tamallin toteu ttamiselle, käyttämiselle, valvom iselle, katse lmoinnille, ylläpitä miselle ja parantam iselle kannattaa k äyttää prose ssimaista to imintamallia. Täm ä PDCA- m allina tunnettu prosessi on kuvattuna kuvassa 1 (ISO/ICE 27001:fi : 8).




**Kuva 1 PDCA- malli sovellettuna tietoturvallisuuden hallintajärjestelmän prosesseihin**

ISO/IEC 27001 määrittelee kuvan 1 mukaisen tietoturvallisuuden hallintajärjestelmän kehittäm isen jatkuvan parantam isen periaatteen ns. PDCA – mallin. Malli tulee sanoista Plan, Do, Check, Act tai SFS:n käännöksenä suomeksi Suunnittele, Toteuta, Arvioi , Kehitä. Sen ylläpito ja kehittäm issykliin kuuluu hallintajärjestelmän rakentam inen (Plan), s en toim eenpano

ja noudattaminen (Do), seuranta ja katselmointi (Check) sekä ylläpito ja kehittäminen (Act). Tämä sykli edellyttää aktiivista toimintaa ja sen on tarkoitus johtaa jatkuvaan parantamiseen(VAHTI 3/2003: 16–18).

### 4.1.1 Tietoturvallisuuden hallintajärjestelmän luominen ja johtaminen

Organisaation on pyrittävä suojaamaan tietonsa niin, että tietoturvallisuuden perusvaatimukset (saatavuus, eheys, luottamuksellisuus) säilyvät. Erilaisissa toiminnoissa tietoturvallisuuden perusvaatimusten tärkeys vaihtelee huomattavasti. Tietoturvallisuutta suunniteltaessa on tunnettava organisaation nykytilanne, sen vahvuudet ja heikkoudet sekä järjestelmät, joiden avulla kriittistä tietoa käsitellään. Luonnollisesti kriittinen tieto on ensin tunnistettava (Laaksonen, 2006:116).

Toimivan tietoturvallisuuden perustana on täsmällinen johtaminen sekä tietoturvallisuuden liittäminen tiiviisti organisaation varsinaiseen liiketoimintaan. Johtamisen sanotaan olevan kykyä motivoida ja opettaa. Tämä pätee hyvin myös tietoturvallisuuden johtamiseen. Tietoturvasta vastaavilla tahoilla tulisikin olla tämä kyky. Sellaiset tietoturvatoimenpiteet, jotka eivät perustu liiketoimintaan, tulee suunnitella ja harkita erityisen tarkasti, sillä niiden tuoma lisäarvo tietoturvallisuuteen ei välttämättä ole kustannusten arvoinen. Toisaalta jotkut asiat tulee tehdä riippumatta siitä, onko niistä liiketoiminnan kannalta välitöntä hyötyä. Tällaisia asioita ovat muun muassa ulkoiset vaatimukset kuten lakien edellyttämät toimenpiteet (Laaksonen, 2006:116).

Liiketoiminnan ja tietoturvallisuuden tavoitteiden harmonisointi kannattaa, sillä tämä vaikuttaa muun muassa resurssien jakamiseen, toiminnan mittaamiseen ja seurantaan. Resurssien käyttöä voidaan tehostaa esimerkiksi laajentamalla laatuorganisaation tehtäväkenttää ulottumaan osaltaan tietoturva-asioihin ja yhdistämällä muihin prosesseihin tietoturvallisuuden toteutumisen kannalta merkityksellisiä elementtejä ja tietoturvamekanismeja. Jotta organisaatiosta kuvan siitä, miten laaja johtamisjärjestelmä tietoturvallisuuden hallinnointiin tulee rakentaa, organisaation on syytä pohtia seuraavia asioita. Minkälaista tietoa organisaatio käsittelee ja voiko jokuhyötyä organisaation tiedoista tai hyötyykö joku sen muuttamisesta? Onko tiedon tuottaminen vaatinut suuria taloudellisia tai muita panostuksia ja miten vaikeata ja kallista tiedon tuottaminen uudestaan on? Onko joku kiinnostunut organisaation tiedoista ja miten tämä pyrkii tietoon käsiksi? Olisi hyvä myös pohtia miten tietoa voidaan viedä organisaatiosta ulos ja minkälaisia tapoja tiedon havittelijat käyttävät? (Laaksonen, 2006:118)

Syytä on pohtia kuinka laajaa ja monimuotoista organisaation toiminta on, ja miten monimutkainen nykyisin käytössä oleva johtamisjärjestelmä on, voidaanko tietoturvan johtaminen yhdistää nykyiseen johtamisjärjestelmään? Lisäksi on hyvä ennakoida millainen organisaation ulkoinen vaatimusympäristö ja miten sen uskotaan kehittyvän ja miten organisaation tulee vastata ulkopuolelta tuleviin tietoturvavaatimuksiin tai onko organisaa-

tiolla käsitystä sitä velv oittavista yleisestä lain säädännöstä tai erityisvelvoitteista tai -oikeuksista? (Laaksonen, 2006:119)

Hyvän tietohallintotavan taustalla on ajattelutapa kokonaisvaltaisesta informaatio teknologian hyödyntäm isestä organisaatiossa. T unnusomaista tällaiselle ajattelutavalle on organisaation eri yksiköiden tarpeen ja toimintojen kartoittam inen, arvioim inen ja priorisointi. Lisäksi hyv ään tietohallintotapaan kuuluu to iminnan organisointi, vastu un jakam inen ja tiedottaminen erilaisista ratkaisuista, joihin tietohallinto on päätynyt. Kokonaisvaltainen hallintotapa tarvitsee erilaisiin osa-alueisiin soveltuvia menetelmiä ja toim intatapoja. Tietoturvallisuus on yksi osa hyvä ä tietohallintotapaa. Yrityksen ylimm än johdon tulisi hyvää tietohallintotapaa käsitellessään pohtia esim erkiksi sitä, onko yr ityksen johdossa riittävässä m äärin tietotekniikkaosaamista. Kaikkien o rganisaation johta jien tulisi tietää ja ymmärtää organisaation merkittävämmät tietoturvariskit ja vastaavasti tietotekniikasta ja tietotur vallisuudesta vastaavien ta hojen tulisi ymm ärtää opetustoiminta strategia ja sen va ikutukset. Näiden kahden tahon yhteensovittamisella ja siihen liittyvällä koulutuksella organisaatiolla on mahdollisuus saada opetustoiminnan kannalta m aksimaalinen hyöty tietojärjestelmistään. Opetustoiminnan tulee määrittää ja kommunikoida tieto järjestelmille as ettamansa vaatim ukset, muk aan lukien tieto turvavaatimukset. Organisaation risk ienhallinnan per iaatteiden ja m enetelmien tulee ka ttaa myös tie totekniikka ja - turvallisuus ja organisaa tion p rojektinhallintajärjestelmien ja -käy täntöjen tulee katt aa myös tietotekniikkaprojektit. Edelleen hyvää tietohallintata paa pohdittaessa tulee selv ittää, onko yrityksen tietohallintostrategia määritelty ja hyväksy tty niin tietohallinnon kuin organisaatiojohdon toim esta ja onko tiet ohallinnon- ja turvallisuuden operointi ja valvonta/hallinta erotettu to isistaan ja vastuut selkeästi m ääritetty ja kommunikoitu (Laaksonen, 2006:123–124).

Tietoturvallisuuden hallintajärjestelmän toimintaa on seurattava ja kerättävä tietoa sen toim innan tehokkuudesta. Jatkuvaa suunnitelmien ja käytän teiden tarkastelua kutsutaan m yös sisäiseksi auditoinniksi. Toiminnan onnistumista arvioidaan säännöllises ti, vähintään vuosittain. Tarkastelussa verrataan, onko järjestelm ä edelleen tietoturvapolitiikan ja m ääriteltyjen tavoitteiden m ukainen ja m issä l aajuudessa suunnitellu t tietoturvam ekanismit on otettu käyttö ön. Tavoitteena on antaa organisaation johdolle työkalut arvioida, ovatko turvallisuutta ylläpitävät tekniset ratkaisut ja vastuullisten toim inta olleet tavoitteis iin nähden riittäviä. Seuranta koostuu menettelytavoista ja tu rvamekanismeista, jo iden avulla pyr itään hava itsemaan tietojenkäsitte lyn virhe et m ahdollisimman pian. Seu rannan avu lla pyritään myös havaitsemaan tietoturvaloukkaukset ja rikkomukset samoin kuin tunnistam aan tietoturvan loukkausy ritykset ja m uut tietoturvallisuuteen vaikuttavat tapahtum at. Samalla mitataan tietoturvamekanismien toimivuutta suhteessa tie toturvallisuustarpeisiin ja tallennetaan tapahtum at, joilla on vaikutusta tietoturvallisuud en hallintajärjestelm än toim ivuuteen ja suorituskykyyn. (Hakala 2006:110)

Tietoturvallissuden ylläp itäminen edelly ttää suu nnitelmaa ja käytänte iden jatkuvaa ja säännöllistä ta rkastelua. Tarkastelua suoritetaan sekä tietotur-

vallisuuden hallintajärjestelmästä vastaavassa prosessissa että organisaation ylimmässä johdossa. Tarkastelun kohteena on sekä tietoturvallisuuden hallintajärjestelmän tehokkuus että suunnittelun lähtökohtien ajanmukaisuus. Järjestelmän tehokkuutta arvioidaan turvallisuuskatselmusten, eitoivottujen tapahtumien raportoinnin sekä henkilökunnan ja sidosryhmien antaman palautteen avulla. Tarkastelussa on kiinnitettävä huomiota tietoturvapolitiikan ja sen tavoitteiden mukaiseen toimintaan sekä siihen, missä laajuudessa suunnitellut tietoturvamekanismit on otettu käyttöön. (Hakala 2006:110)

Suunnittelun ajanmukaisuutta on syytä arvioida säännöllisesti ja silloin, kun toimintaympäristössä tai tekniikassa tapahtuu oleellisia muutoksia. Ajanmukaisuuden arvioinnissa avainasemassa on riskienhallinta. Siinä joudutaan pohtimaan muutosten vaikutusta riskien tunnistamiseen, hyväksyttävän riskin määrittelyyn tai tunnistettuihin jäännösriskeihin. Tarkastelussa kiinnitetään huomiota seuraaviin toimintaympäristön muutoksiin:

- organisaatiomuutokset
- tekniikassa tapahtuneet muutokset
- lainsäädännössä ja sopimuksissa tapahtuneet muutokset
- yhteiskunnallisen ilmapiirin muutokset
- tunnistettujen uhkien muutokset
- käytettyjen tietoturvamekanismien muutokset. (Hakala 2006:110 - 111)

Tietoturvallisuuden hallintajärjestelmää on arvioitava jatkuvasti. Päivittäisen teknisen seurannan lisäksi tietoa järjestelmän toiminnasta voidaan kerätä sisäisten katselmusten avulla. Niitä on järjestettävä säännöllisesti ja hyvissä ajoin ennen muita tarkastelutapahtumia. Seurannan, katselmusten ja tarkastelukierrosten tuloksena syntyneet havainnot edellyttävät turvasuunnitelmien päivittämistä. Sen suorittaminen on sitä helpompaa, mitä paremmin havainnot on dokumentoitu. (Hakala 2006:110)

Tietoturvallisuuden tila kehittyy, kun organisaation työntekijät kaikilla hierarkiatasoilla noudattavat tietoturvaohjeita ja käsittelevät tietoa yhteisesti sovittujen tapojen mukaisesti, ja teknisillä suojauksilla varmistetaan, että tietojärjestelmät prosessoivat ja suojaavat tietoa oikein. Kun organisaatio voi varmistua tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta, sen toimintataso kehittyy muutenkin kuin tietoturvan osalta.

Tietoturvallisuuden hallintajärjestelmän valvonta ja katselmointi tuottavat tietoa järjestelmän kehittämistarpeista. Ne toteutetaan joko korjaavilla tai ehkäisevillä toimenpiteillä. Korjaavat toimenpiteet pyrkivät poistamaan ristiriitoja toiminnan ja sitä ohjaavien määritysten välillä. Tietoturvan hallintajärjestelmän kannalta tärkeimmät määritykset ovat organisaation tietoturvapolitiikka, tietoturvan hallintajärjestelmän politiikka sekä noudatettavat standardit. Ehkäisevät toimenpiteet puolestaan pyrkivät torjumaan potentiaaliset ristiriitojen aiheuttajat. Molempia toimenpiteitä pohdittaessa tarvitaan dokumentoituja menettelytapoja, joilla selvitetään, miten ristiriidat tunnistetaan ja mitkä niiden syyt ovat. Sen jälkeen arvioidaan toimen-

piteiden tarve ja niiden mahdollinen toteutustapa. Samoin dokumentoidaan vaikutusten kirjaamis- ja tarkastelutavat. (Hakala et al 2006: 113)

### 4.1.2 Dokumentointia koskevat vaatimukset

Tietoturvallisuuden hallintajärjestelmä edellyttää runsaasti eritasoista dokumentointia. Osa dokumenteista on selkeitä asiakirjamuotoisia kuvauksia järjestelmän toimintaan liittyvistä käytänteistä ja toimintaa ohjaavista tavoitteista. Seurantatiedot puolestaan ovat luonteeltaan sellaisia, ettei niiden tallentaminen perinteisinä asiakirjoina ole järkevää. Ne tallennetaan yleensä lokitiedostoihin ja hallintasovellusten tietokantoihin (Hakala, 2006: 112).

Asiakirjojen ohjaus ohjaa tietoturvallisuuden hallintajärjestelmän dokumenttien tallentamista. Hallinnan kuvauksessa määritellään prosessit asiakirjojen laatimiselle, muuttamiselle, tarkastamiselle, hyväksymiselle ja julkaisemiselle (Hakala, 2006: 113).

Riittävän yksityiskohtainen ja sovittua rakennetta noudattava dokumentointi on kaiken tietoturvallisuutta ylläpitävän toiminnan ja edistävän toiminnan ehdoton edellytys. Dokumentointi helpottaa myös kaikkea muuta tietojärjestelmiin liittyvää toimintaa: teknistä ylläpitoa, tietojenkäsittelyä ja tietohallintoa. Valitettavan usein se on kuitenkin laiminlyöty. Dokumentteja organisaation tietojärjestelmistä ei ole, ne ovat liian yleisluonteisia tai niihin ei ole kirjattu järjestelmiin tehtyjä muutoksia. Dokumenttien puutteellisuutta perustellaan usein ajan puutteella: dokumentteja ei ole laadittu tai ylläpidetty, koska kaikki aika on kulunut järjestelmän ylläpidon vaatimiin rutiineihin. Puutteellisten dokumenttien aiheuttama selvitystyö, esimerkiksi järjestelmäpäivityksen tai järjestelmän avainhenkilön vaihdon yhteydessä, vie yleensä moninkertaisen ajan verrattuna varsinaisen dokumenttien laatimiseen. Dokumentoinnin vaatima aika on otettava todenmukaisesti huomioon suunnittelussa ja johdon keskeisiä tehtäviä on tarkistaa dokumentoinnin valmistuminen. Tietojärjestelmädokumenttien laatiminen on suhteellisen helppoa, jos organisaatiossa on sovittu yhtenäisestä dokumenttikäytännöstä ja henkilökunta on koulutettu dokumenttien laatimiseen ja niiden versioimiseen (Hakala, 2006: 32).

Tallenteiden ohjauksessa tulee määritellä prosessit miten asiakirjat tunnistetaan, suojataan, säilytetään ja miten kauan, miten ne löydetään ja hävitetään säilytyksen jälkeen ja varmistetaan, että asiakirjat pysyvät käyttökelpoisina ja tunnistettavina määritellyn ajan (Hakala, 2006: 113).

Pelkkä dokumenttien olemassaolo ei takaa dokumentoinnin toimivuutta. Ne pitää tallentaa joko paperille tai sähköisessä muodossa ja niiden on oltava nopeasti ja ainoastaan auktorisoitujen henkiöiden käytettävissä. Lisäksi on oltava menetelmä, jonka avulla voidaan varmistaa, että käytössä on dokumentin viimeisin hyväksytty versio. Tarvittaessa on oltava valmius tarkastella dokumentin aiempaa versiota. Esimerkki: Uuden ohjelmistoversion käyttöönoton yhteydessä dokumentointia muutetaan, mutta vasta vuoden käytön jälkeen järjestelmässä havaitaan vakava virhe ja joudutaan

palaamaan aikaisempaan ohjelmistoversioon. Ohjelmiston palauttamisessa aikaisempaan versioon vanha dokum entointi on kullan arvoinen (Hakala, 2006: 37).

## 4.2 Turvallisuuspolitiikka

Johdon toim iminen es imerkkinä on ratkaisevan tärkeätä henkilöstön sitouttamisessa tietoturvallisuustoimintaan. Hyvät ja toim ivat johtamistavat yhdistettynä haluun lisätä tietoturval lisia toimintatapoja ja kykyyn toim ia itse esimerkkinä muille luovat o tollisen ilmapiirin tietoturvallisen toiminnan olemassaololle ja kehitykselle. Toiminta organisaatiossa on perustuttava tarkasti m ääritetyille ja hyväksytyille toim intaperiaatteille ja käytännöille. Organisaa tiossa on oltava julkais tu tie toturvapolitiikka, nim etty turvahallinto, jonka jäsenten roo lit ja vastuut on määritelty. Koko henkilöstön on oltava tietoinen tästä tie toturvapolitiikasta, määritellyistä tie toturvallisuustavoitteista ja hyväksytyist ä toim intatavoista. Kaikki täm ä on dokumentoitava kirjallisesti, selkeästi ja kattavasti ja saatettava henkilöstön tietoisuuteen (Tammisalo, 2005: 26).

Turvallisuudesta vastuussa olevan tahon on tunnistettava ja hallittava riskit ja suojattava koko organisaatio, sen toim inta ja om aisuus riskeiltä ja niiden aiheuttamilta vahingoilta. Turvaorganisaation täytyy seurata tekniikan kehitystä ja pitää itsensä ajan ta salla, koska nykyteknologia m uuttuu ja kehittyy jatkuvasti vaikeuttaen uhkien ja r iskien torjuntaa ja niiltä suo jautuminen m onimutkaistuu. Tietoturvato iminnasta tiedo ttaminen ja p alautteen antam inen sekä tiet oturvaorganisaatiolle e ttä koko henkilöstölle on tärkeää, vaikka tieto turvaloukkauksia ei olisikaan havaittu. Positiiv inen palaute edesauttaa turvallisuustietoisuutta ja parantaa turvallisuutta, koska se kertoo, että toiminta on ollut tuloksellista (Tammisalo, 2005: 26).

Tiettyjä oletuksia kanna ttaa turvahallinnon tehdä liittyen ympäristön, organisaation ja järjestelmien toimintaan. Näitä oletuksia voidaan pitää väistämättöminä tapahtumina, joita s attuu jossain määrin kaikissa organisaatioissa koulutuksesta ja opastuksesta huolim atta. Nä mä ovat osa jokapäiväistä toimintaa, joihin aina liittyy tietty risk i. Kyseessä voi olla toden näköinen tapahtuma tai ympäristöön liitt yvä riski. Tyypillisiä oletustapahtumia ovat esim erkiksi, että loppukäyttäjät tekevät huolim attomuusvirheitä ja etteivät he omaksu kaikkia toim intatapoja ja ohjeita vaan koettavat oikaista hankalaksi kokem issaan kohdissa. Tai että verkkohyökkäyksiä tehdään ja että järjestelmissä on virheitä ja toimintahäiriöitä. Usein myös oletetaan, että kaikki ulko inen tietoliikenne on suojattu palom uurilla, vaikkei näin todellisuudessa olisikaan (Tammisalo, 2005: 26).

### 4.2.1 Tietoturvapolitiikka

Tietoturvasuunnittelun yhtenä tavoitt eena on luoda organi saatiolle tie toturvapolitiikka. Siinä kerrotaan tietoturvallisuuden strategiasta, toteutusperiaatteista, organisoinnista ja toim intatavoista, jotka ylin johto on hyväksynyt ja joita organisaat iossa pyritään toteuttam aan. Tietoturvapolitiikka

on dokumentti, joka tarjoaa samalla johdon tuen tietoturvallisuudelle ja ohjaa määriteltyyn tietoturvatasoon pääsemistä, sen ylläpitämistä ja kehittämistä. Tietoturvapolitiikka sisältää vain julkista tietoa. Se on julkinen dokumentti, joka julkaistaan henkilöstön, asiakkaiden ja tärkeimpien sidosryhmien käyttöön. Se pitäisi kirjoittaa niin, että kaikki ymmärtävät selkeästi sen sisällön (Hakala, 2006:7).

Tietoturvapolitiikassa voidaan määritellä organisaation käytäntö myös yksittäisessä liiketoimintaprosessissa tai liiketoiminnan kannalta erityisen tärkeässä järjestelmässä. Liitteissä voidaan kuvata tarkemmin näitä käytänteet ja tekniset ratkaisut, joilla turvallisuustavoitteisiin pyritään sekä menettelyt ongelmien ilmetessä. Ne ovat luonteeltaan yleensä joko salaisia tai luottamuksellisia. Tietoturvallisuuden yksityiskohdat kuvataan kuitenkin tietoturvasuunnitelmassa. Tietoturvallisuuspolitiikan ajantasaisuus arvioidaan säännöllisin väliajoin, jotta se vastaisi toiminnassa ja ympäristössä tapahtuneita muutoksia. Näin tietoturvapolitiikka toimii samalla myös johdon apuvälineenä tietoturvallisuusperiaatteiden toteutumisen valvonnassa ja kehityssuunnitelmissa (Hakala, 2006:8).

### 4.2.2 Tietoturvapolitiikan määrittelyasiakirjat

Johdon on hyväksyttävä tietoturvapolitiikan asiakirja, julkaistava se ja tuotava se kaikkien työntekijöiden ja asianmukaisten ulkopuolisten osapuolten tietoisuuteen. Tietoturvapolitiikan asiakirjan on julistettava johdon sitoutuminen tietoturvaan ja tiedottaa organisaation lähestymistavasta hallinnoida sitä. Politiikan on minimivaatimusten mukaan käsiteltävä ainakin tietotekniikan käyttökäytäntöjä, tiedon turvaamiskäytäntöjä, palomuurikäytäntöjä, etäkäyttökäytäntöjä, ylläpitäjien käyttökäytäntöjä ja tietojärjestelmien ylläpitokäytäntöjä (Guel 2007: 30).

### 4.2.3 Tietoturvapolitiikan katselmointi

Tietoturvapolitiikka on katselmoitava suunnitelluin aikavälein tai suurten muutosten yhteydessä. Tällä varmistetaan tietoturvapolitiikan jatkuva soveltuvuus, asianmukaisuus ja vaikuttavuus.

## 4.3 Riskien hallinta

Tietoturvallisuus on osa organisaation johtamistoimintaa. Jokaisen organisaatiotason tehtävänä on huolehtia oman organisaationsa toiminnan ja hankkimiensa palvelujen tietoturvallisuudesta, määritellä tarvittavat periaatteet sekä laatia ja antaa tarvittavat ohjeet. Tietoturvaratkaisujen valinnassa tulee riskianalyysien perusteella ottaa huomioon ratkaisujen taloudellisuus ja tarkoituksenmukaisuus. Ylimmän johdon päätöksiä tarvitaan erityisesti silloin, kun ratkaisut on valittava taloudellisuusvaatimuksista poiketen (VAHTI 1/2001: 8).

### 4.3.1 Riskikartoitus

Dokumentoinnin ollessa puutteellista, riskikartoitus kannattaa tehdä mielekarttojen avulla. Riskikartoituksessa on syytä tarkastella sekä nykytilannetta että tulevaisuuden mukanaan tuomia uhkakuvia. Mitä laajemmin organisaation eri henkilöryhmät osallistuvat kartoitukseen, sitä parempia tuloksia on odotettavissa. Jotta kaikki potentiaaliset riskit ja uhkakuvat tulisivat huomioiduiksi, tarvitaan sekä tietojenkäsittelyn ammattilaisten ja johdon että tietojärjestelmien käyttäjien asiantuntemusta (Hakala, 2006:80).

Lähtökohdaksi kannattaa ottaa tiedot esiintyneistä ongelmista. Tietojärjestelmien käyttäjät muistavat yleensä hyvin kaikki vakavat vahingot, joita vuosien aikana on tapahtunut heidän työssään. Nämä tilanteet kirjataan ylös ja sijoitetaan riskiluokituksen kriteerien perusteella oikeaan luokkaan. Seuraavassa vaiheessa pyritään hakemaan potentiaalisia riskejä: vahinkoja, ongelmia ja tapahtumia, joita ei vielä ole syntynyt, mutta joita kartoittajat pitävät mahdollisina. Ne sijoitetaan samalla tavalla oikeisiin riskiluokkiin. Lopuksi luodaan katseet tulevaisuuteen ja yritetään hakea tekniikan ja toimintaympäristön mahdollisista muutoksista aiheutuvia uhkakuvia. Uhkakuvat sijoitetaan nekin riskiluokitukseen, mutta ne on syytä merkitä siten, että ne erottuvat selkeästi nykyhetken riskeistä (Hakala, 2006: 80–81).

