Hammaslaboratorio Oulun Hammaspaja Oy tietoturvakäytäntö

Sisällys

1. Tietoturvapolitiikka

Tietoturvapolitiikassa määritellään, kuinka yrityksessä pyritään varmistamaan tietoturvan kulloinkin riittävä taso.

Tietoturvatoimintaa ohjaavat tekijät

1. Lainsäädäntö ja muut viranomaisohjeet

2. Toimialaa säätelevät ohjeet suositukset
3. Yrityksen maine
4. Liiketoiminnan vaatimukset
5. Liiketoiminnan jatkuvuuden varmistaminen

1. Vastuu tietoturvasta

Viime kädessä yrityksen ja sen asiakkailleen tarjoamien palvelujen tietoturvasta vastaa yrityksen johto.

Yrityksen jokainen työntekijä on osaltaan vastuussa tietoturvan käytännön toteuttamisesta.

Käytettävien ulkopuolisten palvelujen, kuten esimerkiksi pilvipalvelujen, tietoturvasta vastaa kunkin palvelun tarjoaja. Tietoturvavastuiden määrittely sisällytetään yrityksen ja palveluntarjoajan väliseen palvelusopimukseen. Käyttäjät vastaavat siitä, että he käyttävät palvelua turvallisesti.

Yrityksen johdolla on yrityksen henkilökuntaan nähden direktio-oikeus kaikissa tietoturvaan liittyvissä asioissa.

Vastuu tarkoittaa

1. Päättää asioista niin, että tietoturva tulee otetuksi huomioon
2. Ohjeistaa, kouluttaa ja tukea tietoturvan toteuttamisessa
3. Valvontaa ja mahdollisiin poikkeamiin reagointia
4. Riskilähtöisyyttä ja ennakointia

2. Yleiset tietoturvaperiaatteet

1. Riskilähtöisyys
2. Varautuminen
3. Tietoturvan huomioiminen kaikessa toiminnassa
4. Seuranta, lokitus ja nopea reagointi
5. Jatkuva kehittäminen

2. Tekninen tietoturva

3. Käyttäjätunnukset

1. Jokaisella käyttäjällä on tietokoneisiinsa sekä käyttämiinsä järjestelmiin ja palveluihin omat henkilökohtaiset käyttäjätunnukset
2. Käyttäjät vaihtavat salasanansa säännöllisesti, eivätkä anna tunnuksiaan muiden käyttöön tai tietoon
3. Pääsy yrityksen resursseihin on rajattu käyttöoikeuksin työtehtävien suorittamisen edellyttämään laajuuteen
4. Tarpeettomaksi jääneet käyttäjätunnukset poistetaan säännöllisesti järjestelmistä
5. Määräaikaisissa työsuhteissa käyttäjätunnusten voimassaolo päättyy työsuhteen päättyessä

6. Muille kuin yrityksen työntekijöille käyttäjätunnus yrityksen käyttämiin järjestelmiin voidaan luoda yrityksen johdon päätöksellä

2. Varmistukset

1. Yrityksen omilla työasemilla ja/tai palvelimilla sekä tietojärjestelmissä olevat tiedot varmistetaan säännöllisesti ulkoisille varmistusmedioille, kuten siirtokovalevyille ja/tai muistitukuille
2. Varmuuskopiot säilytetään eri paloteknisessä osastossa kuin missä alkuperäinen data sijaitsee
3. Käytettävien pilvipalvelujen tarjoajat hoitavat palveluissa olevien tietojen varmistukset. Varmuuskopiointivastuu sisällytetään yrityksen ja palveluntarjoajan väliseen palvelusopimukseen.