Ennen tietojärjestelmäkohtaisten riskikartoitusten suorittamista on järkevää tehdä yleinen riskikartoitus. Sen avulla etsitään yleisluontoiset riskit ja uhkakuvat, jotka voivat uhata tietoturvallisuutta missä tahansa tietojärjestelmässä. Tämän kartoituksen tekijöiden valinnassa kannattaa pyrkiä mahdollisimman edustavaan poikkileikkaukseen organisaation henkilökunnasta. Yleisen riskikartoituksen tekemisessä mielekartat ovat oivallinen apuväline. Niiden avulla eri henkilöiden mieliin juolahtavat riskit ja uhkakuvat saadaan koottua samaan dokumenttiin ja ne voidaan nopeasti järjestää riskiluokituksen mukaisesti (Hakala, 2006:81).

Kun tietojärjestelmille yhteiset riskit on löydetty, voidaan lähteä hakemaan tietojärjestelmäkohtaisia riskejä ja uhkakuvia. Yleistä riskikartoitusta voidaan käyttää tarkistuslistana tietojärjestelmää tutkittaessa. Tietojärjestelmäkohtaisessa kartoituksessa saatetaan löytää riskejä, joita yleisessä kartoituksessa ei löytynyt. Jotkut yleiset riskit saattavat puolestaan olla sellaisia, ettei niitä esiinny tutkittavassa tietojärjestelmässä. Jos tietoturvasuunnittelu ei kata organisaation kaikkia tietojärjestelmiä, on muita järjestelmiä kartoitettava ainakin siltä osin kuin ne aiheuttavat riskejä tarkasteltaville järjestelmille. Tämä tarkoittaa ennen muuta tietojen siirtämiseen liittyviä riskejä. Tietojen siirto muihin järjestelmiin voi aiheuttaa riskin luottamuksellisuudelle. Tietojen siirto muista järjestelmistä voi taas vaarantaa tiedon eheyden ja käytettävyyden (Hakala, 2006:81).

### 4.3.2 Riskien arviointi ja tietoturvallisuuden testaaminen

Tietojärjestelmää uhkaavien riskien tultua selvitetyiksi, alkaa riskien arviointi. Arvioinnin keskeisinä kohteina ovat riskien vaikutukset organisaation toimintaan ja riskien realisoitumisen todennäköisyys. Vaikutusten arvioinnissa tietojärjestelmän sisältämät tiedot sijoitetaan tietojen luokitusjärjestelmään. Tämä toimii lähtökohtana pohdittaessa, kuinka vakavia vahinkoja eheys-, käytettävyys- ja luottamuksellisuusriskit voivat aiheuttaa organisaatiolle. Vahinkojen vakavuutta ja tapahtumien todennäköisyyttä tarkastellaan samanaikaisesti. Mitä suurempaa vahinkoa riskin toteutuminen aiheuttaa ja mitä todennäköisempää riskin toteutuminen on, sitä enemmän riskiin on varauduttava (Hakala 2006: 81).

Riskienhallinnan tavoitteena on havaita ja hallita organisaation toimintaan mahdollisesti kohdistuvia ei-toivottuja tapahtumia eli riskejä. Tietoturvallisuuden testaamisen tavoitteena puolestaan on havaita tietoturvaheikkoudet tai toteutettujen suojaustoimenpiteiden toimivuus ja mahdolliset puutteet toiminnassa. Tarkastelu voidaan kohdistaa hallinnollisiin tai teknisiin tekijöihin tarkastuksen kohteista riippuen (Hakala, 2006:150).

ISO/ICE 27001:fi -tietoturvastandardin mukaan organisaatiolla tulee olla yhteisesti päätetty ja hyväksytty tapa suorittaa riskienarviointi ja tietoturvallisuuden testaaminen. Oleellista ei välttämättä ole se, miten testaaminen suoritetaan, kunhan se suoritetaan johdonmukaisesti ja kattavasti samoja menetelmiä käyttäen. Oleellista on huomata, että auditoijan ei tule tarkastaa omaa työtään. Tietoturvapäällikkö ei voi samanaikaisesti toteuttaa tietoturvallisuuden dokumentaatiota ja auditoida sen kattavuutta. Riskien arviointi ja tietoturvallisuuden testaaminen tulee olla säännöllistä, ja sille tulee olla sovittu aikataulu, kohteet ja vastuulliset suorittajat. Analyysin tulee myös johtaa toimintaan, mikäli tähän on aihetta. Tietoturvallisuuden testaaminen ilman korjaavien toimenpiteiden toteuttamista on todellaresurssien tuhlausta (Hakala, 2006:150).

### 4.3.3 Riskienhallinnan keinot

Riskienhallinnan ensimmäinen vaihe on uhkien tunnistaminen. Kun uhkat on tunnistettu ja niiden toteutumisen todennäköisyys ja seurausten vakavuus arvioitu, voidaan suunnitella ja päättää toimenpiteistä riskien hallitsemiseksi. Riskejä voidaan hallita monin keinoin. Keskeisiä toimintavaihtoehtoja ovat esimerkiksi riskin välttäminen. Tämä on usein mahdollista vain, jos ko. toiminnasta pidättäydytään kokonaan. Riski voidaan poistaa, yksittäinen riski voidaan mahdollisesti poistaa kokonaan. Poistaminen saattaa kuitenkin aiheuttaa uusia riskejä. Riski voidaan pienentää. Ensisijaisesti on pyrittävä estämään vahinkojen syntyminen tai vähentämään niiden seurauksia. Riskin seurausten pienentämiseksi voidaan erilaisilla kontrolleilla pyrkiä vähentämään seurausten vakavuutta tai tapahtuman todennäköisyyttä. Riski voidaan siirtää esimerkiksi sopimuksin tai vakuuttamalla tai riskin voidaan pitää omalla vastuulla. Osa riskeistä joudutaan tai kannattaa pitää omalla vastuulla. Tällöin otetaan tietoinen riski siitä, että uhka voi toteutua

Toimet riskien pienentämiseksi voivat olla mm teknisiä toimenpiteitä, kuten uudet laite- tai työtilaratkaisut, konesuojauksen kehittäminen, tekniset varmistukset, hälytinjärjestelmät tai huollon ja kunnossapidon parannukset. Ne voivat myös olla organisaation toimintaan liittyviä toimenpiteitä, kuten yhteisistä pelisäännöistä sopiminen, toiminta ohjeiden laatiminen, valvonnan tai seurannan kehittäminen, tiedonkulun ja työnsuunnittelun parantaminen tai vastuista sopiminen tai yksilöiden toimintamahdollisuuksia parantavia toimenpiteitä, kuten uusien työvälineiden hankinta, ohjeistus, perehdyttäminen ja koulutus, uudet työaika- tai työparijärjestelyt. Kaikkia riskejä ei voida poistaa. Riskienhallintatoimenpiteet on syytä aloittaa suurimmiksi arvioiduista riskeistä ja ulottaa niin laajalle kuin mahdollista. Riskienhallintaan liittyy aina arvioinnit toimenpiteiden kustannuksista. On mietittävä kuinka paljon vakuuttamiseen ja erilaisiin riskiä pienentäviin toimenpiteisiin voidaan taloudellisesti panostaa (VAHTI 7/2003).

## 4.4 Johdon vastuu

Hallinnollinen tietoturvallisuus on määritelty Valtiovarainministeriön julkaisussa VAHTI 6/2003 tavalla, joka sopii kouluorganisaatiolle hyvin. Tietoturvallisuuden johtamistoiminto on organisaation koko tietoturvatoiminnan lähtökohta. Se muodostuu johdon hyväksymistä periaatteista, vastuunjaosta, tarkoitukseen varatuista resursseista sekä riskien arvioinnista. Varsinaiset toimenpiteet perustuvat hallinnollisiin ohjeisiin, joiden pohjana toimivat johdon määrittelemät periaatteet. Ilman kunnollista tietoturvaperiaatteiden luomista, hallinnointia ja suunnittelua turvallisuusjärjestelyt saattavat sisältää suuria puutteita tai ne voivat olla suunnattu vääriin asioihin.

Hallinnollisen turvallisuuden tarkoituksena on luoda organisaatioon tietoturvalliset toimintatavat. Toimintamallien pohjalta luodut henkilöstön koulutusjärjestelyt sekä ohjeistus-, valvonta- ja tarkastusmenettelyt ovat välttämättömiä tietoturvallisuuden kehittämiseksi ja ylläpitämiseksi.

Hallinnollisessa turvallisuudessa on oleellista, että käyttäjät tietävät ja ymmärtävät ne periaatteet, joille organisaation tietoturvallisuus rakentuu. Tätä varten organisaation johdon tulee julkaista organisaation tietoturvapolitiikka. Politiikka jaetaan koko henkilökunnalle. Tietoturvapolitiikan tueksi tulee suunnitella organisaation ohjekokonaisuus ja määritellä vaadittu tietoturvakuvausten taso. Lisäksi laaditaan tietoturvasuunnitelmat, jotka osoittavat organisaatiolle elintärkeät tietojärjestelmät, niiden toipumistoimet sekä vaatimukset poikkeusolojen valmiudelle.
Käyttäjille oleellisia asioita hallinnollisessa turvallisuudessa ovat organisaation tietoturvapolitiikka ja –periaatteet, tietoturvavastuiden jako työjärjestyksissä ja tehtäväkuvauksissa, tietoturvaohjeiden laatu, kattavuus ja niiden koulutus ja allekirjoitetut vakuutukset turvaohjeiden lukemisesta ja noudattamisesta

Käyttäjän tulee olla tietoinen ohjekokonaisuudesta ja erityisesti niistä ohjeista, jotka säätelevät hänen omaa työtänsä. Lisäksi organisaation tieto-

turvavastuut tulee olla selkeästi määriteltynä ja kirjoitettuna muistiin. Käyttäjiä koskevat vastuut tulee kouluttaa ja ohjeistaa, jotta jokainen käyttäjä on tietoinen omista tietoturvavastuista ja pystyy toimimaan vastuunedellyttämällä tavalla. Koulutus tulee aloittaa jo uuden työntekijän perehdytyskoulutuksessa. Käyttäjän tulee myös tietää, kuka on organisaation tietoturvallisuudesta vastaava henkilö.

### 4.4.1 Johdon sitoutuminen

Tietoturvapolitiikka on organisaation julistus, jolla se suojelee omistamaansa eri muodoissa olevaa tietoa. Hallinnolliseen tietoturvaan liittyy keskeisenä osana johdon sitoutuminen julistamansa tietoturvapolitiikan noudattamiseen. Ilman johdon ilmoittamaa sitoutumista tietoturvapolitiikkaan ei voida olettaa kenenkään muunkaan sitä noudattavan.

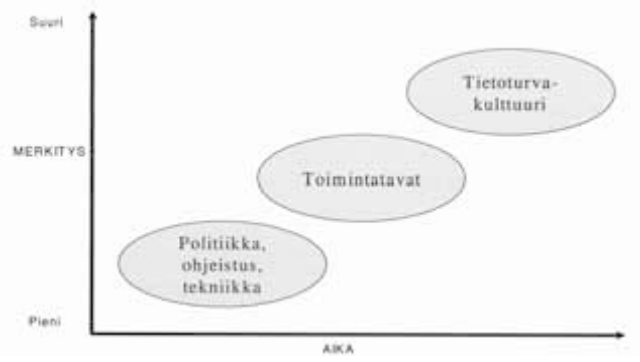
### 4.4.2 Resurssien hallinta

Selvitetään organisaatiolla olemassa olevat resurssit: talous, henkilöstö, laitteistot ja ohjelmistot. Jos resurssit eivät riitä tietoturvapolitiikan toteuttamiseen, määritellään lisäresurssien määrä ja laatu. Luopuminen tarpeellisten lisäresurssien käytöstä saattaa tulla jossakin vaiheessa kalliiksi.

Budjetoinnissa ja sen suunnittelussa on otettava huomioon ainakin seuraavat kohdat:

- Henkilöresurssit ja työntekijöiden tietoturvan hoitoon käyttämä aika
- Tietoturvan hoidossa tarvittavat työkalut, kuten ohjelmistot, laitteistot, tilat ja muut tarvikkeet
- Aineettomat resurssit, kuten koulutus, osaamisen ylläpitäminen ja koulutusmateriaalin tuottaminen (Tammisalo 2007: 34).

Kuva 2 esittää, kuinka tietoturvakulttuurin kehittäminen on pitkä jänteistä työtä ja muutokset näkyvät hitaammin kuin toimintamallien tai teknisten ratkaisujen aiheuttamat muutokset. Toisaalta tietoturvakulttuurin kehittämisen kautta saadaan pysyvämpiä tuloksia (VAHTI 5/2004: 21).




**Kuva 2 tietoturvakulttuurin luominen**

Tietoturvapolitiikka ja -ohjeet luovat rungon henkilöstön toimintatavoille. Nämä ohjeet muodostavat organisaation hyväksymän turvallisuuteen liittyvän käyttäytymismallin, johon vaikuttavat ohjeiden kattavuus, selkeys ja yhdenmukaisuus. Eteen tulevat tilanteet pyritään hoitamaan organisaatiossa vallitsevan käytännön mukaan. Turvallisuuden kannalta rutiinien suorittamiseen vaikuttavat johtajien ja muun henkilöstön esimerkkien lisäksi kirjallisten ohjeiden ja käytännön toimintatapojen yhdenmukaisuus sekä se, ovatko yrityksen muut toimintamallit, esimerkiksi tiedotusten tai henkilöstön rekrytointiin liittyvät käytännöt, sopusoinnussa tietoturvaohjeiden kanssa (Laaksonen et al 2006: 249).

Ohjeistusta laadittaessa kannattaa pyrkiä mahdollisimman yksinkertaiseen ja helposti ymmärrettävään tekstiin. Mikään ei pilaa ohjeiden merkitystä niin tehokkaasti kuin ristiriitainen ja epäselvä teksti paitsi, että henkilöstö näkee johdon olevan noudattamatta ohjeita (Laaksonen et al 2006: 250).

On suositeltavaa, että jo työsopimuksessa sovitaan kulloinkin voimassa olevien tietoturvaohjeiden noudattamisesta. kaikkien tulee noudattaa annettuja ohjeita. On hyvä käydä läpi kaikki muut organisaation ohjeet ja varmistaa siten, että tietoturvallisuuteen liittyvä ohjeistus tukee muita ohjeita ja on linjassa niiden kanssa (Laaksonen et al 2006: 250).

Ihmistä pidetään tietoturvan heikompana lenkkinä, tästä huolimatta ei omaa henkilökuntaa saa ajatella tietoturvallisuuden vihollisena. Henkilöstölle tulee kertoa tietoturvallisuuden merkitys ja vaikutukset sellaisena kuin ne ovat. Keskustelemalla tietoturvariskeistä, kouluttamalla henkilöstöä toimimaan oikealla tavalla ja valvomalla toimintaohjeiden noudattamista voidaan ihmisistä aiheutuvien riskien todennäköisyyttä pienentää (Laaksonen et al 2006: 252).

Koulutuksen tehokkuus riippuu henkilöstön motivaatiosta. Tietoturvakoulutuksessa tulisikin huomioida erilaisten motiivien vaikutus oppimiseen. mikäli henkilöstöllä on omakohtaista kiinnostusta asioiden omaksumiseen, sitä tulisi hyödyntää. Innostunut työn tekijä kylvää innostusta myös ympärilleen. Henkilökunnan ei tarvitse tietää kaikkea tietoturvasta. riittää kun jokainen työntekijä ymmärtää oman työhönsä liittyvät riskit ja tietää, miten nämä riskit minimoidaan (Laaksonen et al 2006: 254).

Usein organisaatioiden tietoturvallisuuden kehittämisessä suurimmat virheet tehdään tietoturvallisuustoimintaa organisoitaessa ja henkilöstöä koulutettaessa. Vaikka henkilöstölle annetaan ohjeita siitä, miten asiat on tehtävä, työntekijöille ei ole tarpeeksi korostettu toimintatapojen perimmäisiä syitä. Tästä johtuen henkilöstö pitää ohjeita helposti byrokraattisena päätöksenä, joka ainoastaan vaikeuttaa työn tekoa. Haitallista vaikutelmaa lisää, jos samaan aikaan otetaan käyttöön tekninen ratkaisu, joka näkyy käyttäjälle edes vähän työntekoa häiritsevänä tai totuttuja rutiineja muuttavana. Suurin osa ihmisistä pitää rutiineista, koska ne luovat heille henkilökohtaista turvallisuudentunnetta. Heidän mielestään kaikki muutokset ovat pahasta, koska niihin liittyy epävarmuutta. Tätä totuttua ei kannata

sivuttaa m ietittäessä tietotu rvallisuuden kehittäm iseksi tehtäviä toim ia, olivatpa ne mitä tahansa (Laaksonen et al 2006: 255).

## 4.5 Tietoturvallisuuden hallintajärjestelmän sisäiset auditoinnit

Organisaation on suoritettava tietotur vallisuuden hallintajärjestelm än si-säisiä auditointe ja suun nitelluin a ikavälein m äärittääkseen, ovatko tieto - turvallisuuden hallintajä rjestelmän valvontavelvo itteet, turvam ekanismit, prosessit ja m enettelytavat vaatimusten mukaiset. Vaatimukset voivat olla esimerkiksi ISO/ICE 27001:fi:n ja sove ltuvan lainsäädännön m ukaiset tai tunnistettujen tietoturvavaatim usten m ukaiset tai että tietoturvallisuuden hallintajärjestelmä on vaikuttavas ti toteutettu ja ylläpidetty tai tieto turval-lisuuden hallintajärjestelm ä on to iminnassa odotusten m ukaisesti (ISO/ICE 27001:fi:26).

Organisaation on suunniteltava audito intiohjelma ottaen huom ioon audi-toitavien prosessien ja alueiden tila ja tärkeys se kä aikaisempien auditoin-tien tulokset. Auditointien kritee rit, laajuus, suo ritustaajuus, ja m enettelyt tulee m ääritellä. Audito ijat tulee va lita ja aud itoinnit suorittaa s iten, e ttä auditointiprosessin objektiivisuus ja tasapainoisuus voidaan varm istaa. Auditoijat eivät saa auditoida omaa työtään (ISO/ICE 27001:fi: 26).

Dokumentoidussa menettelyohjeissa tulee määritellä auditointien suunnit-telua, suorittamista, tulosten raportointia ja tallenteiden ylläpitoa kosk evat vastuut ja vaatim ukset. Auditoitavas ta alueesta vastuussa olevan johdon tulee varmistaa, että toimenpiteet havaittujen poikkeamien ja niiden syiden poistamista varten suoritetaan ilman aiheetonta viivettä. Seurantatoimenpi-teisiin tulee sisältyä suo ritettujen to imenpiteiden toteam inen ja niiden tu - loksista raportoiminen (ISO/ICE 27001:fi: 26).

## 4.6 Tietoturvallisuuden hallintajärjestelmän johdon katselmus

Vastuullisen johtajan tulee olla tiet oinen organisaation tietoturvallisuuden tasosta ja s iitä, ova tko tie toturvallisuusriskit halli nnassa. Keskeistä on myös selvittää, m itkä ovat sekto rin m ahdolliset puutteet ja heikkoudet, niiden m erkitys toim innalle ja m ihin korja aviin toim enpiteisiin on syytä ryhtyä. Johdon käytössä tulee olla myös vertailevaa tietoa suhteessa toisiin esim. sa man toim ialan, kokoluokan ta i tietoteknisen in frastruktuurin omaaviin organisaatioihin.

### 4.6.1 Yleistä

Johdon tulee katselm oida organis aation tietotu rvallisuuden hallin tajärjes-telmä ennalta suunnitelluin väliajoin varm istaakseen sen jatkuva soveltu-vuus ja vaikuttavuus. Standardin va atimaa, vähintään kerran vuodessa, on syytä noudattaa jos käytetään ulkoista ka tselmointia, muuten organisaatio voi määritellä katselmointitiheyden itse. Katselmukseen tulee sisältyä tie-toturvallisuuden hallinta järjestelmän arviointi, mukaan lukien tietoturva-politiikka ja tietotu rvatavoitteet, parannusmahdollisuudet ja m uutostar-

peet. Katselmuksen tulo kset tu lee d okumentoida selke ästi ja niis tä tule e ylläpitää tallenteita (ISO/ICE 27001:fi: 26).

### 4.6.2 Katselmuksen lähtötiedot

Lähtötietoina käytetään sekä tietotur vallisuuden hallintajärjestelmän itsensä tuottamia tietoja että ulkopuolelta saatuja tietoja. Standardissa edellytetään, että seuraavat tiedot käydään lä pi. Tietoturvallisuuden hallintajärjestelmän sisäisten katselmusten ja tarkasteluiden esiin nostamat tulokset. Lisäksi on johdon edellisessä katselmuksessa esiin tuodut epäkohdat, organisaation sisältä tulleet parannusehdotukset, sidosryhmiltä saatu palaute käytävä läpi. Tietoturvallisuuden hallintajärjestelmän toiminnan mittausten tuloksiin ja ehkäisevien ja korjaavien toim enpiteiden nykytilaan on tutustuttava. Syytä on tutustua, onko tietotur vallisuuden hallintajärjestelm ää kehittäviä uusia tekniikoita, palveluja ja työm enetelmiä ilmaantunut markkinoille. Järjestelm ässä on helposti huomiotta jääneitä uhkia ja haavoittuvuuksia. Näiden rooli on saattanut muu ttua ja vaativat m uuttuneissa olosuhteissa toimenpiteitä (Hakala 2006: 115–116).

### 4.6.3 Katselmuksen tulokset

Katselmuksen tuloksena syntyneet päätökset ja niihin liittyvät toimenpideehdotukset dokumentoidaan. Dokumentoinnissa voidaan käyttää luetteloa:

- Yhteenveto tuloksista ja toiminnan yleisarviointi
- Tietoturvallisuuden hallintajärjestelmän tehokkuuden kehittämiskohteet
- Riskienhallinnan muutokset
- Riskien tunnistaminen ja vaikutusten arviointi
- Riskien käsittely
- Menettelytapojen ja turvamekanismien muutokset
- Muuttuneet opiskelutoiminnan tarpeet
- Muuttuneet turvallisuustarpeet
- Opiskelutoimintaprosessien muutokset ja niiden vaikutukset
- Hyväksyttävien riskien määrittely ja kriteerien muutokset
- Muutokset resursseissa
- Tietoturvallisuuden hallintajärjestelmän toiminnan mittaamisen parantaminen (Hakala 2006: 116).

## 4.7 Tietoturvallisuuden hallintajärjestelmän parantaminen

Hyvin hoidettu tietoturvallisuus ja sen jatkuva kehittäminen ovat keskeiset edellytykset, jotta työntek ijät voivat luottaa sähköisiin palveluihin ja niitä tarjoaviin tietojärjestelmiin.

### 4.7.1 Jatkuva parantaminen

Organisaation tulee jatkuvasti parantaa tietoturvallisuuden hallintajärjestelmänsä vaikuttavuutta käyttämällä hyväksi tietoturvapolitiikkaa, tietoturvatavoitteita, auditointien tuloksia, valvottujen tapahtumien analysointia, korjaavia ja ehkäiseviä toimenpiteitä sekä johdon katselmuksia (ISO/ICE 27001:fi: 28).

### 4.7.2 Korjaavat toimenpiteet

Auditoinnit ja johdon katselmukset tuottavat tietoa järjestelmän kehittämistarpeista. Ne toteutetaan käyttämällä joko korjaavia tai ehkäiseviä toimenpiteitä. Korjaavat toimenpiteet pyrkivät poistamaan ristiriitoja toiminnan ja sitä ohjaavien määritysten välillä. Tietoturvallisuuden hallintajärjestelmän kannalta tärkeimmät määritykset ovat organisaation tietoturvapolitiikka, tietoturvallisuuden hallintajärjestelmän politiikka ja noudatettavat standardit. Tietoturvallisuuden hallintajärjestelmän tietoturvamekanismien ja toimintatapojen on myös oltava sopusoinnussa lainsäädännön ja sopimusten kanssa.

### 4.7.3 Ehkäisevät toimenpiteet

Ehkäisevät toimenpiteet puolestaan pyrkivät torjumaan potentiaaliset ristiriitojen aiheuttajat. Pohdittaessa sekä korjaavia että ehkäiseviä toimenpiteitä tarvitaan dokumentoidut menettelytavat, joiden mukaan selvitetään, miten ristiriidat tunnistetaan ja mitkä seikat ovat niiden syynä. Lisäksi arvioidaan tarvittavien toimenpiteiden tarve, mitkä ne ovat ja miten ne toteutetaan sekä millä tavoin niiden vaikutukset kirjataan ja miten niitä tarkastellaan (Hakala 2006: 115–116).

# 5 YHTEENVETO

Tarkasteltaessa tietoturvastandardien vaatimuksia hyvälle tietoturvan hallintajärjestelmälle ja verrattaessa niitä Keskuspuiston ammattiopiston vallitsevaan tietoturvan tilaan voidaan todeta, että tekninen tietoturvan taso on hyvä ja että sitä kehitetään koko ajan. Aivan viime aikoina on IDS/IPS järjestelmä otettu käyttöön ja varmuuskopiolaitteiston siirto eri palotilaan kuin palvelinlaitteisto etenee. Uudet tilat on jo varattu ja odottavat remontin alkamista ja valokuitukaapelin asennusta palvelinhuoneen ja varmuuskopiohuoneen välille.

Hallinnollinen tietoturva ei ole standardin mukaisessa kunnossa, siitä puuttuu monta oleellista osaa. Voidaan jopa sanoa, että standardin mukaista hallinnollista tietoturvatyötä ole oikeastaan aloitettu. Organisaatiolle ei ole johdon taholta määritelty tietoturvapolitiikkaa eikä määritelty, mikä tieto on suojattavaa tietoa. Tilanne on samanlainen kuin useimmissa muissakin suomalaisissa organisaatioissa.

Hallinnollinen tietoturva-ajattelu on hyvin lähellä laatuhallintajärjestelmän käyttöä. Molemmilla toiminnoilla pyritään parantamaan organisaation tuottaman palvelun laatua. Hallinnollinen tietoturva tuo mukanaan tietoturvan hallintajärjestelmän, siinä on samanlainen lähestymistapa kuin laatukäsikirjan mukaan toimittaessa. Keskuspuiston ammattiopistossa on toimittu laatukäsikirjan mukaan vuodesta 2003, joten on perusteltua odottaa että tietoturvankin kohdalla siirryttäisiin laatuajattelun mukaiseen toimintaan. Katsottaessa mitä kaikkea täydelliseen tietoturvan hallintajärjestelmän mukaiseen toimintaan kuuluu, tehtävä voi tuntua liian suurelta ja kalliilta. Standardi ei kuitenkaan vaadi, että kaikki toiminnot on aloitettava kerralla. Se antaa mahdollisuuden asteittaiseen käyttöönottoon, jota parannetaan koko ajan mahdollisuuksien mukaan.

Koulu on organisaationa kuin laiva ja se kääntyy hitaasti. Liikkeellä sen on kuitenkin pysyttävä koko ajan ja muutettava suuntaansa tarpeen vaatiessa. Aika alkaa olla kypsä tietoturvan hallintajärjestelmän käynnistämiselle laajemminkin eri organisaatioissa Suomessa. Tietoturvan hallintajärjestelmän käyttöönotto muodossa joka täyttää sertifiointivaatimukset täydessä laajuudessa on paljon resursseja vaativa toimenpide, eikä se ole välttämättä hyvä vaihtoehto tällä hetkellä. Tietoturvan hallintajärjestelmän asteittaista käyttöönottoa suositellaan Keskuspuiston ammattiopistolle. Sopivat etenemisaskelmat olisivat:

- johdon hyväksymän tietoturvapolitiikan laatiminen
- riskikartoitus
- suojattavan tiedon määritteleminen
- työntekijöiden motivointi tietoturvatyöhön
- koulutus ja tietoturvatietoisuuden lisääminen varsinkin rekrytointivaiheessa
- järjestelmätuen yhtenäiset kirjalliset toimintaohjeet

Tietokoneet, tietoverkot ja tietokannat tulevat kaiken aikaa tärkeämmiksi työvälineiksi ja tiedon lähteiksi. Niiden toimimattomuus aiheuttaa monenlaista harmia. Siksi pitäisi pyrkiä tilanteeseen jossa käyttäjät itse aiheuttavat mahdollisimman vähän haittaa tieto laitteille ja niiden sisältämälle tiedolle. Hyviä ja turvallisia toimintatapoja edistetään työyhteisössä, jossa käyttäjät ovat motivoituneita tietoturvan ylläpitämiseen ja ymmärtävät miksi asialla on merkitystä. Päinvastaisessa tapauksessa aletaan etsiä oikoteitä hankalaksi koetuille tehtäville ja pahimmillaan alennetaan tietoturvan tasoa.

Johtotasolla luotetaan siihen, että tietoturvan suhteen kaikki on hyvin. Mikään asia ei ole niin hyvin, ettei sitä voisi parantaa. Tutkimuksen yhteydessä ilmeni, että rekrytointivaiheessa uusi tulokas tutustutaan talon tietoturvakäytäntöihin. Todellisuudessa näin ei kuitenkaan näytä tapahtuvan. Osasyynä tähän on varmasti se, ettei selkeätä yksinkertaista ohjetta tätä toimintaa varten ole olemassa. Tietoturvaohjeet on sisällytetty useampaan ohjeeseen ja strategiaan. Niiden löytäminen on hankalaa, vaikka tietää mitä etsii, saati sitten uudelle tulokkaalle, joka ei tiedä mitä etsiä. Kirjallista sitoumusta tietoturvan noudattamiseen ei vaadita henkilökunnalta eikä opiskelijoilta. Lyhyt kirjallinen esitys asiasta ja verkosta löytyvä tiedon kertaussivu tarkistuskysymyksin toimisi varmasti paremmin ja kirjallista sitouttamista kannattaisi harkita.

Järjestelmätuki on aiemmin toiminut yhdestä huoneesta käsin, jolloin suullinen tiedon välitys ja kontrolli on toiminut hyvin. Järjestelmätuki on ottamassa tietohallinnon roolin ja toimii useammassa paikassa. Tarve yhtenäisille kirjallisille toimintaohjeille kasvaa kaiken tulisi luoda. Nykyisten hyvien käytäntöjen kirjaamisella voisi aloittaa.

Yllä esitetyt parannukset voisi tehdä kohtalaisen pienin kustannuksin ja itse asia kuitenkin etenisi. Aivan ilmaiseksi sitä ei kuitenkaan saa. Tekijöille on varattava aikaa työn tekemiselle. Tämä tutkimus on tehty ylemmän ammattikorkeakoulututkinnon opinnäytetyönä eikä maksanut opistolle mitään. Yhden tutkimuksen tekemiseen menee noin kaksi vuotta. Menetelmä ei ole kovin nopea ratkaisu akuutteihin ongelmiin, mutta sopii hyvin erilaisiin kehittämistöihin.

Työn liitteessä oleva ISO/ICE 27001 standardin mukainen valvontavelvoite ja turvamekanismiluettelo, jossa Keskuspuiston ammattiopiston tilannekartoitus toimii ohjenuorana, on käyttökelpoinen työkalu toiselle kouluorganisaatiolle, joka haluaa kartoittaa oman organisaationsa tietoturvan tilaa. Työn alkuosa johdattaa tietoturvan hallintajärjestelmän luomiseen organisaatiossa.

## 5.1 Tutkimuksen reliabiliteetti

Mittauksissa on käytetty uusimmissa standardeissa ISO/ICE 27001:fi ja ISO/IEC 27002 määriteltyjä turvamekanismeja ja malleja tietoturvan hallintajärjestelmän kehittämiselle, toteuttamiselle, käyttämiselle, valvomiselle, katselmoinnille ja ylläpitämiselle. Ne ovat kaikkien saatavilla ja toistet-

tavissa samojen ohjeiden mukaan. Standardit laaditaan ja hyväksytään tarkoin laadittujen kriteerien mukaan ja ovat luonteeltaan luotettuja. Tulokset on saatu tietyssä aikaikkunassa ja ne muuttuvat ajan muuttuessa, koska tarkasteltavana on kehittyvä organisaatio. Samaan aikaan suoritettu toinen tutkimus olisi varmaan saanut hyvin yhtenevän tuloksen.

Järjestelmätuelta kysyttäessä tietoturvamekanismeista saatiin joskus poikkeavia vastauksia. Jatkettaessa kyselyä eri henkilöiltä päästiin yhteneviin tuloksiin. Kysytyt kysymykset olivat yksityiskohtaisia ja vaativat hyvää muistamista. Erot syntyivät erilaisesta muistamisesta, mutta lopputulos oli yhteneväinen ja siten luotettava. Kaikissa kysymyksissä, joissa havaittiin poikkeamista arjen käytännöistä tai joiden aihepiiri oli vieras, suoritettiin useampia tarkistuskysymyksiä luotettavuuden vahvistamiseksi.

## 5.2 Tutkimuksen validiteetti

Standardin turvamekanismit ovat huolellisesti laaditut ja kattavat käsitellyn alan laajasti monesta näkökulmasta. Kokonaisuudessa ne muodostavat kattavan mittariston tietoturvan hallintojärjestelmän tilasta ja sitä on helppo verrata standardin ”ihannetilaan”. Kartoitus antaa validin kuvan Keskuspuiston ammattiopiston tietoturvan vallitsevasta tilasta. Tilanne on samanlainen kuin monessa suomalaisessa keskisuuressa organisaatiossa, arjen käytännöt eivät ole sellaiset kuin johto uskoo niiden olevan.

Tiedusteltaessa henkilöiltä turvamekanismien tilasta, jotka joutuvat vastaamaan heidän omalla alallaan saattoi joskus havaita pientä ”pyöristämistä” ylöspäin, eli asiat esitettiin hieman valoisammin kuin ne todellisuudessa olivat. Nämä kohdat karsittiin tarkistuskysymysten avulla. Tietoturvan tila muuttuu kaiken aikaa varsinkin teknillisellä puolella. Tietyin osin vastaukset olisivatkin tänään hieman erilaisia kuin kysyttäessä. Suoritetut muutokset tai suunnitteilla olevat muutokset on pyritty kirjaamaan kyselyjen vastauksiin.

Standardien turvamekanismeja käytetään mittareina. Ne on kehitetty pitkän yhteisöllisen prosessin tuloksena, niitä pidetään yleisesti luotettavina ja niiden uskotaan pureutuvan oleellisiin asioihin. Tämän perusteella on oikeutettua uskoa tulosten olevan rakennevaliditeetiltaan ja kontekstivaliditeetiltaan hyvän ja kuvaavan Keskuspuiston ammattiopiston tietoturvan hallintajärjestelmän tilaa oikein. Samat kysymykset voidaan esittää missä organisaatiossa tahansa, ja jos kysymyksiin saadaan rehelliset vastaukset, voidaan sama tutkimus toistaa missä vain. Vastaukset kuvaavat vain sen organisaation tilaa, missä ne esitetään. Tässä tutkimuksessa esitetyt vastaukset on tarkoitettu opastuksesi kouluoloihin. Sisältövaliditeetin osalta tutkimusprosessi on helposti tarkastettavissa ja arvioitavissa.

Tutkimustulokset ovat hyvin samanlaiset kuin muissakin suomalaisissa keskisuurissa organisaatioissa. Kehitystrendit näyttävät kulkevan samassa tahdissa ja moni muu organisaatio painii samojen ongelmien kanssa. Tämä osoittaa, että korrelatiivinen validiteetti on suuri. Jokaisen organisaation

on kuitenkin suoritettava työ om ista lähtökohdistaan ja ed ettävä omaa tietään.

Tutkimus vertaa Keskuspuiston tietoturvan tilaa standardin esittäm ään ihannetilaan. Näissä olevien eroavu uksia perusteella on helppo ennustaa tulevia tarpeellisia toim enpiteitä. N iiden prioriteetei sta joudutaan toki käymään keskustelua. Tämän perusteella voidaan sanoa tutkim uksella olevan hyvän ennustevaliditeetin.

# 6 KONTRIBUUTIOT

Opinnäytetyön tekem inen tulisi olla opettavainen oppim isprosessi, joka olisi sekä kiinnostava että m iellyttävä. Parhaimmillaan se on mitä parhainta viihdettä ja kaiken li säksi tuottaa hyötyä sen te kijälle itselleen ja työyhteisölle.

Ensimmäinen opiskeluvuosi kului pakolli sten o pintojaksojen suorittam isessa, joista osa sivusi opinnäytetyötä. Tarkoitus oli jatkaa päättötyötä heti kesällä 2008, mutta se ei onnistunut kovin hyvin. Henkilökohtaiset resurssit eivät riittäneet, jonkin asteinen lamaantuminen ja voimattomuus koettelivat. Palautum ien alkoi kuitenkin hiljal leen ja valm istelutyöt pääsivä t käyntiin ensin pohtim istasolla. Varsin ainen kirjoitustyö sai odottaa m yöhäiseen syksyyn. Käynnit opiskelupaikal la Häm eenlinnassa edistivät lisätarmon löytym isessä ja työn m uuttumisessa jälleen kiinnostavaksi. Työ ei varsinaisesti koskaan jäänyt jälkeen aikataulusta, m utta pieni hengähdystauko oli ilm eisesti enemmän kuin pa ikallaan. Tuum austauko toi enem män syvyyttä ja pohdintaa työhön ja anto i aikaa tarkastella asiaa monipuolisemmin. Tietoturvan hallintajärjestelmän luominen organisaatiolle on iso asia, joka ei oikeastaan pääty kosk aan niin kauan kuin organisaatio on olemassa.

## 6.1 Työelämälähtöisyys

Opinnäytetyö on tehty työantajaorgan isaation tarpeita aja tellen. Kesku spuiston am mattiopistolla ei o le o llut tieto turvan hallinta järjestelmää käytössään. Teknillinen tietoturva on kohta laisen hyvässä kunnossa ja sitä kohennetaan kaiken aikaa. Tämä on todettu työssä. Hallinnollinen tietoturvatyö on vielä lähtökuopissaan. Sen käy ttöönotto vaati johdon rohkaisem ista ja asian tarpeelliseksi osoittamista

Tämän työn puitteissa on kerätty tietoa asenteista tiet oturvatyötä kohtaan organisaatiossa, jossa asen teellisesti hyvin harva va stustaa tietoturvan parantamista. Ongelmana on pikemmin oikean tiedon saannin puute. Koulun ohjaus tietoturvasta työhönottohetkellä on niukkaa. Koululla ei ole verkossa oppim issisältöä, jossa tietoturva-asio ita voisi opiskella ja kerrata om atoimisesti tietäen, että saatu tieto on oikeata ja relevanttia. Käydyt keskustelut ja tämä työ py rkivät va ikuttamaan siihen, että se llainen paikka syntyisi ja että koululla si irryttäisiin kohti tietoturvan hallintajärjestelm än käyttöä.

Käynnissä oleva organisaation m uutos edesauttaa tietotur van hallintajärjestelmän käyttöönottoa, koska käy ttäjäkunta laajenee ja käyttörutiinit eroavat toisistaan ilm an yhtenäistä o hjausta. Tämä työ valm istuu oikeaan aikaan, nyt sille on paljon käyttöä. Johto tulisi saada huomaamaan, että tietoturvan ha llintajärjestelmää tarvita an organ isaatiossa ja e ttei työ läh de käyntiin ilman sen sitou tumista asiaan. Hallinnollinen tietoturvatyö e i ole vielä käynnistynyt. Yleinen käsitys on, että uhkien pienentäm iseen voi-

daan vaikuttaa tekniikan avulla 30 % osuudella ja inhim illisten tekijöiden avulla 70 % osuudella. Hallinno llisten toimenpiteiden avulla voidaan vaikuttaa inhimillisiin tekijöihin. Tällä hetkellä kannattaisi sijoittaa hallinnollisiin tekijö ihin, koska järkev ällä toim innalla sillä puo lella saa taisiin enemmän vastinetta rahoille. Teknistä puolta ei pidä kuitenkaan unohtaa.

Tämän työn tekem inen on m aksanut organisaatiolle yhden standardi asiakirjan oston verran. Tästä eteenpäin t yö maksaa ja vaatii resursseja, antaa pohjaa hahmotella tulevaisuuden toim intamallia ja on sam alla kuvaus tämän hetken tietoturvatilanteesta.

## 6.2 Vaikuttavuus

Toistaiseksi uuden tietohallintaorgani saation edustajat ovat tutustuneet koulun tietoturvan tilaa koskevaan se lvitykseen ja hyödyntävät sitä om ien päämääriensä läpiviem iseen johtoku nnassa. Koulun johtokunnalle työssä esitetyt asiat tuntuvat vierailta ja niiden käsittely vienee aikaa.

Opinnäytetyö on tarkoitus jakaa ha lukkaille sähköisessä m uodossa. Sen liiteosan avulla mikä tahansa organisaatio voi ka rtoittaa oman tietoturvansa tilaa ja v errata s itä teoriaos assa esitetty ihin vaatim uksiin. Toim enpide vähentää valm istelutyötä huom attavasti ja auttaa pääsem ään kiinni varsinaiseen tuottavaan työskentelyyn. Vaikka opinnäytetyötä voi soveltaa missä tahansa organisaatio ssa, kuvaavat annetut vast aukset tilannetta koulumaailmassa. Tietoturvaa on käsitelty laaj asti, jopa niin laa jasti, e tteivät kaikki koulut vielä ole valm iita näin suuriin pan ostuksiin. Standardi m ahdollistaa asteittaisen tietoturvamekanismien lisäämisen, kaikkea ei tarvitse toteuttaa kerralla. Tietoturvaongelma voidaan ratkaista pala kerrallaan noudattamalla standardeja ISO/ICE 27001: fi ja ISO/IEC 27002 ja käyttämällä tätä opinnäytetyötä avuksi varsinaisessa toteutustyössä.

## 6.3 Oma asiantuntemus

Tietoturva on ollut oman kiinnostukseni kohteena pitempään. Aikaisemmat kokemukset ovat olleet enemmän yksilötasolla: miten suojata tietty kone ja miten vaikuttaa yhteen käyttäjään. Tämä opinnäytetyö on tuonut laajemman näkemyksen ja laaja-alaisemman teoreettisen näkemyksen tietoturvakäsitteeseen organisaatiotasolla. Käytännössä minulla ei ole johtavaa tai käskevää asemaa organisaatiossamme tietoturvan suhteen. Syksyllä 2008 oli mahdollista kysyä asioista ja yrittää vaikuttaa asioiden etenemiseen. Yritin olla eräänlainen harmaa eminenssi. Selvittelyt ja suositukset oli tehty eri osapuolten myötämielisellä avustuksella. Asioita oli viety eteenpäin niiden tarpeellisuuden ja hyödyn näkökannalta ilman aseman tuomaa valtuutusta. Päämääränä oli ollut saada johtavassa asemassa olevat huomaamaan asian tärkeys ja ajankohtaisuus. Uuden organisaatiomuutoksen myötä johtamistapa on muuttunut byrokraattisempaan suuntaan. ja suora vaikuttaminen hankaloitunut. Entinen johtoryhmä oli helpommin tavoitettavissa satunnaisissa kahvi- ja ruokailutilanteissa. Nykyistä johtokuntaa tapaa harvoin.

Selvittelyn tiimoilta olen joutunut olemaan yhteydessä moneen osapuoleen organisaatiossamme. Johtamistaidon opiskeluilla on ollut osuutta asiaan, että yhteydenpito autenttisine vuorovaikutustilanteineen ovat syntyneet ja ovat olleet oikein suuntautuneet. Olen hyödyntänyt YAMK – koulutusohjelman tarjontaa laajasti opinnäytetyössäni, koettaen huomioida myös taloudelliset näkökohdat, jotka kuuluivat opiskeluohjelmaan. Lähimpien esimiesten kanssa yhteistyö toimii edelleenkin. Yhteyden luominen koulun ylimpään johtoon vaatii uuden strategian luomista ja käytettyjen käyttäytymismallien uudelleenarviointia.

# LÄHTEET


## Standardit

ISO/IEC 2006. ISO/IE C 27001:fi Inform aatioteknologia. Turvallisuus. Tietoturvallisuuden hallint ajärjestelmät. Vaatimukset. Suom en standardoimisliitto SFS, Helsinki.

ISO/IEC 2005. ISO/IEC 27002 Infor mation technology- Security techniques- Code of practice for inform ation security m anagement. International Organization of Standardization, Geneva.

## Valtionhallinnon ohjaukset

Tammisalo, T. 2005. Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja
hyvät käytännöt. STAKES, RAPORTTEJA 5/2005, Helsinki.

Tammisalo, T. 2007. Sosiaali- ja terv eydenhuollon organisaatioiden tietoturvan hallinnointi. STAKES, RAPORTTEJA 5/2007, Helsinki.

Turvakansio, 2008. Orton, Invalidisäätiö. Orton, Invalidisäätiö, Helsinki.

VAHTI 6/2003. Opas julkishallinnon tieto turvallisuus- koulutuksen järjestämisestä. Valtionvarainministeriö, Helsinki.

VAHTI 7/2 003. Ohje riskien arvioinnist a valtionhallinna ssa tietoturvallisuuden edistämiseksi. Valtionvarainministeriö, Helsinki.

VAHTI 5/2004. Valtionhallinnon keskeisten tietojärjestelmien
turvaaminen. Valtionvarainministeriö, Helsinki.

## Kirjat

Hakala, Vainio & Vuorinen, 2006. Tietoturvallisuuden käsikirja. Docendo, Jyväskylä.

Laaksonen, M & Nevansalo, T & T omula, K. 2006. Yrityksen tietoturvakäsikirja. Edita Publishing Oy, Helsinki.

## Verkkomateriaalia

Guel, M 2007. A Short Primer for Developing Security Policies. The SANS Institute, Bethesda.
http://www.sans.org/resources/policies/Policy_Primer.pdf

Nixu 2008. Tietoturv allisuuden hallin ta suomalaisissa organisaatio issa 2007. Nixu Oy, Espoo. Saavutettavissa: http://www.nixu.fi/news/tietoturvatutkimus2007/Tietoturvallisuuden_hallinta_suomalaisissa_organisaatioissa_2007.pdf . Luettu 3.3.2009.

Sundberg, S. 2008. VAHTI päivä 15.12.2008 Johtajan tietoturvaopas – tietoturvallisuus johtajan kannalta. Valtiokonttori, Helsinki. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20081119Valtio/07_Sundberg_Johtajan_tietoturvaopas_2008.pdf

Keskuspuiston ammattiopiston ohjeistuksia

Laatukäsikirja. 2003. Keskuspuiston ammattiopisto, Helsinki.

HEPO. 2002.Orton-Invalidisäätiön henk ilöstöpolitiikka ja henkilös töhallinto. Orton, Invalidisäätiö, Helsinki.

Perehdyttämissuunnitelma. 2009. Keskuspuiston ammattiopisto, Helsinki.

# TERMIT JA MÄÄRITELMÄT

IDS Lyhenne sanoista Intrusion Dete ction System . Tunkeutum isen havainnointijärjestelmä.

IEC The International Electrotechnical Commission. Kansainvälinen sähköalan standardointiorganisaatio.

ISMS Lyhenne sanoista Inform ation Se curity Managing System . Tietoturvallisuuden hallintajärjestelmä.

ISO The International Organization fo r Standardization. Kansainvälinen standardeja laativa organisaatio.

KÄYTETTÄVYYS
Ominaisuus olla saatavilla ja k äyttökelpoinen valtuutetun tahon niin vaatiessa.

PDCA Kehittämismalli. Lyhenne sanoist a Plan, Do, Check, Act tai SFS:n käännöksenä suomeksi Suunnittele, Toteuta, Arvioi, Kehitä.

RISKIANALYYSI
Systemaattinen tie tojen käyttämin en riskien tu nnistamiseen ja niid en vaikutusten arviointiin.

SUOJATTAVA KOHDE
Mikä tahansa kohde, joka on arvokas organisaatiolle.

TIETOTURVALLISUUS
Tiedon luottam uksellisuuden, eheyden ja käytettävyyden s äilyttäminen: lisäksi tähän voi sisältyä m uita ominaisuuksia, kuten aitous, vastuullisuus, kiistämättömyys ja luotettavuus.

TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄ ISMS
Se osa yleistä toim intajärjestelmää, joka liike toimintariskien arvioin tiin perustuen luodaan ja toteutetaan ja jota käytetään, valvotaan, katselm oidaan, ylläpidetään ja parannetaan tavoitteena hyvä tietoturvallisuus.

VAHTI Valtionhallinnon tietoturvallisuuden johtoryhmä.

LIITE 1

KESKUSPUISTON AMMATTIOPISTON TIETOTURVAKARTOITUS

# 1 JOHDANTO

Tässä liiteosassa käydään läpi st andardin ISO/IEC 27002:2005 kappaleissa 6-15 esitetyt turvamekanismit sovellettuna Keskuspuiston ammattiopistossa vuoden 2008 lopulla vallitsevaan ti lanteeseen. Kartoituksessa selvitetään koulun tietoturvan tilaa.

Selvitettäviä kohtia on runsaasti ja ne vaativat perehtymistä vallitsevaan tilanteeseen, jotta totuudenm ukaiset käyt ännöt saataisiin kirjattua. Mallia voi käyttää hyväkseen, ISO standardie n käyttöoikeuksien puitteissa, työn vaatiessa jossakin toisessa organisa atiossa. Keskuspuiston ammattiopisto on toisen as teen ammattioppilaitos ja kartoituks en tilannetta on peilattava tätä taus taa vasten. Te kstissä Kes kuspuiston ammattiopistosta käytetään lyhennettä Keskuspuisto.

Kappaleiden alussa on lyhyt johdatus käsiteltäviin aiheisiin. Ensimmäisessä alikappaleessa kuvataan alikappaleen tavoite ja sitä seuraavissa alikappaleissa standardin mukainen turvamekanismi, jota peilataan Keskuspuiston ammattiopistossa vallitsevaan tilanteeseen. Kappaleet 2-8 ovat toiminnoiltaan selkeitä m onessa organisaatio ssa ja m elko pienellä vaivalla vastattavissa. Kappaleen 9 ja varsin kin kappaleiden 10–12 tarkistus voivat aluksi herättää kysym yksiä. Silloin kannattaa hankkia standardi ISO/IEC 27002, jossa asiat selvitetään hieman tarkemmin. Toistaiseksi standardia ei saa suomenkielisenä, mutta tilanne voi muuttua nopeasti.

Kappalejako alaotsikkoineen noudatt aa standardin ISO/IEC 27001 jakoa. On kuitenkin syytä huom ata, että kappa le 2 vastaa stand ardin liitteen A kappaletta A.5, molemmilla on nimi turvallisuuspolitiikka. Jatko noudattaa molemmissa samaa järjestystä.