3. Verkon tietoturva

1. Yrityksen langalliset ja/tai langattomat lähiverkot suojataan palomuureilla hyökkäyksiltä, viruksilta, haittaohjelmilta ja ulkoa tulevalta liikenteeltä.
2. Verkkolaitteiden, kuten reitintinten, kytkinten ja langattoman verkon päätelaitteet (wifi-tukiasemat) pidetään ohjelmistopäivitysten osalta jatkuvasti ajan tasalla
3. Yrityksen langaton verkko on suojattu ja vaatii kirjautumisen. Verkon suojausavain pidetään ainoastaan yrityksen henkilökunnan tiedossa.
4. Verkon ulkoreunalla olevat aktiivilaitteet kuten palomuurit ja reitittimet pidetään ohjelmistopäivitysten osalta jatkuvasti ajan tasalla

4. Etäkäytön tietoturva

1. Ulkopuoliset palvelutoimittajat pääsevät rajoitetusti tarvitsemassaan laajuudessa käyttämään yrityksen työasemia etätukiratkaisun avulla

5. Palvelinten tietoturva

1. Palvelimet pidetään käyttöjärjestelmien tietoturvapäivitysten suhteen säännöllisesti ajan tasalla
2. Muiden varusohjelmien osalta erityisen kriittisen tarpeen ilmetessä
3. Palvelimissa on asennettuna ajantasainen virus- ja haittaohjelmien torjunta mahdollisuuksien mukaan. Joissakin tapauksissa palvelimilla ajettavat järjestelmät / sovellukset voivat rajoittaa virustorjunnan käyttöä
   Yrityksellä ei tällä hetkellä ole käytössään omia palvelimia.

6. Työasemien tietoturva

1. Työasemiin asennetaan käyttöjärjestelmien ja varusohjelmien tietoturvapäivitykset automaattisesti tai manuaalisesti välittömästi, kun uusi versio on julkaistu
2. Työasemissa on käytössä virus- ja haittaohjelmien torjunta sekä ohjelmallinen palomuuri

7. Mobiililaitteiden tietoturva

1. Puhelimet ja muut mobiililaitteet on suojattava lukitusnäytön pääsykoodilla. Tästä ohjeistetaan käyttäjiä aina, kun heidän käyttöönsä annetaan ko. laitteita
2. Mobiililaitteissa on käytössä virus- ja haittaohjelmien torjunta sekä ohjelmallinen palomuuri

8. Tiedonsiirrot

1. Tiedonsiirto työasemien, mahdollisten palvelinten, tietojärjestelmien ja palvelujen välillä suojataan kulloinkin tarkoituksenmukaisella ja siirtoa mahdollisesti koskevien määräysten edellyttämällä tavalla
2. Sähköpostissa tai sen liitetiedostoina ei saa välittää mitään luottamuksellista aineistoa. Tästä ohjeistetaan käyttäjiä

9. Viestinnän tietoturva

1. Sähköpostiliikenne on suojattu viruksilta ja haittaohjelmilta työasemien virus- ja haittaohjelmien torjunnan avulla
2. Viestintäratkaisuja liiketoimintojen käyttöön valittaessa ja niitä käytettäessä on ratkaisun tietoturva huomioitava

3. Tietojärjestelmien tietoturva

1. Tietojärjestelmiin annetaan käyttöoikeuksia ainoastaan niille työntekijöille, jotka kulloinkin järjestelmää käyttävät
2. Mikäli tarkoituksenmukaista, käyttöoikeuksia rajataan käyttäjäryhmillä järjestelmän sisällä
3. Käyttäjien sisäänkirjautumiset järjestelmään kirjataan lokeihin järjestelmän sisäisten lokituskäytäntöjen puitteissa
4. Tietojärjestelmien pääkäyttäjä- / ylläpitäjätunnukset ovat vain kunkin järjestelmän pääkäyttäjän ja ylläpitäjien sekä asianomaisen järjestelmätoimittajan tiedossa. Niitä ei saa luovuttaa edelleen missään tilanteessa
5. Järjestelmän pääkäyttäjät ohjeistavat, kouluttavat ja tukevat järjestelmän muita käyttäjiä myös tietoturvaan liittyvissä asioissa