# 2 TURVALLISUUSPOLITIIKKA

> Hyvä tietoturva vaatii järjestelmällistä johtamista. Tietoturvallisuuden kehittämisen tärkeimpiä osia on selkeästi rakennettu tietoturvaohjelma, joka pitää sisällään kaikki organisaation toiminnot kattavan politiikan ja ohjeiston. Tavallisesti ohjeisto muodostuu yksittäisistä tiettyyn tarkoitukseen laadituista ohjeista. Tyypillisesti nämä ohjeet vastaavat jonkin viitekehyksen tai standardin vaatimuksia. Nämä vaatimukset puolestaan esitetään yleisellä tasolla yrityksen tietoturvapolitiikassa. (Laaksonen 2006: 145)

## 2.1 Tietoturvapolitiikka

Tavoite Tarjota johdon ohjaus ja tuki tietoturvallisuudelle opetustoimitavoitteiden ja asiaankuuluvien lakien ja asetusten mukaisesti.

### 2.1.1 Tietoturvallisuuspolitiikan määrittelyasiakirja

Turvamekanismi

> Tietoturvapolitiikan määrittelyasiakirjan tulee olla johdon hyväksymä, se tulee julkaista ja siitä tulee tiedottaa kaikille työntekijöille ja merkittäville ulkopuolisille tahoille.

Keskuspuiston tilanne

> Tietoturvapolitiikan määrittelyasiakirjaa ei ole määritelty eikä hyväksytty.

### 2.1.2 Turvallisuuspolitiikan katselmointi

Turvamekanismi

> Tietoturvapolitiikka tulee katselmoida suunnitelluin aikavälein tai mikäli merkittäviä muutoksia tapahtuu, sen jatkuvan soveltuvuuden, asianmukaisuuden ja vaikuttavuuden varmistamiseksi.

Keskuspuiston tilanne

> Tietoturvapolitiikan katselmoitusuunnitelmaa ei ole määritelty eikä hyväksytty.

# 3 TIETOTURVALLISUUDEN ORGANISOINTI

## 3.1 Sisäinen organisaatio

Tavoite Organisaation tietoturvallisuuden hallinta.

### 3.1.1 Johdon sitoutuminen tietoturvallisuuteen

Turvamekanismi

Johdon tulee sitoutua tietoturvallisuuteen ja tukea organisaatiota tietoturvatoiminnassa näkyvästi ja varata toimintaan riittävästi resursseja. Tietoturvan hallinnoinnin täytyy olla tarkasti määritelty ja tietoturvaorganisaation nimetty ja selkeästi vastuutettu. Palautetta on annettava säännöllisesti.

Keskuspuiston tilanne

Tietoturva on hoidettu tekisenä työnä järjestelmätuen kautta. Hallinnollista tietoturvatyötä ei ole varsinaisesti käynnistetty lukuun ottamatta luvan ja rahoituksen antamista laitehankintoihin.

### 3.1.2 Tietoturvallisuuden koordinointi

Turvamekanismi

Organisaation eri osien edustajien, joilla on asiaankuuluvia rooleja ja työtehtäviä, tulee koordinoida tietoturvallisuuteen liittyvät toimet.

Keskuspuiston tilanne

Koordinointityö on melko vähäistä. Työn voisi aloittaa uuden henkilökunnan perehdyttämisellä tietoturvatyöhön ja lisäämällä työsopimuksen mainninan sitoutumisesta organisaation tietoturvapolitiikkaan. Tietoturvapolitiikka pitäisi tietenkin olla laadittuna ja hyväksyttynä ennen sitä.

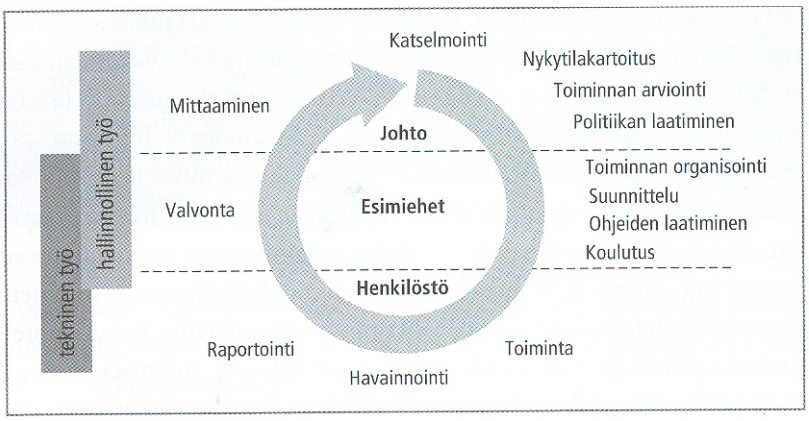
### 3.1.3 Tietoturvallisuutta koskevien vastuiden jako

Turvamekanismi

Kaikki tietoturvavastuut tulee määritellä selvästi.

Keskuspuiston tilanne

Tietohallintopäällikkö on nimetty aivan äskettäin. Hänen tehtäväkseen tullee esittää tietoturvallisuuden hallintojärjestelmän luomista. Tämä työn tarkoituksena on tukea häntä ja johtoa asiassa. Organisaation tämänhetkinen kehitysvaihe on alla olevan kuvan oikeassa yläkulmassa eli nykytilan kartoituksessa prosessin ensimmäisellä kierroksella.




**Kuva 3 Tietoturvaohjelman pääelementit ja prosessin kulku**

Nykytilaan on tultu toiminnan historiakulun ja kehityksen myötä. Tarkoituksena on jatkaa eteenpäin entistä määrätietoisempana ja suunnitellummin. Teknistä työtä on tehty kaiken aikaa, nyt kaivattaisiin hallinnollisen työn osuutta.

### 3.1.4 Tietojenkäsittelypalveluja koskeva hyväksyntäprosessi

Turvamekanismi

Uusia tietojenkäsittelypalveluja ko skeva johdon hyväksyntäprosessi tulee määritellä ja ottaa käyttöön.

Keskuspuiston tilanne

Tietojenkäsittelypalveluja koskeva a johdon hyväksyntäprosessia ei ole olemassa.

### 3.1.5 Salassapitosopimus

Turvamekanismi

Salassapito- tai vaitiolositoumukset, jotka kuvastavat organisaation tarpeita suojata tietoa, tulee yksilöidä ja niitä tulee katselmoida säännöllisesti.

Keskuspuiston tilanne

Luottamuksellisen tiedon käsittelyta voista on mainintoja henkilöstöstrategiassa. Niiden löytäm inen käytännössä on haasteellista kauan talossa olleellekin. Uusi työntekijä tuskin löytää niitä. Uusi seikkaperäinen ohjeistus on tarpeellinen.

### 3.1.6 Yhteydet viranomaisiin

Turvamekanismi

Asiaankuuluvien viranomaisten kanssa tulee pitää asianmukaista yhteyttä.

Keskuspuiston tilanne

Tavallisimmat viranomaiset ovat Opetushallitus, Kansaneläkelaitos ja vakuutuslaitosten edustajat. Näihin yhteydenpito on ollut säännöllistä ja toistuvaa.

### 3.1.7 Yhteydet erityisintressiryhmiin

Turvamekanismi

Tulee ylläpitää asianmukaisia yhteyksiä erikoisintressiryhmiin tai muihin turvallisuusasiantuntijaryhmiin ja ammatillisiin järjestöihin.

Keskuspuiston tilanne

Yhteistyö vammaisjärjestöihin ja toisiin erityisoppilaitoksiin on säännöllistä.

### 3.1.8 Tietoturvallisuuden riippumaton arviointi

Turvamekanismi

Kolmansien osapuolten kanssa tehtävien sopimusten, jotka liittyvät organisaation tiedon tai tietojenkäsittelypalvelujenkäyttöoikeuksiin, käsittelyyn, hallintaan tai niistä viestimiseen tai tuotteiden tai palvelujen lisäämiseen tietojenkäsittelypalveluihin, tulee kattaa kaikki olennaiset turvallisuusvaatimukset.

Keskuspuiston tilanne

Yhteistyö tiedon tai tietojenkäsittelypalvelujenkäyttöoikeuksiin liittyvissä asioissa koskevat tietojärjestelmien huoltotöitä, sähköpostia, opiskelijoiden poissaolorekisteriä, Moodle- ja Pedanet- ympäristöä. Kirjallisia sopimuksia näiden järjestelmien käyttämisestä on tehty niukasti, käytännössä on luotettu suullisiin sopimuksiin.

## 3.2 Ulkopuoliset tahot

Tavoite Ylläpitää organisaation tiedon ja tietojenkäsittelypalvelujen turvallisuutta, kun ulkopuoliset tahot pääsevät näkemään tai käsittelemään niitä, saavat niistä tietoa tai hallinnoivat niitä.

### 3.2.1 Ulkopuolisiin tahoihin liittyvien riskien tunnistaminen

Turvamekanismi

Organisaation tietoon ja tietojenkäsittelypalveluihin kohdistuvat riskit, joita aiheuttavat liike toiminta- ja opiskeluprosesseissa mukana olevat ulkopuoliset tahot, tulee tunnistaa ja asianmukaiset turvamekanismit luoda ennen pääsyn sallimista.

Keskuspuiston tilanne

Kirjallista riskikartoitusta ei ole tehty. Koulun sallittuihin tietojärjestelmäsovelluksiin pääsyä hallitaan autentikoinnin kautta.

### 3.2.2 Turvallisuudesta huolehtiminen asiakassuhteissa

Turvamekanismi

> Kaikista tunnistetuista turvallisuusvaatimuksista tule e huolehtia, ennen kuin asiakkaalle annetaan pääsy organisaation tietoon tai suojattaviin kohteisiin.

Keskuspuiston tilanne

> Kirjallisia ohjeistuksia turvallisuusvaatimuksista ei ole olemassa. Suoraa yhteyttä organisaation ydintietoihin tai suojattaviin tietoihin ei ole annettu.

### 3.2.3 Turvallisuudesta huolehtiminen kolmansien osapuolten suhteen

Turvamekanismi

> Kolmansien osapuolten kanssa tehtävien sopimusten, jotka liittyvät organisaation tai tietojenkäsittelypalveluj en käyttöoikeuksiin, käsittelyyn, hallintaan tai niistä viestimiseen tai tuotteiden tai palvelujen lisäämiseen tietojenkäsittelypalveluihin, tulee kattaa kaikki olennaiset turvallisuusvaatimukset.

Keskuspuiston tilanne

> Kolmansien osapuolten kanssa ei ole tehty kirjallisia sopimuksia, jois sa varmistuttaisiin, ettei väärinymmärryksiä pääse syntymään osapuolten välille.

# 4 SUOJATTAVIEN KOHTEIDEN HALLINTA

Tietoturvan näkökulm asta katsottuna ka ikkia tietotekniikkalaitteita tulee suojata. Organisaation ja henkilöstöt urvallisuuden kannalta laitte illa on erilaisia arvoja toiminnallisuuden ja tietoturvan kannalta. Mitä tärkeämpää tai luottamuksellisempaa tietoa kohde sisältää, sen suojatu mmassa paikassa sen tulisi olla.

## 4.1 Vastuu suojattavista kohteista

Tavoite Saavuttaa organisaation suojattavien kohteiden riittävä suojaus ja ylläpitää sitä.

### 4.1.1 Suojattavien kohteiden luetteloiminen

Turvamekanismi

Kaikki suojattavat kohteet tulee yksilöidä selkeästi, kaikki merkittävät kohteet tulee luetteloida ja luetteloiden ylläpidosta huolehtia.

Keskuspuiston tilanne

Suojattavat ja tärkeät tai merkitykselliset kohteet on yksilöity selkeästi ja luetteloitu ja luetteloa ylläpidetään jatkuvasti.

### 4.1.2 Suojattavien kohteiden hallinnointi

Turvamekanismi

Kaikille tiedolle ja tiedonkäsittelyp alveluihin liittyv ille suojattaville kohteille tulee nimetä hallinnoitsija, joka on tietty organisaation osa.

Keskuspuiston tilanne

Kaikille tiedoille on nimetty hallinnoitsija.

### 4.1.3 Suojattavien kohteiden hyväksyttävä käyttö

Turvamekanismi

Tiedon ja tietojenk äsittelypalveluihin liittyvien suojattavien kohteiden h yväksyttävän käytön säännöt tulee yksilöidä, dokumentoida ja toteuttaa.

Keskuspuiston tilanne

Hyväksyttävän käytön säännöt ovat suu llisessa muodossa ja niitä toteutetaan. Yhtym inen Arla-instituutin kanssa on lisännyt tarvet ta kirjallisten ohjeiden teolle.

## 4.2 Tiedon luokitus

Tavoite Varmistaa, että suojattavalla tiedolla on riittävä suojaus.

### 4.2.1 Luokitusohjeita

Turvamekanismi

Tieto tulee luokitella sen arvon, lakisäteisten vaatimusten, arkaluontoisuuden ja kriittisyyden perusteella.

Keskuspuiston tilanne

Kirjallisia keskitettyjä ohjeistuksia ei ole. Nykyiset ohjeet ovat hajasijoitettuna muiden ohjeistuksien sisään mm. Tietosuoja työsuhteessa, Turvakansio ja Kehittämissuunnitelma vuosille 2008–2010.

### 4.2.2 Tiedon merkitseminen ja käsittely

Turvamekanismi

Tiedon merkitsemistä ja käsittelyä koskeva asianmukainen ohjeisto tulee laatia ja ottaa käyttöön organisaation määrittelemien luokitteluperiaatteiden mukaisesti.

Keskuspuiston tilanne

Kirjallisia ohjeita ei ole. Tietoa ei merkitä tulostettaessa. Suojattu ja luottamuksellinen tieto on saavutettavissa ainoastaan asianmukaisin oikeuksin. Oikeudet saaneet henkilöt ovat sitoutuneet suullisesti noudattamaan luottamuksellisuuden vaativia menettelyjä tulostuksessa, tiedon tallennuksessa ja siirrossa ja tuhoamisessa.

# 5 HENKILÖSTÖTURVALLISUUS

Tietoturvallisuuteen vaikuttavat sekä tekniset että inhimilliset uhkat. Usein puhutaan 70–30- säännöstä: turvallisuudesta 70 % muodostuu ihmisten toiminnasta, asenteista, ymmärryksestä ja osaamisesta. Vastaavasti 30 % turvallisuudesta koostuu teknisten ja teknologisten ratkaisujen ja menetelmien vaikutuksista.
Ihmisten toiminta on suurin turvallisuutta uhkaava tekijä. Suurin osa tästä uhasta muodostuu organisaation sisäisestä toiminnasta ja osaamisesta sekä kolmansien osapuolten – alihankkijoiden, yhteistyökumppaneiden ja asiakkaiden – henkilöstöstä. Henkilöstöturvallisuuden tarkoituksena on ehkäistä henkilöstöön liittyviä uhkia, kuten inhimillisiä virheitä, väärinkäytöksiä ja varkauksia. Uhkia ehkäistään ja turvariskejä pienennetään valitsemalla sopivat kontrollit, joiden avulla kiinnitetään huomiota henkilöiden koko työsuhteen aikaiseen ja sen jälkeiseen turvallisuuteen. Erilaiset kontrollit koskevat esim erkiksi henkilöstön palkkausprosessia, toimenkuvien ja vastuiden määrittämistä, sopimuksellista velvoittamista, turvaohjeistusta, -koulutusta ja turvatietoisuuden ylläpitoa sekä toimenpiteitä työsuhteen loppuessa ja salassapitovelvoittamista työsuhteen jälkeen.

## 5.1 Ennen työsuhteen alkua

Tavoite Varmistaa, että työntekijät, toimittajat ja ulkopuoliset käyttäjät ymmärtävät velvollisuutensa ja ovat sopivia heille harkittuihin tehtäviin, sekä vähentää varkauksien, petosten ja palvelujen väärinkäytön riskiä.

### 5.1.1 Roolit ja vastuut

Turvamekanismi

Työntekijöiden, toimittajien ja ulkopuolisten käyttäjien turvallisuusroolit ja -vastuut tulee määritellä ja dokumentoida organisaation turvallisuuspolitiikan mukaisesti.

Keskuspuiston tilanne

Turvallisuusroolit ja -vastuut esitetään suullisesti perehdyttämisohjeistuksen mukaan. Työsopimuksessa ei ole mainintaa asiasta. Selkeät kirjalliset ohjeet tulisi olla.

### 5.1.2 Valinta

Turvamekanismi

Kaikkien työnhakijoiden, toimittajien ja ulkopuoleisten käyttäjien taustat tulee tarkistaa noudattaen asiaan liittyviä lakeja, määräyksiä ja eettisiä normeja. Tarkistusten tulee myös olla suhteellisia ottaen huomioon liiketoimintavaatimukset, käsiteltävän tiedon luokitus ja oletetut riskit.

Keskuspuiston tilanne

Henkilöstön hankinnassa on pääämääränä mahdollisimman pätevä ja yhteistyökykyinen henkilökunta. Valinnassa kiinnitetään huomiota:

- koulutukseen ja kokemukseen perustuvaan ammatilliseen pätevyyteen
- palvelualttiuteen
- yhteistyökykyyn työyhteisössä ja hyviin vuorovaikutustaitoihin
- kykyyn palvella säätiön asiakkaita heidän omalla äidinkielellään.

(Laatukäsikirja 2003)

### 5.1.3 Työsopimuksen ehdot

Turvamekanismi

Osana sopimusvelvoitteitaan työn tekijöiden, toimittajien ja ulkopuolisten käyttäjien tulee hyväksyä ja allekirjoittaa työsopimuksensa ehdot, joiden tulee ilmaista niin heidän kuin organisaation vastuut tietoturvallisuudesta.

Keskuspuiston tilanne

Keskuspuiston työsopimuksessa ei ole mainintaa työntekijän tai organisaation vastuista tietoturvallisuuden suhteen. Työsopimuksen solmimisen yhteydessä käydään läpi perehdyttämissuunnitelman mukaiset asiat. Suunnitelmasta puuttuu osio, jossa perehdyttäminen tietokoneen turvalliseen käyttöön, tietoturvaan yleensä sekä luottamuksellisen ja arkaluonteisen tiedon käyttöön (Perehdyttämissuunnitelma 2009).

## 5.2 Työsuhteen aikana

Tavoite Varmistaa, että työntekijät, toimittajat ja ulkopuoliset käyttäjät ovat tietoisia tietoturvallisuuteen kohdistuvista uhkista ja niiden merkityksestä, omista velvollisuuksistaan ja vahinkovastuustaan ja että heillä on keinot tukea organisaation turvallisuuspolitiikkaa tehdessään normaalia työtään, sekä vähentää inhimillisen erehdyksen riskiä.

Tietosuojalakien säännöksiä sovelletaan silloin, kun käsitellään henkilötietoja. Henkilötietolain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Henkilötietoja käsiteltäessä on noudatettava henkilötietolakia, jollei muualla laissa toisin säädetä. Henkilötietolain mukaan henkilötiedoilla tarkoitetaan kaikenlaisia luonnollisia henkilöitä, heidän ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, joista heidät tai heidän perheenjäsenensä voidaan tunnistaa. Henkilö pitää siis olla tunnistettavissa. Jos tiedoista ei voida tunnistaa yksittäistä henkilöä, kyseessä ei ole henkilötieto (HEPO, 2002).

Laissa yksityisyyden suojasta työelämässä säädetään, että työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamisiin tai työnantajan työntekijöille tarjoamiin etuisuuksiin taikka johtuvat työtehtävien erityisluonteesta. Tästä ei voida poiketa edes työntekijän suostumuksella. Tarpeellisuus voi johtua mm. työnsuorittami-

sesta, työolosuhteista, työsuhteessa aiheutuvien velvoitteiden hoitamisesta tai työtehtävien erityisluonteesta (HEPO, 2002).

Sen lisäksi, mitä tässä on ohjeistettu, noudatetaan Invalidisäätiön yleistä tietosuojaohjetta, henkilöstölakia, lakia yksityisyyden suojasta työelämässä ja lakia lasten kanssa työskentelevien rikostaustan selvittämisestä (HEPO, 2002).

### 5.2.1 Johdon vastuut

Turvamekanismi

Johdon tulee edellyttää, että työntekijät, toimittajat ja ulkopuoliset käyttäjät noudattavat turvallisuutta organisaatioon luotujen periaatteiden ja menettelytapojen mukaisesti.

Keskuspuiston tilanne

Säätiön henkilöstöhallinto on hajautettu. Kunkin yksikön johtaja tai vastuualueen esimies toimii alaistensa välittömänä esimiehenä vastaten työsuhteen ehtojen noudattamisesta työyhteisössään. Henkilöstön työsuhteeseen liittyvien lakien, työehtosopimusten ja muiden määräysten ja ohjeiden yhdenmukaisesta noudattamisesta vastaa talouspäällikkö (1.1.2009 alkaen rehtori) palkkatoimiston esimiehenä. Käytännössä jokainen työntekijä kuuluu johonkin tiimiin, jonka esimiehenä on tiiminvastaava. Tiimien esimiehenä on toimialajohtaja.

### 5.2.2 Tietoturvatietous, -koulutus ja -harjoittelu

Turvamekanismi

Kaikille organisaation työntekijöille ja tarvittaessa myös toimittajille ja ulkopuolisille käyttäjille tulee antaa organisaation periaatteita ja ohjeita sekä niissä tapahtuvia muutoksia koskevaa asiaankuuluvaa koulutusta heidän toimenkuvansa kannalta tarkoituksenmukaisella tavalla.

Keskuspuiston tilanne

Koulutus suoritetaan organisaation perehdyttämissuunnitelman mukaisesti. Tietoturva osuuteen olisi syytä kiinnittää suurempaa huomiota.

### 5.2.3 Sanktiomenettely

Turvamekanismi

Työntekijöille, jotka ovat rikkoneet turvasäännöksiä, tulee määritellä sanktiomenettelyt.

Keskuspuiston tilanne

Työntekijää, joka on tehnyt virhetoimintoja, pyritään ohjaamaan oikeiden toimintatapojen käyttämisessä. Virhetoimintojen jatkuessa vähennetään oikeuksia toimia kyseisellä alueella.

## 5.3 Työsuhteen päättyminen ja muuttuminen

Tavoite Varmistaa, että työntekijät, toimittajat ja ulkopuoliset käyttäjät jättävät organisaation tai muuttavat työsuhdettaan järjestyksenmukaisella tavalla.

### 5.3.1 Päättämisvastuut

Turvamekanismi

Vastuut työsuhteen päättämisestä tai työsuhteen muuttamisesta tulee määrittää ja jakaa selkeästi.

Keskuspuiston tilanne

Vastuut työsuhteen päättämisestä tai työsuhteen muuttamisesta on määritelty HEPO:ssa, Invalidisäätiön henkilöstöpoliittisessa ohjekirjassa. Rehtori solmii työsuhteet johtotason työntekijöiden kanssa ja toimialajohtajat muiden työntekijöiden kanssa. He ilmoittavat tapahtuneista muutoksista työsuhteissa järjestelmähallinnalle sähköpostitse tai puhelimitse riippuen asian kiireellisyydestä.

### 5.3.2 Suojattavan omaisuuden palauttaminen

Turvamekanismi

Kaikkien työntekijöiden, urakoitsijoiden ja ulkopuolisten käyttäjien tulee palauttaa kaikki hallussaan oleva organisaation suojattava omaisuus työsuhteen tai sopimuksen päättyessä.

Keskuspuiston tilanne

Kaikkien työntekijöiden, urakoitsijoiden ja ulkopuolisten käyttäjien on palautettava kaikki hallussaan olevat organisaation kohteet työsuhteen tai sopimuksen päättyessä.

### 5.3.3 Käyttöoikeuksien poistaminen

Turvamekanismi

Kaikkien työntekijöiden, urakoitsijoiden ja ulkopuolisten käyttäjien käyttöoikeudet tietoon ja tietojenkäsittelypalveluihin tulee poistaa heidän työsuhteensa tai sopimuksensa päättyessä tai käyttöoikeuksia tulee korjata muutosten mukaisesti.

Keskuspuiston tilanne

Kaikkien työntekijöiden, urakoitsijoiden ja ulkopuolisten käyttäjien on palautettava kaikki hallussaan olevat organisaation laitteet ja niihin liittyvät käyttöoikeudet työsuhteen tai sopimuksen päättyessä.

# 6 FYYSINEN TURVALLISUUS JA YMPÄRISTÖN TURVALLISUUS

Fyysisen ympäristön suojauksella käsitetään sekä organisaation tuotanto- ja toimitilojen että siellä sijaitsevien tietojenkäsittelylaitteiden fyysistä suojaamista. Tällä ehkäistään niiden riskien ja vahinkojen toteutumista, jotka aiheutuvat joko valtuudettomasta fyysisestä pääsystä organisaation tiloihin, tietoihin ja tietojärjestelmiin tai fyysisestä ympäristöstä (kuten virransyöttö tai jäähdytys).

Standardi ISO/IEC 27002ohjeistaa käymään läpi ainakin seuraavat osa-alueet.

Fyysisen ympäristön suojaus koostuu kiinteistöjen ja tilojen suojauksesta rakenteellisesti, kulunvalvonnan osalta, teknisestä valvonnasta ja vartioinnista, erilaisten palo-, vesi-, sähkö-, murto- ja muiden vahinkojen sekä ihmisten virheellisestä toiminnasta johtuvien vahinkojen torjunnasta. Tärkeät tiedot ja tietojärjestelmät on säilytettävä tietojen kriittisyyden huomioon ottavissa ja säilytystarkoitukseen soveltuvissa turvallisissa tiloissa. Tyypillisiä uhkia ovat puutteellisista määrityksistä tai puutteellisesta toiminnasta ja ohjeistuksesta johtuvat uhkat.

Tietojärjestelmien ohella suojataan myös esimerkiksi laitetilat ja tietoliikennekaapelit. Jotta arkaluonteiset tiedot eivät olisi saatavilla ilman asianmukaisia valtuuksia organisaation sisällä tai kolmansille osapuolille, on luotava käytännöt toimitilojen, toimistotilojen ja työhuoneiden suojaamiseksi ja erityiset ohjeet näyttöpäätteillä, työpöydillä ja jaetuissa tulostimissa ja telefax-laitteissa näkyvien tietojen suojaamiseksi. Toimitilojen suojaamisessa täytyy erityistä huomiota kiinnittää tiloihin, joissa käsitellään asiakas- ja potilastietoja ja jossa voi oleilla potilaita, asiakkaita, heidän omaisiaan tai ulkopuolisia henkilöitä. Tällaisia tiloja ovat esimerkiksi kaikki vastaanotto- ja odotustilat, hoito- ja toimenpidetilat ja -huoneet sekä osastot.

Organisaation tilojen ulkopuolella sijaitsevien tietojen ja tietojärjestelmien suojaamisesta täytyy huolehtia asianmukaisesti. Näitä ovat sekä kolmansien osapuolten hallussa olevat järjestelmät (kuten ulkoistetut ja huollossa olevat) että organisaation henkilöiden hallussa olevat laitteet (kuten kotitietokoneet, kannettavat tietokoneet, mukana kuljetettavat paperit ja muut dokumentit, USB-avaimet ja matkaviestimet).

Omaisuuden viemiseen organisaation tilojen ulkopuolelle on oltava valtuutusmenettely. On varmistuttava, että käytöstä poistettaviin tietojärjestelmiin, esimerkiksi kovalevyille, ei jää tietoja ulkopuolisten saataville. Kaikkia niitä organisaation tiloja tai organisaation ulkopuolisia tiloja, jotka ovat joko fyysisesti suojattuja tai fyysistä suojausta edellyttäviä ja joissa voi sijaita tai käsitellään esimerkiksi arkaluonteisia tietoja, kutsutaan myöhemmin turvatiloiksi. Turvatilat voivat olla luokiteltuja esimerkiksi sen mukaan, millaisia ja kuinka arkaluonteisia tietoja siellä säilytetään.

Esimerkiksi tietokone- ja ti etoliikennelaitteille va rattuja huoneita ja konesaleja voidaan kutsua korkean turvallisuuden tiloiksi.

## 6.1 Turva-alueet

Tavoite Estää luvaton tunkeutuminen organisaation toimitiloihin ja tietoaineistoihin sekä estää niiden vahingoittuminen ja toiminnan häiriintyminen.

### 6.1.1 Fyysinen turva-alue

Turvam ekanismi

Turvatilojen, siis n iiden tilo jen, jo issa säilyte tään tie toja ja tie tojärjestelmiä, on oltava riittävän tukevia ja suojattuja estämään valtuudeton pääsy tietoihin. Tä mä sisältää seinä-, la ttia- ja k attorakenteet, ove t ja m uut sisäänkäynnit sekä ikkunat.

Keskuspuiston tilanne

Koulun korkean turvallisuuden tiloik si voidaan laskea palvelinhuone ja tietohallinnon työhuone. Tietohallin non koneilta on periaatteessa pääsy moneen kriittiseen kohteeseen verkon kautta, mutta koneet ovat suojattuja.

Palvelinhuone sijaitsee m aatasossa kukkulan laella, josta m aa viettää alamäkeen eikä kerää vettä sisään. Tulvim isvaara ul koapäin on hyvin pieni. Sähkönsaantia on varmistettu UPS-laitteella, se turvaa palvelimien hallitun alasajon. Tulipalon varalle tilassa on palonilmaisin ja savunilmaisin, jotka on kytketty kiin teistön palonilm oitinjärjestelmään. Jäähdytinlaitteisto 10kW, estää liian korkeat läm pötilat palvelinhuoneessa (Turvakan sio 2008).

Tilan s einät ovat p aksua kive ä ja o vi palonk estävä luko llinen m etalliovi. Ulkoseinäelementteinä ovat tukevat puusta ja lasista valm istetut osat. Tämä seinä on tilan heikoin kohta, mutta ei vaarallisen heikko.

Tilaa on e ristetty yleisestä tiloista lukitulla ovella. Avaimia oveen on jae ttu rajatus ti avainhenk ilöille ja ava imista pidetään kirjaa. Lukossa on loki auditointia varten. Tilassa ei o le merkintöjä, jotka paljastaisivat tilan luonteen. Sisään pääsevät ainoastaan oike utetut henkilöt. Vieras huoltohenkilöstö pääsee sisään ainoastaan saatettuna.

Varmuuskopiolaitteet o vat s amassa tilass a kuin palve linlaitteet, tämä o n selvä riskitekijä. Asia vaikuttanee myös vakuutuskorvauksiin.

Tietohallinnon työhuone on lukittu tila rak ennuksen yläkerro ksessa ilman vesipisteitä. Ovi on ohjeistettu lukittavaksi kun kukaan ei ole paikalla. Tietokoneet vaativat käyttä jätunnuksen salasanan kirj autumisen yhteydessä. Avaimia oveen on jaettu rajatus ti avai nhenkilöille ja avaimista pidetään kirjaa. Huoneessa on kiinteistön hälyty sjärjestelmään kytketty palonilmaisin.

### 6.1.2 Kulunvalvonta

Turvam ekanismi

Kaikki turvatilat on s uojattava riittävin kulu nvalvontakontrollein. On huomattava, että fyysistä kulunvalv ontaa vastaavat m ekanismit on syytä ottaa käyttöön m yös kaikkeen pääs yyn sähköisessä m uodossa oleviin tietoihin. Tämä koskee sekä oikeuksien määrittelyä että tapahtumien kirjausta.

Keskuspuiston tilanne

Organisaatiossa on riko sturvallisuutta kehitetty asentam alla kiin teistöön kulunvalvontajärjestelmä, antam alla henkilökunnalle kuvalliset henkilökortit, sekä asentam alla riskikohteis iin teknisiä järjestelm iä mm. rikosilmoitinjärjestelmä ja kam eravalvonta. Tekniset järjestelm ät auttav at v artijoiden työssä ja nopeuttavat avunsaantia ongelmatilanteissa. (Turvakansio, 2008)

Jokaisen ty öntekijän velvollisuus on ilm oittaa epäilyttäv istä henkilö istä vartioille, tai puhelinvaihteeseen. Jokainen on henkilökohtaisesti vastuussa hallussaan olevista avaim ista, kulkutunnisteista ja henkilökorteista. Mikäli henkilö hukkaa korttinsa, avaim ensa tai kulkutunnisteensa hän on velvollinen ilmoittamaan siitä välittömästi tekniseen toimistoon. Kortin, avainten tai kulkutunnisteen lainaaminen toiselle henkilölle on ehdottomasti kiellettyä. (Turvakansio, 2008)

Koulu sijaitsee sam assa rakennuksessa sairaalan kanssa. Rakennus on keskimäärin yli 50 vuotta vanha ja sis äänkäyntejä on paljon. Koulussa ja sairaalassa käy paljon liikuntarajoitteisia ihm isiä, joten ovien lukitsem ista ei ole pidetty hyvänä vaihtoehtona ainakaan toistaiseksi. R akennuksessa kulkee paljon ihm isiä. Opiston puolella osastojen ovet on suljettu m uuna kuin työaikana. Luokkahuoneet ja työpajat ovat tavallisesti auki työaikana. Erikoisluokissa on poikkeavia käytäntöjä . Opettajien ja toim istohenkilöiden työhuoneet ovat lukittuja, kun kukaan ei työskentele niissä. Osastojen käytävien liikennettä seurataan jatkuv asti ja vieraiden liikkumista opastetaan tiedusteluin. Toim istohenkilökunnan työhuoneiden ovet ovat lukittuja, kun huoneessa ei ole ketään ja m onitorit on käännetty poispäin sisäänkäynti-ovista, jotta salakatselu estyisi.

### 6.1.3 Toimistojen, tilojen ja laitteistojen suojaus

Turvamekanismi

Toimistojen, tilojen ja laitteis tojen fyysinen turv allisuus tulee suunnitella ja toteuttaa.

Keskuspuiston tilanne

Opettajien ja toim istohenkilöiden työhuoneet ovat lukittuja kun kukaan ei työskentele niissä. Osastojen käytävie n liikennettä seurat aan jatkuvasti ja vieraiden liikkumista opastetaan ti edusteluin. Toimistohenkilökunnan työhuoneiden ovet ovat lukittuja, kun huoneessa ei ole ketään ja monitorit on

käännetty poispäin sisääntulo-ovista, jotta salakatselu es tyisi. Työpäivän päätyttyä työhuoneiden ovet lukitaan.

### 6.1.4 Suojaus ulkoisia ja ympäristön aiheuttamia uhkia vastaan

Turvamekanismi

Fyysinen suojaus tulipa lojen, tulvien, maanjäristysten, räjähdysten, mellakoiden ja muiden luonn ollisten tai ihm isten aih euttamien katas trofien varalta tulee suunnitella ja toteuttaa.

Keskuspuiston tilanne

Samassa rakennuksessa sijaitsee sairaala. Rakennus on tehokkaasti suojattu paloilmaisimin ja hälytysjärjestelmä on kytketty suora an pelastuslaitokselle. Rakennus on jatkuvasti vartioitu.

### 6.1.5 Turva-alueella työskentely

Turvamekanismi

Turva-alueella työskentelyn fyysinen suojaus ja ohjeet tulee suunnitella ja toteuttaa.

Keskuspuiston tilanne

Turva-alueille pääsee vain järjestelmäasiantuntijan kanssa saatettuna.

### 6.1.6 Julkinen pääsy, toimitukset ja kuormausalueet

Turvamekanismi

Kulkualueita, kuten toim itus- ja kuorm ausalueita, sekä muita pisteitä, joiden kautta luvattom at henkilöt saattavat päästä tiloihin, tulee valvoa ja ne tulee mahdollisuuksien mukaan eristää tietojenkäsittelypalveluksista luvattoman pääsyn estämiseksi.

Keskuspuiston tilanne

Kulkualueilla ei ole opasteita turva-aluille ja kaikki turva-alueet on eristetty lukituin ovin ilman tunnistetietoja. Kuormausaluilla on kameravalvonta.

## 6.2 Laiteturvallisuus

Tavoite Estää omaisuuden häviäminen, vahingoittuminen, varastaminen tai vaarantuminen sekä organisaation toiminnan keskeytyminen.

### 6.2.1 Laitteiden sijoitus ja suojaus

Turvamekanismi

Suojataan laitteistot asianm ukaisesti siten, että estetään mahdollisuudet niiden varastamiseen tai vahingoittam iseen sekä niiden vahingoittum iseen

ympäristöstä johtuvista tekijöistä. Sijoituksessa kiinnitetään huomiota valtuudettoman tietoihin pääsyn estämiseksi kaikissa tilanteissa, myös korjaus- ja huoltotoimien yhteydessä.

Keskuspuiston tilanne

Järjestelmälaitteet on sijoitettu suojattuihin tiloihin. Varmuuskopiointi on sijoitettu fyysisesti samaan tilaan kuin pääpalvelimet. Tämä on iso tietoturvariski ja vakuutusriski. Esim erkiksi tulipalon sattuessa suuren vahingon mahdollisuus on ilmeinen. Järjestelmän hallinnan mahdollistavat ohjaustietokoneet ovat suojatussa tilassa ja koneet on suojattu salasanoin.

Julkisissa tiloissa olevat tietokoneet (kirjasto, luokkahuoneet ja osa henkilökunnan työkoneista) on suojattu Lenten Reborn korteilla. Tämä palauttaa koneet alkutilanteeseensa käynnistyksen yhteydessä. Korttien käyttö on lisäänty mässä. Niitä asennetaan atk-luokassa oleviin koneisiin, jotka ovat monen käyttäjän koneita. Toimenpide on rauhoittanut häiriökäytöstä. Näillä koneilla ei ole tietosuojattavaa aineistoa.

Henkilökunnan tietokoneet on sijoitettu suojatusti lukittaviin työhuoneisiin. Ovet lukitaan poistuttaessa ja kirjautuminen ulos koneelta on automatisoitu. Vieraat eivät saa kulkea osastoilla saattamatta. Kriittiset laitteet on sijoitettu suojatuille alueille.

Osalla opiskelijoita on käytettävissään henkilökohtainen kone, joissa on rajoitetut käyttöoikeudet ja rajoitettu pääsy lähiverkkoon. Tietotekniikan edistyneillä opiskelijoilla on täydet oikeudet omiin koneisiinsa ja omaan lähiverkkoonsa, joka on erotettu koulun lähiverkosta palomuurilla.

### 6.2.2 Kaapeloinnin turvallisuus

Turvamekanismi

Tietoliikenne ja tietoliikennevälineet on suojattava. On turvattava tietoliikenteen katkottomuus ja tietojen saatavuus sekä estettävä salakuuntelu ja tietojen muuttuminen niitä siirrettäessä.

Keskuspuiston tilanne

Runkokaapelit ovat valokuitua ja kerroskaapelit kuparia. Runkoverkko toimii 1Gb ja kerroskaapelointi 100Mb nopeudella. Kerroksissa 2,3,4,5 ja 6 on suljettu kerrosjakamo. Runkokaapelien nousujohdot kulkevat lukituissa kaapelikuiluissa. Siirto kaapelikuilusta kerrosjakamoon kulkee välikaton päällä tai korkealla olevilla kaapelihyllyillä. Kerroskaapeleihin pääsy huomaamatta on hankalaa, mutta ei mahdotonta.

### 6.2.3 Laitteiden huolto

Turvamekanismi

Laitteistot huolletaan ja suojataan huollon ajaksi asianmukaisesti. Huollon tarpeessa olevien, huollettavien tai huoltoon kuljetettavien laitteiden sisäl-

tämien tietojen tuhoutuminen, vahingoittuminen ja valtuudeton pääsy niihin on estettävä.

Keskuspuiston tilanne

Suurin osa tietolaitteista huolletaan ja ylläpidetään oman järjestelmätuen avulla. Palvelimet huolletaan omalla paikallaan luotettavan toimittajan kanssa saatettuna.

### 6.2.4 Toimitilojen ulkopuolelle vietyjen laitteiden turvallisuus

Turvamekanismi

Organisaation ulkopuolella sijaitsevien tietojen ja tietojärjestelmien suojauksesta on huolehdittava vastaavalla tavalla kuin huolehditaan organisaation tiloissa olevasta suojauksesta. Työskentelytavat on mukautettava ulkopuolisiin olosuhteisiin. On kiinnitettävä erityistä huomiota kannettavan tietokoneen käyttöön, säilytykseen ja tietojen suojaamiseen, mukana kuljetettavien paperitulosteiden säilytykseen ja kommunikointiin esim erkiksi matkapuhelimella.

Keskuspuiston tilanne

Tietosuojatut sähköiset dokumentit sijaitsevat koulun palvelimilla osana oppilasrekisteriä tai opetushenkilöstön kotikansioita. Työasemilla ei ole tarkoitus säilyttää tietosuojattuja aineistoja, eikä siten myöskään kannettavilla koneilla. Kannettavista tietokoneista on pidettävä hyvää huolta ja huomioitava tietoturva kaiken aikaa.

### 6.2.5 Laitteistojen turvallinen käytöstä poistaminen ja kierrättäminen

Turvamekanismi

Kaikista organisaation käytöstä poistettavista tietojärjestelmistä on tutkittava esimerkiksi kovalevyille jääneet tiedot, kuten arkaluon teiset ja luottamukselliset tiedot. On varmistettava, että tietoa ei katoa eikä joudu asiattomiin käsiin. Samaa varmistetaan myös tuhottavien tietovälineiden, kuten levykkeiden, cd-levyjen ja vastaavien osalta. Käyttökelpoiset osat kierrätetään kun se voi tapahtua tietoturvaa vaarantamatta.

Keskuspuiston tilanne

Käyttökoneet kierrätetään ylikirjoittamalla kovalevyt. Koneiden kunto tarkistetaan ja ne korjataan tai päivitetään. Työn tekee järjestelmätuki tai tietotekniikan opiskelijat opettajan ohjauksessa.

### 6.2.6 Suojattavien kohteiden siirtäminen pois työpaikalta

Turvamekanismi

Laitteita, tietoaineistoja tai ohjelmia ei saa siirtää pois työpaikalta ilman ennalta saatua valtuutusta.

Keskuspuiston tilanne

Suojattavia laitteita ei siirretä pois vaan ne huolletaan koulun tiloissa.

# 7 TIETOLIIKENTEEN JA KÄYTTÖTOIMINTOJEN HALLINTA

Yksi organisaation toim innan ja to imintakyvyn varm istamisen oleellinen osa on varm istaa organisaation kaikkien henkilöiden o ikeanlainen ja turvallinen tehtävien hoito ja tietojärjestelmien käyttö.

## 7.1 Menettelyohjeet ja velvollisuudet

Turvamekanismi

Määrittämällä eri tehtävissä toimivien henkilöiden tarkat vastuut, velvollisuudet ja valtuudet luodaan pohja tietot urvapolitiikan m ukaiselle toim innalle, jotka täydennetään tarvittavilla käyttö- ja toimintaohjeilla. Jakamalla tarvittaessa vastuut osiin ja eriyttämällä ne useammalle henkilöille voidaan ehkäistä m ahdollisuus tärkeid en ja kriitt isten tietojen ja tie tojärjestelmien väärinkäyttöön ja huolimattomuudesta aiheutuviin riskeihin.

Kaikkien tietojärjestelmien käyttäjien on siis tie dettävä, miten järjestelmiä pitää ja saa käyttä ä ja mihin ta rkoitukseen niitä käytetään, s ekä m illainen käyttö on kiellettyä. Kaikkien henkilöid en, jotka käsittelevät järjestelmien sisältämiä tietoja, on tunnettava oikeanlaiset ja sallitut käsittelytavat ja käsittelysäännöt.

Keskuspuiston tilanne

Järjestelmätuen tehtävät on hajautet tu sen työntekijöille. Vastuunalaisimmat tehtävät ovat toim ivuosiltaan v anhimmilla toim enhaltijalla ja m uilla on omat vastattavat sektorinsa. Kykyä toimia toistensa varamiehinä on sopivasta olem assa, vaarantam atta kuitenkaan koko järjestelm än ole massaoloa.

Ennen vuotta 2009 järjestelm ätuki on o llut fyysisesti sijo itettuna pääkoululle ja etäpisteitä, lukum äärältään n. 20 kappaletta, palveltiin pääkoululta käsin. Etäpisteet ovat pieniä tai keskisuuria. Vuoden 2009 alussa Arla-instituutti tuli osaksi Keskuspuistoa. Lisäksi Keskuspuist on Metsälän yksikkö on kasvam assa suureksi yksiköksi. Vanhat m enettelytavat eivät tule riittämään, ne kaipaavat uusimista. Kirjalliset yhtenäiset toimintaohjeet on laadittava.

Turvamekanismi

Menettelyohjeet tu lee d okumentoida, niitä tu lee ylläpitää ja niiden tulee olla kaikkien niitä tarvitsevien käyttäjien saatavilla.

Keskuspuiston tilanne

Ainoastaan suulliset sopimukset ovat olemassa ja ne ovat toim ineet hyvin. Arla-instituutin liittym inen organisaa tion on lisännyt tarvet ta kirjalliselle ohjeistukselle. Kirjalliset ohjeet ovat työn alla ja valmistuvat lähiaikoina.

### 7.1.1 Muutosten hallinta

Turvamekanismi

Tietojärjestelmien kehityksessä, testauksessa ja tuotantoon otossa noudatetaan täsmällisiä ohjeita ja menettelyitä, jotta kehitystoiminta ei avaa portteja turvariskeille ja jotta voidaan varmistua, että käyttöön otettavat tuotteet ja palvelut eivät vaaranna tietoturvallisuutta. Myös toimittaessa kolmansien osapuolten kanssa luodaan sellaiset käytännöt, joilla voidaan taata, ettei organisaation tietoturvallisuus vaarannu.

Keskuspuiston tilanne

Järjestelmiä uusitaan tarvittaessa ja kun markkinoilta on saatavissa koeteltuja ja varmasti toimivia uusia tai pä ivitysversioita järjestelmän osista. Nämä hankitaan yhteistyössä yhteistyökumppaneiden kanssa siinä vaiheessa kun lastentaudit on saatu korjatuiksi ja osat jo toimivat virheittä muualla.

### 7.1.2 Tehtävien eriyttäminen

Turvamekanismi

Tehtävät ja vastuualueet tulee eriyttää, jotta vähennetään organisaation suojattavien kohteiden luvattoman ja tahattoman muuntelun ja väärinkäytön riskiä.

Keskuspuiston tilanne

Järjestelmätuen tehtävät on hajautettu sen työntekijöille. Vastuunalaisimmat tehtävät ovat toimivuosiltaan vanhimmilla toimenhaltialla ja muilla omat sektorinsa, mistä vastaavat. Kukyä toimia toistensa varamiehinä on sopivasta olemassa, vaarantamatta kuitenkaan koko järjestelmän olemassaoloa.

### 7.1.3 Kehitettävänä, testattavana ja tuotannossa olevien palveluiden erottaminen

Turvamekanismi

Kehitettävät, testattavat ja tuotannossa olevat palvelut tulee erottaa toisistaan, jotta pienennetään tuotantojärjestelmän luvattoman käytön ja muutosten riskiä.

Keskuspuiston tilanne

Tuotantojärjestelmässä ei tehdä testejä. Jos testejä on suoritettava, niitä varten luodaan oma testausympäristö.

## 7.2 Ulkopuolisten palvelujen toimittamisen hallinta

Tavoite Käytettäessä kolmansien osapuolten palveluita ja tuotteita on huolehdittava, että kaikessa toiminnassa ja yhteistyössä otetaan huomioon tietoturvallisuus ja noudatetaan laadittuja toimintamalleja. Kolmannen osapuolen on osaltaan noudatettava kaikkia niitä käytäntöjä, joita siltä edellytetään. Turvallisuus täytyy huomioida sekä sopimuksellisesti, käytännön toiminnassa

ja tietojen vaihdossa että käytettävissä teknisissä ratkaisuissa (sähköposti, kulunvalvonta, huolto ym.). Turvallisuutta täytyy tarkkailla ja rikkeisiin puuttua sovitun mukaisesti.

### 7.2.1 Palvelujen toimittaminen

Turvamekanismi

On varmistettava, että ulkopuolinen palveluntoimittaja toteuttaa, käyttää ja ylläpitää sopimukseen sisällytettyjä turvamekanismeja, palvelunmäärittelyjä ja toimitustasoja.

Keskuspuiston tilanne

Kriittisten palvelujen toimittamisessa organisaation edustaja on aina paikalla varmistamassa asiankuuluvan toiminnan.

### 7.2.2 Ulkopuolisten palvelujen tarkkailu ja katselmointi

Turvamekanismi

Ulkopuolisen tahon toimittamia palveluja, raportteja ja tallenteita tulee tarkkailla ja katselmoida säännöllisesti. Tarkastuksia tulee myös suorittaa säännöllisesti.

Keskuspuiston tilanne

Ulkopuoleisia verkkopalveluja ovat: www-sivut, Moodle, Pedanet. Näitä palveluja seuraavat ja valvovat ne tahot, jotka ovat sen tehtäväksi saaneet, www-sivuja valvoo markkinointi, Moodlea sen hallintaoikeuksin varustetut käyttäjät ja Pedanetiä valmentavan puolen hallintaoikeuksin varustetut käyttäjät.

## 7.3 Järjestelmän suunnittelu ja hyväksyntä

Turvamekanismi

Tietojärjestelmien ja tietoverkkojen hallinnan ja hoidon vastuut on oltava riittävän asiantuntemuksen omaavilla henkilöillä, ja hallintatehtävien hoitoon on varattava riittävästi henkilö- ja muita resursseja sekä tarvittavia apuvälineitä ja työkaluja. Vastuuhenkilöt tuntevat ja tietävät järjestelmät ja toimintaohjeet, joita noudattamalla ylläpidetään järjestelmien ja tietoverkkojen turvallisuutta, toimintakuntoa, käytettävyyttä ja hallitaan järjestelmien käyttäjiä. Järjestelmien toimintaa seurataan ja erilaisissa vika-, ongelma- ja kuormitustilanteissa ryhdytään asianmukaisiin toimiin. Seurantatietoa käytetään hyväksi suunnittelutehtävissä.

Keskuspuiston tilanne

Järjestelmästä vastaa järjestelmätuki. Vika- ja ongelmatilanteista pidetään kirjaa. Näitä tietoja käytetään hyväksi ylläpidettäessä ja parannettaessa järjestelmää.

### 7.3.1 Kapasiteetin hallinta

Turvamekanismi

Resurssien käyttöä tulee tarkkailla ja säätää sekä tehdä ennusteita tulevista kapasiteettivaatimuksista, jotta voidaan varmistaa järjestelmältä vaadittava suorituskyky.