4. Verkkopalveluiden tietoturva

10. Käytettävien palveluiden tietoturva

1. Käytetään ainoastaan tietoturvallisiksi todettuja palveluja
2. Lähtökohtaisesti jokaisella käyttäjällä on henkilökohtainen tunnus ja riittävän vahva salasana
3. Työsuhteen päättyessä tai palvelun käytön loppuessa on huolehdittava, että palvelun käyttäjätunnus poistetaan tai ainakin lukitaan
4. Työntekijät eivät saa käyttää henkilökohtaisia tilejään yrityksen asioiden hoitoon eivätkä yrityksen tilejä henkilökohtaisten asioiden hoitoon
5. Kaikkien käytettävien palvelujen on oltava yrityksen pääkäyttäjän hallinnoitavissa käyttäjätunnusten perustamisen ja poistamisen suhteen
6. Palveluympäristön sijainti on valittava tarvittaessa niin, että se täyttää palvelun luonteen, sen sisällön tai siellä säilytettävän datan osalta asetetut määräykset

2. Tarjottavien palveluiden tietoturva

1. Tarjottavat palvelut on suunniteltava ja toteutettava niin, että ne ovat tietoturvallisia käyttäjille, yrityksille ja rekisteröidyille sekä yritykselle itselleen

2. Kaikki tässä dokumentissa esiin tuodut tietoturvan näkökulmat on otettava tilanteeseen ja palvelun luonteeseen soveltaen huomioon

3. Palveluympäristön sijainti on valittava tarvittaessa niin, että se täyttää palvelun luonteen, sen sisällön tai siellä säilytettävän datan osalta asetetut määräykset

4. Mikäli käyttäjä voi rekisteröityä ja sen jälkeen kirjautua palveluun, on käyttäjän salasana tallennettava salatussa muodossa. Käyttäjän kirjautuessa käyttäjän syöttämää salasanaa on verrattava tallennettuun salasanaan niin, että käyttäjän antama salasanan salataan, jolloin vertaamisessa käytetään salattuja salasanoja

Fyysinen tietoturva

1. Toimitilat on suojattu asiattomalta pääsyltä lukituksen/hälytyslaitteen avulla.

6. Paperimuodossa olevien henkilötietojen käsittely

1. Työkorttien toiset kappaleet säilytetään lukitussa arkistossa niille säädetyn säilytysajan. (Toiset kappaleet lähetetään työn mukana tilaajalle.)

7. Organisaation tietoturva

1. Tietoturvapolitiikka sekä yksityiskohtaisempi ajantasainen käytännön tietoturvaohjeistus pidetään yrityksen henkilöstön saatavilla.

2. Yrityksen johto vastaa tietoturvaan liittyvästä ohjeistuksesta ja koulutuksesta henkilökunnan perehdytyksen ja jatkuvan kouluttamisen puitteissa

8. Dokumentointi

Yleistä dokumentaatiota ovat

1. Tietoturvakäytäntö (tämä dokumentti)

2. Tietosuojakäytäntö

3. Mahdollinen muun tietoturvaohjeistus

Dokumentaatiota päivitetään tarpeen ja muuttuneen tilanteen mukaan.

9. Seuranta

Yrityksen johto seuraa tietoturvan toteutumista sekä havainnoi toimintaympäristön ja yleisen tietoturvatilanteen muutoksista johtuvia kehitystarpeita.

Havaittuihin puutteisiin reagoidaan tarvittavalla nopeudella ja laajuudella.

10. Tiedottaminen

Yrityksen johto tiedottaa ja ohjeistaa henkilöstöä muuttuneesta tietoturvatilanteesta tarpeen mukaan.

Jokainen yrityksen työntekijä on velvollinen ilmoittamaan esimiehelleen tai yrityksen johdolle havaitsemistaan tai epäilemistään tietoturvauhista, -puutteista tai -tapahtumista.

11. Hyväksyminen ja voimaantulo

Oulun Hammaspaja Oy:n johto on 17.04.2018 hyväksynyt tämän tietoturvakäytännön ja se on voimassa samasta päivästä lukien.