Keskuspuiston tilanne

Järjestelmätuki seuraa verkon liikennettä hallittavilta kytkimiltä säännöllisesti. Palvelimien liikennettä ja palvelutoiminnan kuormitusta seurataan palvelimilta käsin. Ulkoista liikennettä seurataan ja kapasiteettivajeen uhatessa liikennöintikapasiteettia on nostettu. Ongelmien alkaessa ilmetä niihin puututaan järjestelmällisesti. Kapasiteettiongelmien alkaessa ilmetä, niihin haetaan sopiva ratkaisu. Laitteiden toimintaa seurataan ennakoivasti ja ongelmat pyritään ratkaisemaan ennen niiden toteutumista.

### 7.3.2 Järjestelmän hyväksyntä

Turvamekanismi

Uusien järjestelmien, järjestelmäpäivitysten ja uusien versioiden hyväksymiskriteerit tulee luoda ja kehityksen aikana ja ennen hyväksyntää on suoritettava riittävät testit.

Keskuspuiston tilanne

Uusiksi järjestelmiksi, järjestelmäpäivityksiksi ja uusiksi versioiksi hyväksytään vain käytännössä hyvin toimivia tuotteita, joiden toimivuus on varmistettu. Ennen uusimista toimivuus tarkistetaan yhteistyökumppaneilta ja tieto varmistetaan useammasta lähteestä.

## 7.4 Suojaus haittaohjelmia ja liikkuvia ohjelmia vastaan

Turvamekanismi

Erilaisilta haittaohjelmilta ja verkkohyökkäyksiltä on suojauduttava asianmukaisin keinoin, esimerkiksi käyttämällä virustorjuntaa, palomuureja ja verkkohyökkäysten havainnointiohjelmistoja (IDS, Intrusion Detection Software). Havaittujen haittaohjelmien tuhoaminen ja normaalitilaan paluu on oltava suunniteltua. Tuotantokäyttöön otettavien ohjelmistojen virheellisyyksistä on suojauduttava jo ohjelmistojen vaatimusmäärittely-, kehitys- ja testausvaiheissa ja niitä on tarkkailtava tuotantokäytön alettua.
Tietojärjestelmien ja työasemien käyttäjät on koulutettava ja ohjeistettava oikeanlaiseen tietojärjestelmien käyttöön, jotta haittaohjelmat eivät pääse organisaation tietojärjestelmiin eivätkä jatkaleviämistään. Käyttäjien on oltava tietoisia riskeistä, osattava havainnoida uhkatilan teita, tunnistaa mahdollisten virusten ja muiden vastaavien haittaohjelmien toiminta ja osattava toimia tilanteessa siten, että korjaustoimiin voidaan ryhtyä pikaisesti ja ongelmat saadaan ehkäistyä ja korjattua.
Haittaohjelmien havaitsemis- ja estotoimet sekä niistä toipumismekanismit ja asiaankuuluvat käyttäjien valppautta lisäävät ohjeet tulee ottaa käyttöön.

Keskuspuiston tilanne

Uudistettu palomuuri on käytössä ja sen toimintaa auditoidaan säännöllisesti. Sähköposti on suojattu haittaohjelmilta. Työasemat ja palvelimet on suojattu haittaohjelmien toiminnalta. IDS otetaan käyttöön lähipäivinä. Käyttäjien, etenkin uusien käyttäjien tietoturvakoulutukseen voisi kiinnittää lisää huomiota. Tämän hetkinen ohjeistus on niukahkoa, sitä voisi lisätä intranet-verkkoon.

## 7.5 Varmuuskopiointi

Turvamekanismi

Erilaisia vikatilanteita varten tietojärjestelmistä on otettava varmistukset, joilla voidaan tarpeen mukaan palauttua vikaa edeltäneeseen tilanteeseen. Varmistustoimet ovat mahdollisuuksien mukaan automatisoituja, mutta palautustoimissa noudatetaan aina etukäteen sovittuja proseduureja ja hyväksymismenettelyitä.
Vikatilanteita voivat olla esim erkiksi laitteiden ja levyjen vikaantumiset, tietojen tahaton korruptoituminen ohjelmisto- tai tietoliikennevirheiden vuoksi sekä käyttäjien tekemät tahattomat tiedostojen poistot tai ylikirjoitukset.

Keskuspuiston tilanne

Keskeiset verkkotoiminnot: Verkkokäyttöjärjestelmä, oppilasrekisteri ja poissaolorekisteri, taloushallinnon ohjelmat, sähköposti ja muut toiminnot on sijoitettu palvelinklusteriin. Siellä toiminnot on jaettu kahdelle palvelimelle. Poikkeustapauksissa toinen palvelin voi korvata molempien palvelimien toiminnot. Järjestelmä ei halvaannu yhden palvelimen häiriötilanteessa. Toiminnot tosin hidastuvat. Tämän ansiosta kaikki data on kahdessa paikassa. Pikavarmuuskopioita tehdään palvelinlevyille. Varsinaiset varmuuskopiot tehdään palvelinhuoneessa olevalle nauharobotille, ne tehdään automaattisesti ja säännöllisesti. Varmuuskopiorobotti on väärin sijoitettu, se on samassa tilassa ja samassa palo-osastossa kuin palvelimet. Suunnitelma robotin siirtämiseksi toiseen palo-osastoon on olemassa ja sen toteuttaminen on aloitettu. Suunnitelmaan sisältyy myös osa, jossa käsitellään erillisen varmuuskopionauhaerän tekemistä ja sen sijoittamista toiseen varmaan paikkaan. Palautuksia varmuusnauhoilta on tehty onnistuneesti. Kirjallisia ohjeita toiminnalle ei ole.

## 7.6 Verkon turvallisuuden hallinta

Tavoite Verkkopalveluiden ja tietoverkkojen käytöstä on oltava selkeät määräykset ja ohjeet, ja kaikkien verkkopalveluita käyttävien henkilöiden on tiedettävä säännöt ja noudatettava niitä.

### 7.6.1 Verkon turvamekanismit

Turvamekanismi

Tietojärjestelmien kehityksessä, testauksessa ja tuotantoon otossa noudatetaan täsmällisiä ohjeita ja menettelyitä, jotta kehitystoiminta ei avaa portteja turvariskeille ja jotta voidaan varmistua, että käyttöön otettavat tuotteet ja palvelut eivät vaaranna tietoturvallisuutta. Myös toimittaessa kolmansien osapuolten kanssa luodaan sellaiset käytännöt, joilla voidaan taata, ettei organisaation tietoturvallisuus vaarannu.

Keskuspuiston tilanne

Tarvittavat kehitys ja testaus jotsuoritetaan virtuaaliympäristössä. Tuotantoon otetaan vain koeteltuja ja muualla testiajettuja päivityksiä tai sovelluksia. Kolmansina osapuolina käytetään, jos vaan mahdollista, organisaatiolle tunnettuja ja luetettavaksi havaittuja osapuolia. Poikkeustapauksissa saattaminen toteutetaan erityistä varovaisuutta noudattaen.

### 7.6.2 Verkkopalvelujen turvaaminen

Turvamekanismi

Tietojärjestelmien ja tietoverkkojen hallinta ja hoito on oltava erityisen vastuullista toimintaa. Järjestelmäpäälliköt, pääkäyttäjät ja muut eri järjestelmistä ja sovelluksista vastaavat henkilöt, joilla yleensä on normaalikäyttäjää laajemmat valtuudet järjestelmien käyttöön, ovat soveltuvia vastuullisten tehtävien hoitoon. He ymmärtävät oikeuksien hallinnasta aiheutuvat uhkat, osaavat asennoitua vastuullisesti tehtäviinsä ja noudattaa tietoturvallisia menettelytapoja jokapäiväisissä toimissaan. Vastuuhenkilöiden koulutukseen ja osaamiseen kiinnitetään yleensä erityistä huomiota, koska esimerkiksi epäpätevät henkilöt, jotka eivät ole tehtäviensä tasalla tai joiden osaaminen on vanhentunutta, aiheuttavat tietoturvariskin.

Keskuspuiston tilanne

Tietohallintopäällikkö vastaa järjestelmän toiminnasta vuoden 2009 alusta. Hänellä on tukenaan tarvittava määrä eritasoisin pääkäyttäjäoikeuksin varustettuja henkilöitä, jotka on perehdytetty tehtäviinsä. He noudattavat tietoturvallisia menettelytapoja jokapäiväisissä toimissaan.

## 7.7 Tietovälineiden käsittely

Tavoite

Tietovälineiden, kuten asiakirjojen ja dokumenttien, nauhojen, cd-levyjen, levykkeiden, USB-muistien ja muiden tietokoneisiin liitettävien medioiden sekä järjestelmädokumentaation täytyy olla suojattu asianmukaisesti katoamiselta ja varkauksilta, valtuudettomalta pääsyltä ja valtuudettomalta muuttamiselta. Erityisesti arkaluontoisia tietoja sisältävät tietovälineet on suojattava; näitä tietoja sisältävät tietovälineet on suojattava vähintään sen tasoisesti kuin tietojen turvaluokitus edellyttää ja tietovälineiden käytöstä on oltava yksityiskohtainen ohjeistus.

### 7.7.1 Siirrettävän tietovälineen hallinta

Turvamekanismi

Erityisesti siirrettävien tietovälineiden (paperi, levykkeet, cd-levyt, USB-muistit) käytölle on oltava ohjeistus ei vätkä tällaisille tietovälineille talletetut suojattavat tiedot saa prosessin missään vaiheessa vaarantua.

Keskuspuiston tilanne

Tulostimet, joilla tulostetaan tietosuojattuja asiakirjoja sijaitsevat henkilökunnan miehitetyissä tai lukituissa työhuoneissa sijoitettuna paikkaan, johon ei ole suoraa pääsyä, eikä suoraa näkyvyyttä. Tällä estetään tulosteiden jääminen ajelehtimaan. Julkisia tulostimia käytetään vain suojaamattomien papereiden tulostamiseen. Jokaisella on oma USB-muistinsa, josta sen käyttäjä on henkilökohtaisessa vastuussa. Työasemiin, joita vierailevat luennoitsijat käyttävät, on asennettu tehostettu haittaohjelmien poisto-ohjelma.

### 7.7.2 Tietovälineen poistaminen käytöstä

Turvamekanismi

Tietovälineet tulee poistaa käytöstä turvallisella ja varmalla tavalla määriteltyjä menettelytapoja noudattaen, kun niitä ei enää alkuperäisessä tehtävässään tarvita.

Keskuspuiston tilanne

Tietovälineet käytetään useampaan kertaan. Ne kierrätetään alkuperäistä vaatimattomampiin tehtäviin, joissa ei tarvita suurta konetehoa. Kovalevyt tyhjennetään ylikirjoittamalla tarpeeksi monta kertaa. Opetuskäytössä olleet koneet kertaalleen ja henkilökunnan käytössä olleet koneet kolmeen kertaan, jonka jälkeen kovalevylle asennetaan uusi käyttöjärjestelmän asennus.

### 7.7.3 Tietojen käsittelyohjeet

Turvamekanismi

Tiedon käsittelyä ja tallennusta koskevat ohjeet tulee laatia tiedon suojaamiseksi luvattomalta paljastumiselta tai väärinkäytöltä.

Keskuspuiston tilanne

Organisaatiossa on käytössä ”puhtaan pöydän strategia” ja se on julkaistu henkilöstöstrategia asiakirjassa.

### 7.7.4 Järjestelmän dokumentoinnin turvaaminen

Turvamekanismi

Järjestelmän dokumentaatio tulee suojata luvattomalta käytöltä.

Keskuspuiston tilanne

Järjestelmän dokumentaatio on suojatussa paikassa verkossa ja saavutettavissa ainoastaan salasanan avulla.

## 7.8 Tiedonvaihto

Tavoite Ylläpitää organisaation sisällä tai jonkun ulkopuolisen tahon kanssa vaihdettujen tietojen ja ohjelmien turvallisuutta.

### 7.8.1 Tiedonvaihtoperiaatteet ja – menettelytavat

Turvamekanismi

Kaikentyyppisillä viestintäpalveluilla tapahtuvaa tiedon vaihtoa tulee suojata ottam alla käyttöön m ääritellyt tiedonvaihtoperiaatteet, m enettelyohjeet ja turvamekanismit.

Keskuspuiston tilanne

Menetelmät otetaan käy ttöön sitä mukaan kun niit ä tarvitaan. Turhaa tiedonsiirtoa vältetään. Luottam uksellista tietoa ei vaihdeta ulkopuolisten tahojen kanss a. Sisäise ssä vaihdossa pääsyoikeu det m äärittelevät jokais en oikeudet nähdä tarpeelliset tiedot. Oppilaan poissaoloja voivat seurata oppilas itse ja hänen huoltajansa käyttäjätunnuksen ja salasanan avulla.

### 7.8.2 Tiedonvaihtosopimukset

Turvamekanismi

Organisaation ja ulkopuolisten tahojen tulee laatia sopim ukset tiedon ja ohjelmien vaihdosta.

Keskuspuiston tilanne

Menetelmät otetaan käyttöön sitä mukaan kun niitä tarvitaan.

### 7.8.3 Fyysiset tietovälineet kuljetuksen aikana

Turvamekanismi

Tietoa sisältävät välineet tulee suojat a luvatonta pääsyä, väärinkäyttöä ja turmeltumista vastaan, kun niitä kuljetetaan organisaation fyysisten rajojen ulkopuolelle.

Keskuspuiston tilanne

Tietoa s iirretään eniten kannettavis sa tietokoneissa. Luo ttamuksellista tietoa ei saa siirtää tarp eettomasti kanne ttaviin kon eisiin, jotka viedään pois suojatusta työpisteestä. Tämän ollessa välttäm ätöntä on tieto salakirjoitettava ja luk ittava s alasanalla. Ohjeen m ukaista toim intaa jo kapäiväisessä käytössä ei ole seurattu.

### 7.8.4 Sähköinen viestintä

Turvamekanismi

Sähköisestiviestittyä tietoa tulee suojata asianmukaisesti.

Keskuspuiston tilanne

Luottamuksellista tietoa ei saa jakaa kuin luvan kanssa ja sillo in on varmistettava luottamuksellisuuden säilyminen siirron aikana.

### 7.8.5 Liiketoiminnan tietojärjestelmät

Turvamekanismi

Periaatteita ja menettelytapoja tulee kehittää ja toteuttaa suojaamaan liiketoiminnan tietojärjestelmien välisissä yhteyksissä käytettäviä tietoja.

Keskuspuiston tilanne

Organisaation sisäisessä tiedonsiirrossa eri toimipisteiden välillä käytetään suojattuja ja salattuja yhteyksiä, joilla suojataan tiedon eheyttä ja estetään väärinkäyttöä.

## 7.9 Verkkoasiointipalvelut

Tavoite Toiminnan tarkoitus on varmistaa verkkoasiointipalvelujen turvallisuus ja niiden turvallinen käyttö. Tietoturvakäytäntöjä, jotka liittyvät sähköisiin verkkoasiointipalveluihin ja verkon kautta välitettyihin tapahtumiin tulisi harkita, jotta tiedon eheys ja saavutettavuus taattaisiin käytettäessä julkisia verkkoja.

### 7.9.1 Verkkoasiointi

Turvamekanismi

Julkisissa verkoissa kulkevaa verkkoasiointiin liittyvää tietoa tulee suojata vilpilliseltä ja sopimuksen vastaiselta toiminnalta ja luvattomalta paljastamiselta ja muuttamiselta.

Keskuspuiston tilanne

Julkisissa verkoissa kulkeva liikennöinti ei ole suojattua. Kyse on enimmäkseen tiedonetsinnästä ja -hausta julkisista tietolähteistä. Tavallisimmat siirrot ovat sivustojen ja tiedostojen siirtoja, joita suojataan palomuurilla ja haittaohjelmien suojausohjelmilla. Sähköpostin käyttö on mahdollista suojatussa muodossa. Luottamukselliset tapahtumat ja siirrot suoritetaan suojatussa verkossa.

### 7.9.2 Verkon kautta välitetyt tapahtumat

Keskuspuiston Ammattiopistolla on alun kolmattakymmenettä toimintapistettä. Yhteyksien ylläpitoon käytetään Elisa Yritysverkkoa, se on yrityksille ja yhteisöille tarkoitettu tietoliikennekokonaisuus, jonka rakenta-

misessa verkkotekniikka ja liittymänopeudet valitaan asiakkaan tarpeiden mukaan. Liittymän peruspakettiin kuuluu asiakaspäätelaite, TCP/IP suljetussa VPN:ssä, 29 IP osoitetta sekä liityntäyhteys Elisan verkon liityntäpisteeseen. Toimipisteen liittymänopeudet voidaan valita kiinteillä liitynnöillä välillä 64 kbt/s – 1 000 Mbit/s saatavuuden mukaan. Reititin tai muu asiakaslaite on osa kokonaispalvelua.

Turvamekanismi

Verkon kautta välitettyihin tapahtumiin liittyvää tietoa tulee suojata, jotta estetään epätäydellinen lähetys, väärään paikkaan ohjaaminen, luvaton viestien muuttaminen, luvaton paljastaminen, luvaton viestin kopiointi tai toisto.

Keskuspuiston tilanne

Kaikki liikenne etäpisteisiin kulkee pääkoulun kautta, myös tavallinen IP-liikenne. Liikenne kulkee suojatussa VPN- putkessa. Tapahtumat esimerkiksi oppilasrekisteriin kulkevat suojattuna koko matkan.

### 7.9.3 Julkinen informaatio verkossa

Verkkopalveluiden yleistyttyä on tavallista, että organisaatio laajentaa julkaisukäytäntöjään ja julkaisee erilaista materiaalia verkkosivuillaan. On helposti löydettävissä runsaasti esimerkkejä organisaatioista, joissa toimintaprosesseja ei muuteta tietoja verkkoon julkaistaessa, ja niinpä verkkojulkaisemista ei liitetä normaaleihin julkaisukäytäntöihin. Tästä syystä verkkosivustoja ja niiden sisältämiä tietoja ei ylläpidetä vaadittavalla tavalla, ja verkosta saatavat tiedot voivatkin usein olla vanhentuneita ja jopa virheellisiä. Tämä puolestaan aiheuttaa erilaisia uhkia sekä organisaatiolle että sen palveluita käyttäville.

Turvamekanismi

Julkisissa järjestelmissä saatavilla olevan tiedon eheyttä tulee suojata, jotta estetään sen luvaton muuttaminen.

Keskuspuiston tilanne

Koulun www-sivujen säilytys on ulkoistettu. Sivujen päivitys, huolto ja seuranta tapahtuvat koululta käsin, jo sta huolehditaan sivujen eheydestä. Markkinointiosasto on vastuussa toiminnosta koulun puolelta. Tukea tietoturvaongelmiin saadaan palvelun tarjoajalta.

## 7.10 Tarkkailu

Luvattomia tietojenkäsittelytoimintoja on havainnoitava. Järjestelmiä on monitoroitava ja tietoturvatapahtumat tallennettava lokiin. Järjestelmätuen kirjautumisia ja virheellisiä kirjautumisia on seurattava ja siten varmistettava, että järjestelmäongelmat tunnistetaan. Organisaation on noudatettava kaikkia asianmukaisia ja laillisia toimenpiteitä havainnoidessaan järjestelmää ja kirjautumisprosesseja.

### 7.10.1 Tapahtumalokit

Turvamekanismi

Tapahtumalokit, joihin tallennetaan käyttäjien toiminta, poikkeamat ja tietoturvatapahtumat, tulee koota ja niitä tulee säilyttää sovittu aika myöhemmin tehtäviä tutkimuksia ja pääsyn valvonnan tarkkailua varten. Toiminnassa ei saa toimia lainvastaisesti.

Keskuspuiston tilanne

Tapahtumalokit kootaan salasanalla suojattuun, tavalliselle käyttäjälle näkymättömään paikkaan. Lokia pääsee katsomaan vain autentikoinnin kautta. oikeuksia on jaettu rajoitetusti. Lokeja seurataan säännöllisesti.

### 7.10.2 Järjestelmän käytön tarkkailu

Turvamekanismi

Menettelyohjeet tietojenkäsittelypalvelujen käytön tarkkailuun tulee laatia ja toimintojen tarkkailun tuloksia tutkia säännöllisesti.

Keskuspuiston tilanne

Suulliset ohjeet ovat olemassa ja niiden puitteissa järjestelmää monitoroidaan säännöllisesti ja suoritetaan tarvittavat toimenpiteet.

### 7.10.3 Lokitietojen suojaus

Turvamekanismi

Lokitietoja ja niiden kirjauspalveluja tulee suojata luvattomilta muutoksilta ja luvattomalta pääsyltä.

Keskuspuiston tilanne

Auktorisoidut käyttäjät pääsevät käsiksi suojattuihin lokitietoihin, muussa tapauksessa käyttäjän on murtauduttava järjestelmään. Muutoksista jää jälki lokitiedostoon.

### 7.10.4 Pääkäyttäjä- ja operaattorilokit

Turvamekanismi

Järjestelmän pääkäyttäjien ja operaattorien toiminnot tulee kirjata.

Keskuspuiston tilanne

Pääkäyttäjien ja operaattorien toiminnot kirjataan lokiin.

### 7.10.5 Häiriöiden kirjaus

Turvamekanismi

Häiriöt tulee kirjata ja analysoida ja ryhtyä asianmukaisiin toimenpiteisiin.

Keskuspuiston tilanne

Häiriöt kirjataan ja käydään läpi auditoinnin yhteydessä. Häiriöt analysoidaan, sen jälkeen laaditaan korjaussuunnitelma ja toteutetaan se, jonka jälkeen havainnoidaan toimiko korjaus. Jos korjaus ei toimi pohditaan tarvitaanko lisätoimenpiteitä. Jos ei, palataan alkupisteeseen ja pohditaan vaihtoehtoisia korjaustoimenpiteitä tai jatketaan askel kerrallaan valitulla tiellä. Suoritetut toimenpiteet kirjataan, jotta ne voidaan tarvittaessa kumota.

### 7.10.6 Kellojen synkronointi

Turvamekanismi

Kaikkien samassa organisaatiossa tai turvallisuusalueella olevien olennaisten tietojenkäsittelyjärjestelmien kellot tulee synkronoida sovitun tarkan ajanlähteen kanssa.

Keskuspuiston tilanne

Verkkokäyttöjärjestelmän laitteiden kellot on synkronoitu sovittuun ajanlähteeseen. Apulaitteet on synkronoitu sovitun tarkkuuden puitteissa sopivaan synkronointikelloon.

# 8 PÄÄSYOIKEUKSIEN VALVONTA

Yksi tietoturvallisuuden oleellisim mista osa-alueista on pääsynhallintaan liittyvät m äärittelyt ja toim enpiteet. Kuinka tietojä rjestelmien ja niissä olevien tietojen käyttö ja käyttäjät määritellään, kuinka käyttöoikeuksia ja käyttövaltuuksia hallitaan ja m illaisilla menetelmillä käyttäjät tunnistetaan ja heidän henkilöllisyytensä todennetaan.

## 8.1 Opetustoiminnan asettamat vaatimukset

Tavoite Keskuspuiston ammattiopisto on ammatillinen erityisoppilaitos, jonka asiakkaat eli oppijat ovat kohdanneet monia vaikeuksia terveyden ja oppimisen kanssa. Oppilaiden tietoturvasta ja tietosuojasta on huolehdittava pieteetillä hyödyntäen riittävää hetkeen sopivaa tekniikkaa.

### 8.1.1 Pääsynvalvonnan toimintaperiaatteet

Turvamekanismi

Pääsyn hallinnointi käsittää, millaisia politiikkoja, sääntöjä ja käytäntöjä hallinnointiin on käytettävissä ja käyt ettävä. Hallinno inti käsittää esim erkiksi oikeuksien määrittelyn: millaisia pääsyoikeuksia tieto ihin luodaan ja millaisia oikeuksia voidaan valtuuttaa er ityyppisille käyttäjille ja käyttäjäryhmille.

Keskuspuiston tilanne

Henkilökunnalla on yksilöll iset käyttäjätunnukset ja salasanat käytössä. Pyrkimyksenä on, että kaikki käyttäisivät turvallista salasanaa. Työasemille ja lähiverkkoon kirjautum inen va atii tunnistuksen. Käyttäjätunnukseen liittyy oikeuksia nähdä ja suorittaa er ilaisia tehtäviä. Verkkojärjestelm ään on rakennettu oikeuksien jakojärjestelm ä, joka sallii ta rvittavien toimintojen suorittam isen. Sovelluksilla on om a kirjautum iskäytäntönsä. Henkilökunnalla on yleensä oma kotikansio palvelimella.

Opiskelijoilla on käytössä ryhm äkirjautumistunnukset eri opintosuunnitelmien mukaan. Nämä tunnukset antava t oikeuden suorittaa perustoim intoja työ asemilla ja nähdä perusas iat verkkoas emilla. Opiskelijakohtais ia kotikansiota ei yleensä ole.

## 8.2 Käyttöoikeuksien hallinta

Tavoite Käyttöoikeuksien hallinta sisältää käyttäjien hallintaan koskevat määritykset:

- millä menetelmillä tietojärjestelmien käyttäjät rekisteröidään
- millaista rekisteriä käyttäjistä pidetään
- millaisia ominaisuuksia kustakin käyttäjästä kirjataan esimerkiksi käyttäjälle myönnettävän varmenteen attribuuteiksi

- kuinka hallinnoidaan sitä, että kukin käyttäjä saa nimenomaan hänelle kuuluvat käyttövaltuudet tietoihin.

Lisäksi luonnollisesti käyttäjien ja käyttövaltuuksien poistaminen on osa käyttäjien hallinnointia.

Hyväksytyt menettelytavat ja ratkaisut erilaisten käyttäjien todennusmenetelmien käytölle määritellään, tarvittaessa kunkin turvatason tiedoille erikseen. Tiettyihin järjes telmiin voidaan esim erkiksi hyväksyä käyttäjätunnusten salasanam enettelyn käyttö, kun ta as pää sy tiettyihin jä rjestelmiin voidaan valtuuttaa vain käyttäjien va hvalla tunnistam isen käytöllä. Määrättyjen ja tie toturvallisesti v aarallisten m enetelmien käyttökiellot es imerkkinä jaettujen osastokohtaisten kä yttäjätunnusten ja salasanojen on syytä mainita.

### 8.2.1 Käyttäjien rekisteröinti

Turvamekanismi

Käyttöoikeuksien rekis teröintiin ja rekisteröinnin poistoon tulee ka ikissa usean käyttäjän tietojärjestelmissä ja palveluissa olla menettelyohjeet.

Keskuspuiston tilanne

Uuden työntekijän palkkauksen yhteyde ssä käydään läpi perehdytysjakso. Jaksoon sisältyy tietotekniikkaosio, jo ssa käydään läpi koulun tietoverkon rakenne siellä olevat ty ökalut kuten: oppilasrekiste ri, poissaolorekisteri, intranet, koulun Internet-sivut, Moodle , Pedanet. Lisäksi tulija perehdytetään tietokoneen ja tietoverkon turvalliseen käyttöön.

### 8.2.2 Pääkäyttäjän oikeuksien hallinta

Turvamekanismi

Etuoikeuksien jakamista ja käyttöä tulee rajoittaa ja valvoa.

Keskuspuiston tilanne

Etuoikeuksia jaetaan hyvin rajoitetusti luotettaville koulutuksen saanneille henkilöille, jotta he pystyisivät suorittamaan työtehtävänsä.

### 8.2.3 Käyttäjän salasanojen hallinta

Turvamekanismi

Salasanan myöntämistä tulee valvoa määritellyllä hallintaprosessilla.

Keskuspuiston tilanne

Palkkauksen yhteydessä rehtori tai toimialajohtaja tilaa järjestelmähuollolta käyttäjätunnukset ja käyttäjäoikeudet. Tilaus suoritetaan sähköpostilla tai kiireellisessä tapauksessa puhelim ella. Työsuhteen päättyessä m enetellään samalla tavalla.

### 8.2.4 Käyttöoikeuksien uudelleenarviointi

Turvamekanismi

Johdon tulee sovitun menettelyn mukaisesti säännöllisin väliajoin tarkistaa uudelleen käyttäjien käyttöoikeudet.

Keskuspuiston tilanne

Johto on delegoinut nämä tehtävät järjestelmätuelle ja kriittisten ohjelmien hallinnoijille. He havainnoivat käytännön tilanteita ja auditoivat lokeja ja vetävät niistä johtopäätöksensä. Ensisijaisesti tarjotaan opastusta ja koulutusta, toissijaisesti rajoitetaan käyttöoikeuksia.

## 8.3 Käyttäjän velvollisuudet

Turvamekanismi

Estää tietojen luvaton käyttö sekä tiedon ja tiedonkäsittelypalvelujen vaarantuminen tai varkaus.

Keskuspuiston tilanne

Koululla on käytössä sellaisia ryhmäsalasanoja, joilla voi kirjautua tietokoneelle ja joilla on rajoitettu pääsy tietoverkkoon. Opiskelijat käyttävät näitä tunnuksia yleisessä käytössä olevilla tietokoneilla opetusluokissa. Opiskelijat, joilla on henkilökohtainen työasema käytössään, käyttävät henkilökohtaista käyttäjätunnustaan. Heillä on järjestelmänvalvojan oikeudet työasemassaan, mutta oikeudet verkossa ovat rajoitetut.

Henkilökunnalla on omat tunnuksensa ja kaikille on jaettu oikeuksia tarpeen ja tehtäväkuvauksen mukaan. Lähtökohtana on kuitenkin ollut, ettei oikeuksia ole liian paljon.

Henkilökunnan velvollisuuksiin kuuluu estää asiaton oleskelu kiinteistössä varmistamalla, että kaikki ikkunat, työhuoneisiin johtavat ovet, osastojen ovet sekä ulko-ovet ovat lukitut. Viimeisenä osastolta poistuvan työntekijän tulee lukita osastoa rajoittavat ovet (HEPO, 2002).

### 8.3.1 Salasanan käyttö

Turvamekanismi

Käyttäjiltä tulee vaatia hyvän turvallisuuskäytännön noudattamista salasanan valinnassa ja käytössä.

Keskuspuiston tilanne

Ryhmäkäyttäjätilit toimivat ilman salasanaa, koska monilla käyttäjillä on vaikeuksia muistaa niitä. Tämän takia näiden käyttäjien oikeudet ovat hyvin pienet. Tietokoneetkin palautuvat alukeperäisiin asetuksiinsa käynnistyksen yhteydessä. Kaikkien käyttäjien, jotka aikovat tehdä pysyviä muutoksia tietokoneelle tai haluavat pääsyn tiettyyn verkkoasemaan tai ohjelmaan, täytyy kirjautua omilla tunnuksillaan. Salasanan lainaaminen ei ole sallittua.

### 8.3.2 Valvomattomat käyttäjien laitteet

Turvamekanismi

Käyttäjän tulee varmistaa, että valvontaa vaille jäävillä laitteilla on turvasuojaus.

Keskuspuiston tilanne

Luottamukselliset asiakirjat saa tulostaa ainoastaan suojatuille kirjoittimille ja ne on poistettava tulostimista heti tulostamisen jälkeen. Yleiset kirjoittimet on tarkoitettu ainoastaan julkisille asiakirjoille. Siirrettävät tallennusvälineet on aina irrotettava laitteista ja siirrettävä suojattuun tallennuspaikkaan. Yleiset kopiokoneet vaativat ryhmäkäyttäjätunnistuksen.

### 8.3.3 Puhtaan pöydän ja puhtaan näytön politiikka

Turvamekanismi

Papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän politiikka sekä tietojenkäsittelypalveluja koskeva puhtaan näytön politiikka tulee ottaa käyttöön.

Keskuspuiston tilanne

Mikään luottamuksellinen asiakirja ei saa olla näkyvillä työpöydällä, tulostimessa tai näyttöruudulla. Tarpeettomiksi käyneet asiapaperit tuhotaan silppurilla ja päälle jäaneet vartioimattomat näytöt suljetaan nopeasti automatiikan avulla. Uudelleen avaaminen tulee olla mahdollista ainoastaan salasanan avulla.

## 8.4 Verkkoon pääsyn valvonta

Turvamekanismi

Pääsynhallintamenetelmät on määriteltävä tarkoin etukäteen. Niiden vahvuuden ja turvallisuuden on vastattava tietojärjestelmien ja tietojen turvatasoa. Tarvittaessa jokaiseen tietojärjestelmään on laadittava erillinen politiikka, jossa määritellään käyttäjien tunnistamisen menetelmät, millaisia tunnisteita käytetään, millaisia yhteyksiä tietojärjestelmiin on käytössä ja miten tietojärjestelmien käyttöä tarkkaillaan. Kaikista politiikkojen ja ohjeiden mainitsemista menetelmistä ja teknisistä yksityiskohdista ilmenee tarkkaan, onko kyseessä pakollinen ominaisuus, suositus tai hyväksyttävä (mutta ei suositeltava) vaihtoehto. Pääsynhallinta perustuu ja noudattaa organisaation tietoturvapolitiikkaa.

Keskuspuiston tilanne

Koulun lähiverkkoon ei pääse ilman tunnuksia. Tunnukset on jaettu ryhmiin. Yleistunnus antaa oikeuden käyttää tietokonetta, mutta ei hallinnoida sitä. Verkkoresurssit on mitoitettu vaatimattomiksi. Eri osastoilla on omat samantyyppiset tunnuksensa. Huoltaja voi huoltaa työasemia ja hänellä on hieman suuremmat näkymät ja oikeudet verkkoon. Henkilökunnan tunnukset kuuluvat omiin ryhmiinsä. Järjestelmäasiantuntijoilla on suurem-

mat oikeudet hallinnoida verkon laitte ita. Pääkäyttäjällä on suurimm at oikeudet.

### 8.4.1 Verkkopalvelujen käytön periaatteet

Turvamekanismi

Käyttäjille tulee sallia pääsy ainoastaan niihin palveluihin, joihin heille on erityisesti myönnetty pääsyoikeudet.

Keskuspuiston tilanne

Verkkokäyttöjärjestelmä on käytössä. Ka ikki järjestelm ään kirjautuneet muodostavat objektin, jolla on tietyt oi keudet tehdä asioita. P erusoikeudet on asetettu niin alas, ettei vahingonteko ole helppoa. Näkymä verkkoon on suppea ja koostuu lukuoikeuksista. Valta osalla käyttäjistä o n perusoikeudet. Henkilökunnalla on palvelim ella om a kotihakem isto, joka varm uuskopioidaan.

Palvelut verkossa:

- tulostus
- opiskelijarekisteri
- poissaolorekisteri
- taloushallinnon ohjelmat
- sähköposti
- Intranet
- verkkoasemat
- Moodle
- Pedanet

Jokaisella autentikoituneella käyttäjällä on omat oikeutensa. Oikeudet jaetaan käyttäjäryhmittäin.

### 8.4.2 Ulkopuolisia yhteyksiä käyttävien henkilöiden todentaminen

Turvamekanismi

Etäkäyttäjien pääsynvalvonnassa tul ee käyttää järjestelm änvalvonnan kannalta tarkoituksenmukaisia todennusmenetelmiä.

Keskuspuiston tilanne

Etäkäyttäjät pääsevät rajoitetusti suppeille ei kr iittisille alueille organisaation verkkoon. Etäkäyttäjien on autent ikoiduttava suojatusti. Etäkäyttötoimintoja ovat sähköposti, oppilaide n poissaolojärjestelmä ja henkilökunnan kotikansiotoiminta. Toiminnat on suoja ttu palomuurilla ja ohjelmistoautentikoinnilla.

### 8.4.3 Laitteiden tunnistus verkoissa

Turvamekanismi

Automaattista käytettäv än laitteisto n tunnistusta verkossa, tulee harkita keinona todentaa yhteyslupia määritellyistä paikoista tai laitteista.

Keskuspuiston tilanne

Langallinen verkkokäyttöjärjestelmä vaatii käyttäjän kirjautumisen, laitetta ei tunnisteta. Opiskelijoiden ryhmätunnukset antavat rajoitetun näkymän verkkoon. Henkilökohtaiset kirjautumistunnukset ja salasanat päästävät työn suorittamisen kannalta tarpeellisille alueille tarpeellisin oikeuksin. Harkinnan alla on WLAN- verkon kautta verkkoon kytkeytyvien laitteiden tunnistus. WLAN- vierasverkkoa ei ole käytössä. Tulossa oleva IDS- laitteisto tulee tunnistamaan epäilyttävästi käyttäytyvät laitteet ja eristämään ne verkosta.

### 8.4.4 Etähuoltoyhteyksien suojaus

Turvamekanismi

Fyysistä ja loogista pääsyä etähuoltoyhteyksien käyttämiin portteihin tulee valvoa.

Keskuspuiston tilanne

Etähuoltoyhteyksiä on hyvin vähän käytössä. Olemassa olevat yhteydet ovat suojatut ja salatut sekä kirjautuminen salasanasuojattua. Yhteyksien käyttöä seurataan, jotta varmistetaan, ettei luvatonta yhteyttä saada rakennetuksi.

### 8.4.5 Verkkoyhteyksien looginen jaottelu

Turvamekanismi

Tietojenkäsittelypalvelujen, käyttäjien ja tietojärjestelmien ryhmät tulee eristää toisistaan verkossa.

Keskuspuiston tilanne

Verkkoyhteyksiä käyttävät esim. sähköpostin käyttäjät, poissaolotietojen selaajat, kalenterin synkronoijat ja kotikansion selaajat. He pääsevät katsomaan omia rajoitettuja alueitaan, jotka eivät ole kiinni toisissaan.

### 8.4.6 Verkkoyhteyksien valvonta

Turvamekanismi

Jaetuissa verkoissa, erityisesti organisaation rajojen ulkopuolelle ulottuvissa, käyttäjien mahdollisuutta verkkoyhteyteen tulee rajoittaa pääsynvalvontaperiaatteiden ja liiketoimintasovellusten vaatimusten mukaisesti.

Keskuspuiston tilanne

Kaikki liikenne organisaation ja Internetin välillä on rajoitettu palomuurilla ja pääsynvalvonnalla. Pääsy on tiettyihin sovelluksiin kuten sähköpostiin, poissaolon seurantaan ja omaan kotikansioon. Varsinaista etäkäyttöä ei ole. Etätoimipisteistä on reititetty yritysverkkoyhteys pääkoululle.

## 8.5 Käyttöjärjestelmään pääsyn valvonta

Tavoite Tavoitteena on estää luvaton pääsy käyttöjärjestelmiin.

### 8.5.1 Turvalliset sisään kirjautumismenettelyt

Turvamekanismi

Pääsyä käyttöjärjestelmään tulee valvoa turvallisen sisään kirjautumismenettelyn avulla.

Keskuspuiston tilanne

Kirjautuminen tietokoneille ja verkkoon on mahdollista vain organisaation oman verkkojärjestelmän kautta, jossa autentikointi tapahtuu. Opetuskäytössä on muutama poikkeus: tietoteknikkaa opiskelevat autentikoituvat palomuurilla eristetyssä verkossaan työasemalleen tai toimialueellensa omilla ehdoillaan, mutta eivät näe koulun verkkojärjestelmää.
Kirjautumiset kirjataan lokiin ja niitä seurataan. Järjestelmästä lähtee hälytys järjestelmänvalvontaan kun tietoturvapolitiikkaa rikotaan.

### 8.5.2 Käyttäjän tunnistaminen ja todentaminen

Turvamekanismi

Jokaisella käyttäjällä tulee olla yksilöllinen tunniste (käyttäjätunnus) vain käyttäjän henkilökohtaiseen käyttöön. Lisäksi tulee valita soveltuva todennuskeino, jolla varmennetaan käyttäjän väitetty henkilöllisyys.

Keskuspuiston tilanne

Henkilökunnalla on kaikilla yksilöllinen käyttäjätunnus ja henkilökohtainen salasana verkkokirjautumista varten. Suojatuilla sovelluksilla on omat käyttäjätunnus/salasana parinsa. Opettajat käyttävät ryhmätunnusta työasemalle kirjautuessaan ja näkevät suuppean ei kriittisen osan verkkoa rajoitetuin oikeuksin.

### 8.5.3 Salasanojen hallintajärjestelmä

Turvamekanismi

Salasanojen hallintajärjestelmän tulee olla vuorovaikutteinen ja varmistaa salasanojen laatu.

Keskuspuiston tilanne

Salasanojen hallintajärjestelmä verkkokäyttöjärjestelmään on vuorovaikutteinen ja salasanojen laatu on varmistettu järjestelmätuen ohjeiden mukaan. Suojattujen sovellutusten käynnistys mahdollistuu verkkoautentikoitumisen kautta omasta lähiverkosta.

### 8.5.4 Järjestelmän apuohjelmien käyttö

Turvamekanismi

Sellaisten apuohjelmien, jotka saattavat pystyä ohittamaan järjestelmän ja sovelluksen turvamekanismit, käyttöä tulee rajoittaa ja valvoa tarkasti.

Keskuspuiston tilanne

Apuohjelmia, jotka pystyvät ohittamaan turvamekanismit ei ole asennettu.

### 8.5.5 Istunnon aikakatkaisu

Turvamekanismi

Käyttämättömien istuntojen tulee sulkeutua, kun ne ovat olleet käyttämättä määritellyn ajan.

Keskuspuiston tilanne

Istuntojen aikakatkaisut ovat sovelluskohtaisia. Monet sovellukset katkaistaan tietyn ajan kuluttua. Aivan tarkkaa kuvaa jokaisen sovelluksen ominaisuuksista ei ole olemassa. Työasemissa on näytönsäästäjän aikakatkaisu, joka vaatii uudelleenkirjauksen.

### 8.5.6 Yhteysajan rajoittaminen

Turvamekanismi

Yhteysajan rajoittamista tulee käyttää lisäturvana suuren riskin sovelluksissa.

Keskuspuiston tilanne

Sovelluksissa käytetään sovelluskohtaisia aikakatkaisuja. Lisäksi työasemat sulkeutuvat oltuaan asetetun ajan käyttämättöminä.

## 8.6 Sovellukseen ja tietoon pääsyn valvonta

Tavoite Tavoitteena on estää luvaton pääsy sovelluksissa säilytettäviin tietoihin.

### 8.6.1 Tietojen käytön rajoittaminen

Turvamekanismi

Sovellusten käyttäjien ja sovellusten tukihenkilöide pääsy tietoihin tai sovellusten toimintoihin tulee rajoittaa määriteltyjen pääsynvalvontaperiaatteiden mukaan.

Keskuspuiston tilanne

Luottamuksellista tietoa sisältävät sovellukset vaativat kirjautumisen. Kirjautumisen yhteydessä tapahtuva autentikoituminen antaa oikeudet toimia sovelluksessa. Oikeudet määräytyvät ennalta laaditun suunnitelman mukaan. Oikeuksia myönnetään rajoitetusti, mutta riittävästi toiminnan turvaamiseksi.

### 8.6.2 Arkaluontoisen sovelluksen eristäminen

Turvamekanismi

Arkaluonteisille sovelluksille tulee järjestää eristetty tietokoneympäristö.

Keskuspuiston tilanne

Keskuspuistossa ei ole käytössä arkaluontoisia sovelluksia.

### 8.6.3 Tietokoneen matkakäyttö

Turvamekanismi

Tulee ottaa käyttöön määritellyt toimintaperiaatteet ja turvamekanismit. joilla suojaudutaan tietokoneen matkakäytön ja etäyhteyksien aiheuttamasta riskeiltä.

Keskuspuiston tilanne

Tietokoneen liittäminen etäkäyttötoiminnon kautta organisaation tietojärjestelmään järjestelmään ei ole mahdollista. Jokainen käyttäjä, joka on vastaanottanut tietokoneen matkakäyttöön, on sitoutunut huolehtimaan koneestaan ja sen sisältämästä tiedosta. Luottamuksellista tietoa ei pitäisi säilyttää koneella. Koneen rikkoutuminen ja tiedon tuhoutuminen onkin ollut suurempi ongelma kuin tiedon joutuminen vääriin käsiin.

### 8.6.4 Etätyö

Turvamekanismi

Etätyötoimintaa varten tulee kehittää ja ottaa käyttöön periaatteet, toimintasuunnitelmat ja menettelytavat.

Keskuspuiston tilanne

Etäkäyttö järjestelmän puolelle huoltotoimintaa varten on vain yksi suojattu yhteys oman reititetyn yritysverkon kautta. Yhteys on suojattu käyttäjätunnuksin ja salasanoin. Tulkinnanvaraista on pidetäänkö sähköpostia, opiskelijoiden poissaolojärjestelmää ja henkilökunnan kotikansioiden saavutettavuutta etätyönä. Tietty suojausriski tällä kohtaa on ja asiaa kannattaisi pohtia tarkemmin.

# 9 TIETOJÄRJESTELMIEN HANKINTA, KEHITYS JA YLLÄPITO

Organisaation tietoturvallisuustason ylläpitämiseksi ei riitä, että organisaation toim innassa, tietojen käsittelyssä ja tiedonvälityksessä noudatetaan turvallisia tapoja ja m enetelmiä. Myös käytettä vien tie tojärjestelmien ja sovellusten turvallisuu desta on h uolehdittava. Tietojärjestelm ät täytyy suunnitella ja toteuttaa siten, että turva-aukkoja ei ole sovellusten ja järjestelmien sisällä. Käytettävien tietojen oikeellisuus täytyy taata koko käsittelyprosessin ajan: oikeellisuus täytyy taata aina järjestelmään käsiteltäväksi tai käytettäväksi vastaanotettavista tie doista (syö tetietojen tarkastus,) järjestelmän tuottam iin tietoihin (tu lostustietojen tarkastus) a sti kaik issa käsittelyn vaiheissa. Tieto voi olla m itä tahansa esimerkiksi tietojärjestelmän sisäisesti to iselta proses silta vastaano tettavaa tie toa, toise sta tietojärjestelmästä vastaanotettavaa tietoa, tiedostosta luettavaa tietoa tai käyttäjän järjestelmään syöttämää tietoa. Erityisesti sähköpostitse vastaanotettavan tiedon alkuperästä tulee varmistua.

Tietojärjestelmät on suunniteltava si ten, e ttä lak ien va atimukset (es imerkiksi henkilö- ja potilas tietojen kä sittelyssä ja s uojaamisessa) autom aattisesti to teutuvat niissä ja että m ahdolliset lakim uutokset void aan r iittävän helposti ottaa huom ioon esim erkiksi järjestelmien määrityksiä ja konfiguraatioita m uuttamalla. L akien nouda ttaminen ja noudattam atta jättäm inen ei saa olla käyttä jän to imista kiinni, vaan tie tojärjestelmän on aina m ahdollisuuksien mukaan ohjattava tai pakotettava käyttä jä oikeanlaiseen toimintaan. Edellä mainittu koskee myös kaikkia kansallisia ja kansainvälisiä standardeja.

## 9.1 Tietojärjestelmien turvallisuusvaatimukset

Tavoite Tavoite on varmistaa, että tietojärjestelmät kehitetään turvallisiksi.

### 9.1.1 Turvallisuusvaatimusten analyysi ja määrittely

Turvamekanismi

Uuden tai olem assa olevan tieto järjestelmän kehittämistä koskevien liik etoimintavaatimusten tulee määrittää turvamekanismien vaatimukset.

Keskuspuiston tilanne

Tietojärjestelmiä kehitetään varovasti ja h arkiten välttäen k aikkia turh ia riskejä, jotka voisivat vaarantaa tietojärjestel mien toim ivuuden. Pääsääntöisesti laitteistoksi ja järjestelmiksi hyväksytään ainoastaan koeteltuja ja toimivuutensa käytännössä osoittaneita kom ponentteja, joista yhteistyökumppaneilla on hyvät kokem ukset. Sovellustasolla Keskuspuisto on m ukana muutamassa kehitysprojektissa, jotta sa isi itsellensä soveliaan sovelluksen. Näissä projekteissa sovelluksissa havaitut puutteet on saatu korjattua nopeasti. Kehitysprojekteissa ei ole enää ollut kyse uuden sovellukse n luomisesta vaan toim ivan käytössä olevan sovelluksen m uokkaamisesta erityisopetusympäristöön.

## 9.2 Virheetön tietojenkäsittely sovelluksissa

Tavoite Tavoitteena on estää virheitä, tiedon katoamista, sen luvatonta muuttamista ja väärinkäytön mahdollisuus.

### 9.2.1 Syöttötietojen oikeellisuuden tarkistus

Turvamekanismi

Sovellukseen syötettävä tieto tulee va hvistaa päteväksi, jotta varmistettaisiin sen oikeellisuus ja asianmukaisuus.

Keskuspuiston tilanne

Kriittisiin sovell uksiin on kirjauduttava sisään interaktiivisesti. Kirjautuminen tuo mukanaan kirjautuneelle tiet yt oikeudet nähdä ja suorittaa erilaisia toim intoja. Oikeuksien jaossa noudatetaan pidättyväisyyttä. Käyttäjän on osoitettava hallitsevansa sovelluksen käytön saadakseen lisää oikeuksia. Oikeuksien tarpeellisuuden harkitsee sovelluksen haltija.

Kenttiin syötettävän datan arvoja on ra joitettu, jotta väärän tiedon syötöltä vältyttäisiin. Rajoitusten ulkopuolisten arvojen syö ttö on estetty. Tallennustapahtumista syntyy kirjaam ishistoria. Sovelluksen haltia voi selata tapahtumia ja korjata sattuneet virhek irjaukset. Väärän tiedon syöttäm isen torjuminen on jatkuvan kehityksen kohteena.

### 9.2.2 Sisäisen käsittelyn valvonta

Turvamekanismi

Jotta käs iteltävän tiedo n vääristym iset tah attomien tai tahallisten oh jelmointivirheiden seu rauksena hav aitaan, tu lee so velluksiin sisälly ttää tiedon oikeellisuustarkistuksia.

Keskuspuiston tilanne

Suoritetut transaktiot ovat lukum äärältään vähäisiä ja kaikki oppilaiden merkinnät tarkastetaan manuaalisesti usein. Taloushallinnon sovelluksissa on omat tarkastuksensa.

### 9.2.3 Viestien eheys

Turvamekanismi

Viestien aitouden varm istamista ja eheyden suojaam ista sovelluksissa koskevat vaatim ukset tulee yk silöidä ja as ianmukaiset tu rvamekanismit tunnistaa ja toteuttaa.

Keskuspuiston tilanne

Taloushallinnolla on om at sovelluksen sisään rakennetut tarkistuksensa. Oppilasrekisterin tiedot käydään m anuaalisesti läpi vähint ään kaksi kertaa vuodessa HOJKS keskusteluissa ja tu lostetaan lukukausien päättyessä. Virheellisyydet paljastu vat silloin. Opintokokonaisuudet arvioidaan kun osasuoritukset on tehty, tästäkin synt yy tarkistuspiste. Poissaolom erkinnät

käydään läpi kuukausittain, jolloin vi rhemerkinnöistä käydään keskustelu. Varsinaisia kriittisiä toimintoja massatuotantona ei esiinny.

### 9.2.4 Tulostustietojen oikeellisuuden tarkistus

Turvamekanismi

Sovelluksista tulostetun tiedon oikeellisuus tulee tarkistaa kussakin tilanteessa tallennetun tiedon käsittelyn virheettömyyden ja asianmukaisuuden varmistamiseksi.

Keskuspuiston tilanne

Tulostukset ovat vähäisiä. Tulostuksen yhteydessä suoritetaan manuaalinen tarkistus.

## 9.3 Salakirjoitusmekanismit

Tavoite Tavoitteena on suojata tiedon luottamuksellisuus, alkuperäisyys tai eheys salakirjoitusmekanismeilla.

### 9.3.1 Salakirjoitusmekanismien käytön periaatteet

Turvamekanismi

Tulee kehittää ja ottaa käyttöön ne periaatteet, joita sovelletaan salakirjoitusmekanismien käyttöön tietojen suojaamisessa.

Keskuspuiston tilanne

Etäpisteiden välillä on reititetty yritysverkko. Julkisen Internet verkon kautta ei lähetetä luottamuksellisia viestejä tai tapahtumia. SSL on käytössä kirjautumisessa verkkopalveluihin.

### 9.3.2 Salakirjoitusavainten hallinta

Turvamekanismi

Salausavainten hallintamenettelyjen tulee olla käytössä silloin, kun organisaatio käyttää salakirjoitustekniikoita.

Keskuspuiston tilanne

Opistolla on oma CA ja avainhallinta on järjestelmätuen takana.

## 9.4 Järjestelmätiedostojen turvallisuus

Tavoite Tavoitteena on varmistaa järjestelmätietojen turvallisuus.

### 9.4.1 Tuotannossa olevan ohjelmiston valvonta

Turvamekanismi

Menettelytapojen, joilla valvotaan ohjelmien asentamista tuotannossa oleviin järjestelmiin, tulee olla käytössä

Keskuspuiston tilanne

Tuotannossa olevat järjestelmien, sovelluksien ja ohjelmien päivityksen suorittaa ja valvoo asiantunteva järjestelmänvalvoja asianmukaisilla auktorisointi-oikeuksilla. Järjestelmissä käytetään ainoastaan hyväksyttyä asennuskoodia.

### 9.4.2 Järjestelmän testiaineistojen suojaus

Turvamekanismi

Testiaineistot tulee valita huolellisesti ja niitä tulee suojata ja valvoa.

Keskuspuiston tilanne

Testiajot ajetaan virtuaaliympäristössä. Yleensä testiajot ovat mittasuhteiltaan rajoitetut ja materiaali hävitetään kun testiajot on suoritettu.

### 9.4.3 Ohjelmien lähdekoodin pääsyn valvonta

Turvamekanismi

Pääsyä ohjelmien lähdekoodiin tulee rajoittaa.

Keskuspuiston tilanne

Ohjelmien lähdekoodit ovat yleensä suljettuja koodeja ja sijaitsevat paikoissa, joihin ei ole vapaata pääsyä. Ainoastaan tiettyjen sovellusten, joita käytetään työasemilla, asennustiedostot ovat näkyvillä, mutta ei muokattavissa.

## 9.5 Kehitys- ja tukiprosessien turvallisuus

Tavoite Tavoitteena on ylläpitää sovellusjärjestelmien ohjelmien ja tietojen turvallisuutta.

### 9.5.1 Muutosten valvontamenettely

Turvamekanismi

Muutosten toimenpanoa tulee valvoa sovitulla muutosten valvontamenettelyllä.

Keskuspuiston tilanne

Työkaluja muutosten valvonnalle ei tällä hetkellä ole olemassa. Muutoksia kriittisissä ohjelmissa tarkkaillaan tunkeutumisseurannan ja järjestelmälokien kautta.

### 9.5.2 Käyttöjärjestelmän muutosten jälkeinen sovellusten tekninen tarkastus

Turvamekanismi

Käyttöjärjestelmän muutosten yhteydessä liiketoiminnan kannalta kriittiset sovellukset tulee tarkistaa ja testata, jotta varmistetaan, ettei organisaation toiminnalle tai turvallisuudelle aiheudu haitallisia vaikutuksia.

Keskuspuiston tilanne

Verkkokäyttöjärjestelmän päivitykset suunnitellaan huolella ja ainoastaan koetellut ja toimintavarmuutensa osoittaneet päivitykset suoritetaan. Päivitystoiminnon jälkeen varmistetaan päivityksen toimivuus. Työasemat hankitaan vuosisopimuksella mukaan ja varustetaan vakioidusti laitteistojen ja ohjelmistojen suhteen. Koneet testataan ennen käyttöönottoa.

### 9.5.3 Ohjelmistopakettien muutoksia koskevat rajoitukset

Turvamekanismi

Ohjelmistopaketteihin tehtäviä muutoksia tulee välttää, ne tulee rajoittaa tarpeellisiin muutoksiin ja kaikkia muutoksia valvoa tarkasti.

Keskuspuiston tilanne

Verkkojärjestelmän muutokset tehdään kohdan 7.5.2 mukaan hallitusti. Sovelluspaketit valitaan järjestelmään sopivuuden, käytettävyyden ja pedagogisten ominaisuuksiensa mukaan harkiten.

### 9.5.4 Tietovuodot

Turvamekanismi

Tietovuodon mahdollisuudet tulee ehkäistä.

Keskuspuiston tilanne

Järjestelmätuki tarkkailee säännöllisesti ulos menevän ja sisään tulevan liikenteen määriä, havaitakseen tavanmukaisesta poikkeavia määriä. Se tarkkailee myös resurssien hyödyntämistä pullonkaulojen muodostumisen ja ei toivotun liikenteen syntymisen ehkäisynä. IDS/IPS on tulossa tukemaan toimintaa. Maaliskuussa 2009 se on käytössä.

### 9.5.5 Ulkoistettu ohjelmistokehitys

Turvamekanismi

Organisaation tulee valvoa ja tarkkailla ulkoistettua ohjelmistokehitystä.

Keskuspuiston tilanne

Organisaatiolla ei ole ulkoistettua ohjelmistokehitystä.

# 10 TIETOTURVAHÄIRIÖIDEN HALLINTA

Tietoturvaloukkausten ja normaalista poikkeavien tilanteiden valvonta ja seuranta, havaitseminen ja raportointi sekä oikeisiin toimenpiteisiin ryhtyminen ongelmien korjaamiseksi ja mahdollisten seuraamusten määrittämiseksi ovat oleellinen osa tietoturvallisuuden ylläpidon prosessia.

Valvonnalla, seurannalla ja erilaisella tarkkailulla on tarkoitus havaita kaikki poikkeamat ja sellainen valtuudeton toiminta organisaatiossa, joka voi vaarantaa tietojenkäsittelyn ja tietojen turvallisuuden. Seuranta sisältää menetelmät aina kiinteistön ja tilojen valvonnasta (esim erkiksi kulunvalvonta, tunnistimet ja hälyttimet, kameravalvonta) tietojärjestelmien tilan ja niitä käyttävien henkilöiden ja tapahtumien seurantaan ja kirjaamiseen. Tapahtumaseurannassa kirjataan sekä henkilöiden toimenpiteet että järjestelmässä automaattisesti tapahtuvat toiminnat mukaan lukien erilaiset vika- ja häiriötilanteet.

Valvonnasta saatujen tapahtumatietojen, lokitiedostojen, nauhojen ja vastaavien säilytysaika ja säilytystapa on määriteltävä. Joidenkin seurantatietojen osalta säilytysaika voi olla pitkä, kuten lokitiedot luottamuksellisten tietojen käsittelystä. Mahdollisesti todistusaineistona tarvittavien tietojen säilytys takaa sekä organisaation, yksittäisen henkilön että organisaation sidosryhmän oikeusturvan säilymisen.

Poikkeamista ja havaituista loukkauksista raportoidaan välittömästi ja tehdään riittävät hälytykset joko automaattisesti tai havaitsevan henkilön toimesta. Hälytys käsitellään sekä tietoturvaorganisaatiossa korjaaviin toimenpiteisiin ryhtymiseksi mahdollisimman pikaisesti että jo hdossa, mahdollisten seuraamusten voidaan määrittelemiseksi. Henkilöstöllä ja kolmansilla osapuolilla on oltava tieto, miten ja kenelle havaituista potentiaalisista tietoturvallisuuteen vaikuttavista tietojärjestelmien haavoittuvuuksista, ongelmista tai epäilyttävistä tilanteista pitää raportoida.

## 10.1 Tietoturvatapahtumista ja -heikkouksista raportointi

Tavoite

Tavoite on varmistaa, että tietoturvatapahtumista ja tietojärjestelmiin liittyvistä heikkouksista viestitetään siten, että korjaaviin toimenpiteisiin voidaan ryhtyä ajoissa.

### 10.1.1 Tietoturvatapahtumien raportointi

Turvamekanismi

Tietoturvatapahtumista tulee raportoida mahdollisimman nopeasti ja asiankuuluvaa hallintakanavaa käyttäen.

Keskuspuiston tilanne

Tietoturvatapahtumista tulee raportoida järjestelmätukea. Raportin voi vastaanottaa jokainen järjestelmätuen työntekijä. Vastaanottaja ohjaa toi-

menpiteen sille jäsenelle, jonka oikeude t ja taidot riittä vät korjaavan toimenpiteen toteuttamiseksi.

### 10.1.2 Tietoturvallisuuden heikkouksista raportointi

Turvamekanismi

Kaikkien ty öntekijöiden, toim ittajien ja tieto järjestelmien tai -palve lujen käyttäjien e dellytetään kiinnittäv än huom iota ja raporto ivan kaikista järjestelmissä tai palve luissa havaituista tai epäilyttävistä suojauksen heikkouksista.

Keskuspuiston tilanne

Raportointi vajaatoim innoista verkossa ja sovelluksista on nopeata ja tehokasta. Kyky erottaa toim imattomuus tietoturvariskistä ei aina ole itsestään selvää, mutta toimimattomuusilmoitusten joukossa olevat epäilyttävät tapahtumat tutkitaan myös.

## 10.2 Tietoturvahäiriöiden ja parannuskohtien hallinta

Tavoite Tavoite on varmistaa, että tietoturvahäiriöiden hallinnan toimintamalli on johdonmukainen ja tehokas.

### 10.2.1 Vastuut ja menettelytavat

Turvamekanismi

Hallintavastuut tu lee m ääritellä ja l uoda m enettelytavat, joilla taataan pikainen, tehokas ja järjestelmällinen reagointi tietoturvahäiriöihin.

Keskuspuiston tilanne

Järjestelmätuella on suu lliset m enettelytavat r eagoida tietoturvahäiriöihin. Pieniin häiriöihin voi puuttua paikalla oleva tukihenkilö, suuremmista häiriöistä rapor toidaan v älittömästi, no peimmalla m ahdollisella tilanteesee n sopivalla tavalla, vastaavien suurempien valtuuksien haltijalle.

### 10.2.2 Tietoturvahäiriöistä oppiminen

Turvamekanismi

Tietoturvahäiriöiden tyy pin, m äärän ja kus tannusten m ittaamista ja seu raamista varten tulee olla menettelytavat.

Keskuspuiston tilanne

Keskuspuistolla ei ole mittareita osoittamaan tapahtumien kustannusvaikutuksia. Tapahtum a arvioidaan ja jos se todetaan vaara lliseksi, siih en e tsitään sopiva suojautumiskeino.

### 10.2.3 Todisteiden kokoaminen

Turvamekanismi

Jos tietoturvahäiriön jälkeen johonkin henkilöön tai organisaatioon kohdistuviin seurantatoimenpiteisiin liittyy siviili- tai rikosoikeudellisia oikeustoimia, tulee kerätä, säilyttää ja esittää todistusaineistoa kyseisen lainkäyttöalueen (tai lainkäyttöalueiden) todistusaineistoa koskevien sääntöjen mukaisesti.

Keskuspuiston tilanne

Toistaiseksi oikeustoimia vaativia tapahtumia ei ole ilmaantunut.

# 11 OPETUSTOIMINNAN JATKUVUUDEN HALLINTA

Tällä hetkellä ei pidetä aivan kiiree llisenä asian a saada tämän kappaleen sisältämää asioita standardin edellyttäm ään kuntoon. Kappale kuvaa pikemminkin kehityssuuntaa tulevaisuudessa.

Opetustoiminnan kannalta tietoverkkojen ja tietokoneiden jatkuva toiminta ei ole välttäm ätöntä. Päivänkään k atkos ei aiheuta ylipääsem ättömiä ongelmia. Kriittis iä opetus aloja ovat n e, jotk a käyttävät kokop äiväisesti tietokonetta opiskeluvälineenään ja ovat r iippuvaisia lisen ssipalvelimista. Opettaminen ja oppiminen ovat mahdollisia ilman tietokonetta.

## 11.1 Opetustoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia

Tavoite

Tavoitteena on ehkäistä opetustoiminnan keskeytyminen ja suojata kriittisiä opetustoimintaprosesseja tietojärjestelmien merkittävien häiriöiden tai onnettomuuksien vaikutuksilta ja taata prosessien viiveetön jatkaminen.

### 11.1.1 Tietoturvallisuuden sisällyttäminen opetustoiminnan jatkuvuuden hallintaprosessiin

Turvamekanismi

Opetustoiminnan jatkuvuutta varten tulee koko organisaat iossa kehittää ja edelleen ylläpitää hallittua prosess ia, joka käsittelee organisaation opetustoiminnan jatkuvuuden edellyttämiä tietoturvavaatimuksia.

Keskuspuiston tilanne

Tietokone ja tietoverkot ovat opetuksen tukipalveluja. Esim erkiksi tietotekniikan opiskelijat ovat hyvinkin ri ippuvaisia tietokone ista, suunnitteluassistentit ovat riippuvais ia tietokoneesta ja verkos ta esimerkiksi, kun taas esimerkiksi catering alan opiskelijat eivät tarvitse tietokonetta kuin satunnaisesti. Jär jestelmätuki on prio risoinut korjaustoim intansa häiriötapauksissa niin, että ensisija isesti ylläpidetään verkon toimintaa kun taas yksittäiset työas emat ovat toissijais essa asem assa. Tavallisimmat es iintyneet häiriöt ovat olleet käyttäjien aikaansaamia työasemiensa vikatilanteita.

### 11.1.2 Opetustoiminnan jatkuvuus ja riskien arviointi

Turvamekanismi

Opetustoimintaprosessit m ahdollisesti k eskeyttävät tapah tumat ja niid en todennäköisyys, vaikutus ja seuraam ukset tietoturvallisuuden kannalta tulee yksilöidä

Keskuspuiston tilanne

Tulipalon, vesivahinkojen, suurten sähköka tkosten riskit voivat toteutua odottamatta. Kiinteis tössä sija itsee saira ala, jo ten riske ihin liittyvät to i-minnot on suojattu keskiverto kiinte istöä huolellisemm in. Pe lastuslaitok-selle on suo ra au tomaattinen hälytysyhteys. Se on todettu toim ivaksi. Or-ganisaation om asta m ielestä tämän he tken suu rimpana riskinä ja keskey t-tämisuhkana pidetään epäluotettavan ta i vihamielisen käyttäjän pääsyä or-ganisaation lähiverkkoon. Tä tä silmälläpitäen on ryhdytty toim enpiteisiin IDS/IPS järjestelm än hankkim iseksi ja asentam iseksi. Ha nkinta on jo käynnistynyt.

### 11.1.3 Tietoturvallisuutta sisältävien jatkuvuussuunnitelmien kehittäminen ja toteuttaminen

Turvamekanismi

Tätä varten tulee keh ittää ja ottaa käyttöön suunnitelmat, joilla opetusto i-minta saadaan ylläpidettyä ja palaut ettua sekä tiedon saatavuus varm istet-tua vaaditulla tasolla ja vaaditu issa aikarajoissa kriittisen op etustoiminnal-listen prosessien keskeytymisen tai toimintahäiriön jälkeen.

Keskuspuiston tilanne

Tällä hetkellä on käytössä m enetelmät, joilla verkko ja työasem at saadaan käytännössä käyttöön tavallisissa virhetilanteissa riittävän nopeasti. Kirjal-lisia suunnitelmia ei ole olemassa. Katastrofiluonteisten tilanteiden jälkeis-ten toipumis- ja jatkuvuussuunnitelm ien laatiminen olisi kuitenkin paikal-laan.

### 11.1.4 Opetustoiminnan jatkuvuussuunnistelun puitteet

Turvamekanismi

Suunnitelmat tulee pitää yhtenäisissä puitteissa niiden kaikkien tasojen yh-teensopivuuden, tietoturvavaatimusten käsittelyn johdonmukaisuuden sekä testaamisen ja ylläpidon tärkeysjärjestyksen yksilöimisen takaamiseksi.

Keskuspuiston tilanne

Opetustoiminnan jatkuvuussuunnitelm aa tietoturvan kannalta ei ole ole-massa. Jatkuvuussuunnitelm a on käytännössä toteutettu s iten, että opetus jatkuu häiriötilanteista huolimatta.

### 11.1.5 Opetustoiminnan jatkuvuussuunnitelman testaus, ylläpito ja uudelleenarviointi

Turvamekanismi

Opetustoiminnan jatkuvuussuunnitelm ia tulee testata ja päivittää säännöl-lisesti niiden toimivuuden ja tehokkuuden varmistamiseksi.

Keskuspuiston tilanne

Tietoturvan jatkuvuussuunnitelm aa ei ol e luotu eikä sitä sen vuoksi voi myöskään testata.

# 12 SOPEUTUMINEN VAATIMUKSIIN

Vaatimustenmukaisuuden tunnistaminen edellyttää tietoisuutta niistä laeista, jotka ohjaavat tieto järjestelmien käyttöä. Seuraavassa lista tärkeimmistä laeista:

516 / 2004: Sähköisen viestinnän tietosuojalaki
759 / 2004 Laki yksityisyyden suojasta työelämässä
477/2001 Laki henkilötietojen käsittelystä työ- tai virkasuhteessa
523 / 1999 Henkilötietolaki
725 / 1978 Laki yhteistoiminnasta yrityksissä
731 / 1999 Suom en perustuslaki – yks ityiselämän, kotirauhan ja kunnian turvaaminen

Lisäksi: Laki sähköisistä allekirjoituksista
Arkistolaki

## 12.1 Lakisääteisten vaatimusten noudattaminen

Tavoite Tavoite on kaikkien lakien sekä asetusten, säädösten, sopimusten ja velvoitteiden ja kaikkien turvallisuusvaatimusten noudattaminen.

### 12.1.1 Sovellusten lainsäädännön tunnistaminen

Turvamekanismi

Kaikki asiaankuuluviin asetuksiin, sää döksiin ja sopim uksiin perustuvat vaatimukset sekä organ isaation toim intamalli niiden täy ttämiseksi tulee määritellä selvästi ja dokumentoida sekä pitää ajan tasalla tietojärjestelmää varten.

Keskuspuiston tilanne

Organisaation strategiassa määritetään, että lakeja, asetuksia ja sopimuksia noudatetaan. Tietoturvaa va rten ei ole olem assa erillistä dokum entoitua toimintamallia vaatimusten täyttämistä varten.

### 12.1.2 Aineettomat oikeudet

Turvamekanismi

Lainsäädännöllisten, säädösten ja so pimusten vaatim usten noudattam inen varmistetaan käytettäessä m ateriaalia, johon saatta a liittyä aineettom ia oikeuksia tai tekijänoikeudella suojattuja ohjelmistotuotteita. Tätä varten on luotava asianmukaiset menettelytavat.

Keskuspuiston tilanne

Organisaatiotasolla on luotu menettelytavat, joilla varmistetaan oikeat menettelytavat. Organisaa tio käyttää ainoas taan ohjelm istotuotteita, joid en tekijänoikeuspuitteet on tunnettu asenne ttaessa vakioituja asennuspaketteja.

### 12.1.3 Organisaation tallenteiden suojaus

Turvamekanismi

Tärkeitä tallenteita tul ee suojata katoam iselta, tuhoutum iselta ja väärentämiseltä lakisääteisten, säädösten, s opimusten ja opetustoim innan vaatimusten mukaisesti.

Keskuspuiston tilanne

Tärkeät tallentee t on s uojattu vika sietoisille p alvelimille, joista tehd ään säännöllisesti varmuuskopiot. Palvelinten käyttö vaatii tunnistuksen. Varmuuskopiointilaitteiston p itäisi sijaita toisessa pa lo-osastossa kuin palvelinjärjestelmä. Varmuuskopioista osan tulisi sijaita jossakin toisessa suojatussa paikassa, jotta varm istettaisiin varmuuskopioiden saavutettavuus siltä varalta, että ensimmäiset ovat tuhoutuneet.

### 12.1.4 Tietosuoja ja henkilötietojen yksityisyys

Turvamekanismi

Tietosuoja ja yksityisyys tulee varm istaa asiaan liittyvissä laeissa, määräyksissä ja mahdollisesti sopimuskohdissa edellytetyllä tavalla.

Keskuspuiston tilanne

Keskuspuistossa noudatetaan lakia, asetuksia ja sopimuksia. Tietosuojaa ja yksityisyyttä kunnioitetaan. Niiden loukka uksia vältetään m äärätietoisesti. Varsinaista varm istustoimenpidettä, muita kuin käyttä jäpalautteet, as ian seurannalle ei ole olemassa.

### 12.1.5 Tietojenkäsittelypalvelujen väärinkäytön estäminen

Turvamekanismi

Käyttäjiä tu lee es tää k äyttämästä tie tojenkäsittelypalveluja luvattom iin tarkoituksiin.

Keskuspuiston tilanne

Käyttäjien k äyttöoikeuksia on hallin nollisesti pyritty saatta maan toim intamahdollisuus säilyttäe n niin rajoitetuksi, että väärink äytökset e ivät olisi huomaamatta mahdollisia. Havaittaessa luvatonta toimintaa käyttäjälle annetaan opas tusta oik eissa toim intatavoissa. Va sta toisena vaihtoeh tona käytetään käyttäjäoikeuksien rajoittamista tai kie ltämistä. Vakavampia luvattomia käyttöjä ei ole toistaiseksi havaittu.

### 12.1.6 Salakirjoitusmekanismeja koskevat säädökset

Turvamekanismi

Salakirjoitusmekanismeja tulee käyttää kaikkien asiankuuluvien sopimusten, lakien ja määräysten mukaisesti.

Keskuspuiston tilanne

Yleisesti käytössä olevina salausmekanismeina käytetään vain käyttöjärjestelmissä tai sovellusohjelmissa olevia valmiita salausmenetelmiä.

## 12.2 Turvallisuuspolitiikan ja standardien noudattaminen ja tekninen vaatimustenmukaisuus

Tavoite Tavoite on varmistaa, että järjestelmät toimivat organisaation turvallisuuspolitiikan ja -standardien mukaisesti.

### 12.2.1 Turvallisuuspolitiikan ja standardien noudattaminen

Turvamekanismi

Esimiesten tulee varmistaa kaikkien vastuualueeseensa sisältyvien turvamenettelyjen virheetön suorittaminen turvallisuuspolitiikan ja -standardien vaatimusten noudattamisen takaamiseksi.

Keskuspuiston tilanne

Järjestelmätuki on seurannut turvamenettelyjen noudattamista ja havaittaessa luvatonta toimintaa käyttäjälle annetaan opastusta oikeissa toimintatavoissa. Vasta toisena vaihtoehtona käytetään käyttäjäoikeuksien rajoittamista tai kieltämistä. Vakavampia luvattomia käyttöjä ei ole toistaiseksi havaittu.

### 12.2.2 Teknisen kelpoisuuden tarkastus

Turvamekanismi

Tavoite on tarkastaa säännöllisesti, että tiedonkäsittelypalvelut täyttävät turvallisuuden toteutusstandardin vaatimukset.

Keskuspuiston tilanne

Manuaalisia tarkistuksia on suoritettu säännöllisesti. Dokumentoituja tarkastusohjeita tai automatisoituja tarkastustyökaluja ei ole.

## 12.3 Tietojärjestelmän tarkastusnäkökohtia

Tavoite Tavoite on maksimoida järjestelmän tarkastusprosessien tehokkuus ja minimoida tietojärjestelmän tarkastusprosessista tai – prosessiin aiheutuvat häiriöt.

### 12.3.1 Tietojärjestelmän tarkastusmekanismit

Turvamekanismi

Auditointivaatimukset ja -toim innot, jotka sisältävät tuotannossa olevien järjestelmien tarkastuksia, tulee suu nnitella huolellisesti ja hyväksyä opetustoimintaprosessien keskeytymisen riskin minimoimiseksi.

Keskuspuiston tilanne

Järjestelmätuki suorittaa henkilöst ösuojalakia noudattaen auditointeja, säännöllisesti selvittäen poikkeam ien syyt ja suorittaen tilanteen vaatim at toimenpiteet.

### 12.3.2 Tietojärjestelmän tarkastusvälineiden suojaus

Turvamekanismi

Pääsyä tietojär jestelmän audito intivälineisiin tulee suo jata m ahdollisen väärinkäytön tai vaarantumisen estämiseksi.

Keskuspuiston tilanne

Tietojärjestelmien auditointityökalut s ijaitsevat operatiivis en järjestelmän ulkopuolella. Niiden saavut ettavuus on rajattu käyttä jätunnuksella ja salasanalla. Tunnuksien määrä on rajattu.