Tietosuojan osoitusvelvollisuutta edistävät työpajatilaisuudet

#tuki2018 #stöd2018

Työpaja #3 – 4.9.2017

- **Tietoturvallisuuden toteuttaminen organisaation toiminnassa – mitä asetus edellyttää, ja miten vaatimukset käytännössä toteutetaan**
- **Riskienhallinta osa 3, riskien hallinta ja toimenpiteiden seuranta sekä arviointityöpajojen toteuttaminen**

Kuntaliitto Kommunförbundet

TIETOSUOJAVALTUUTETUN TOIMISTO

Valtori | Valtion tieto- ja viestintätekniikkakeskus

OIKEUSMINISTERIÖ JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto

Tilaisuuden ohjelma

#tuki2018 #stöd2018

- 8.30 Kahvi
- 9.00 Tilaisuuden avaus – Tuula Seppo, Kuntaliitto & Kimmo Rousku, valtiovarainministeriö
- 9.15 Mikä on tarvittava tietoturvallisuuden vähimmäistaso?
- 10.30 Bio- ja jaloittelutauko
- 10.45 Työpaja jatkuu: Tietoturvallisuuden toteuttaminen organisaation toiminnassa – mitä asetus edellyttää ja miten vaatimukset käytännössä toteutetaan
- 12.15 Lounastauko (omakustanne)
- 13.00 Riskienhallinta osa 3, riskien hallinta ja toimenpiteiden seuranta sekä arviointityöpajojen toteuttaminen
- 14.30 Kahvitauko
- 14.45 Työpaja jatkuu
- 16.00 Yhteenveto ja kotitehtävä
- 16.15 Työpaja päättyy

Tietoturvallisuus organisaation toiminnassa – miten vaatimukset käytännössä toteutetaan?

Tietoturvallisuuden hallintajärjestelmä (ISMS) – esimerkki: ISO/IEC 27000-standardiperhe

- ISO/IEC 27000 standardiperhe on otsikoitu “Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät”
- Maailmanlaajuisesti käytetyimpiä tietoturvan viitekehyksiä
- Puhutaan tietoturvasta, mutta se käsitetään lähinnä sateenvarjokäsitteeksi: suojattava kohde / tieto on keskiössä.
- ISO/IEC 27001 on standardisarjan päädokumentti, jossa määritellään keinot organisaation tietoturvallisuuden hallintajärjestelmän luomiseen, ylläpitoon ja jatkuvaan parantamiseen.
- ISO/IEC 27002 täydentää 27001 -standardia määrittämällä tarkentavia tietoturvallisuuden hallintaa koskevia menettelyohjeita
- Muut 27000 -perheen standardit tukevat 27001 -standardin soveltamista määrittämällä ohjeita ja kriteerejä mm. tietoturvallisuuden hallintakeinojen mittaamiseen, auditointiin ja sertifiointiin
- Standardin noudattamisella ja sen osoittamisella voidaan osaltaan vastata osoitusvelvollisuuden täyttämisen velvoitteeseen
- Huomaa myös 27005 (riskienhallinta), 27032 (kyberturvallisuus), 27035 (tietoturvahäiriöiden hallinta), 27036 toimittajasuhteiden tietoturvallisuus

Tietoturvallisuuden hallinta

#tuki2018 #stöd2018

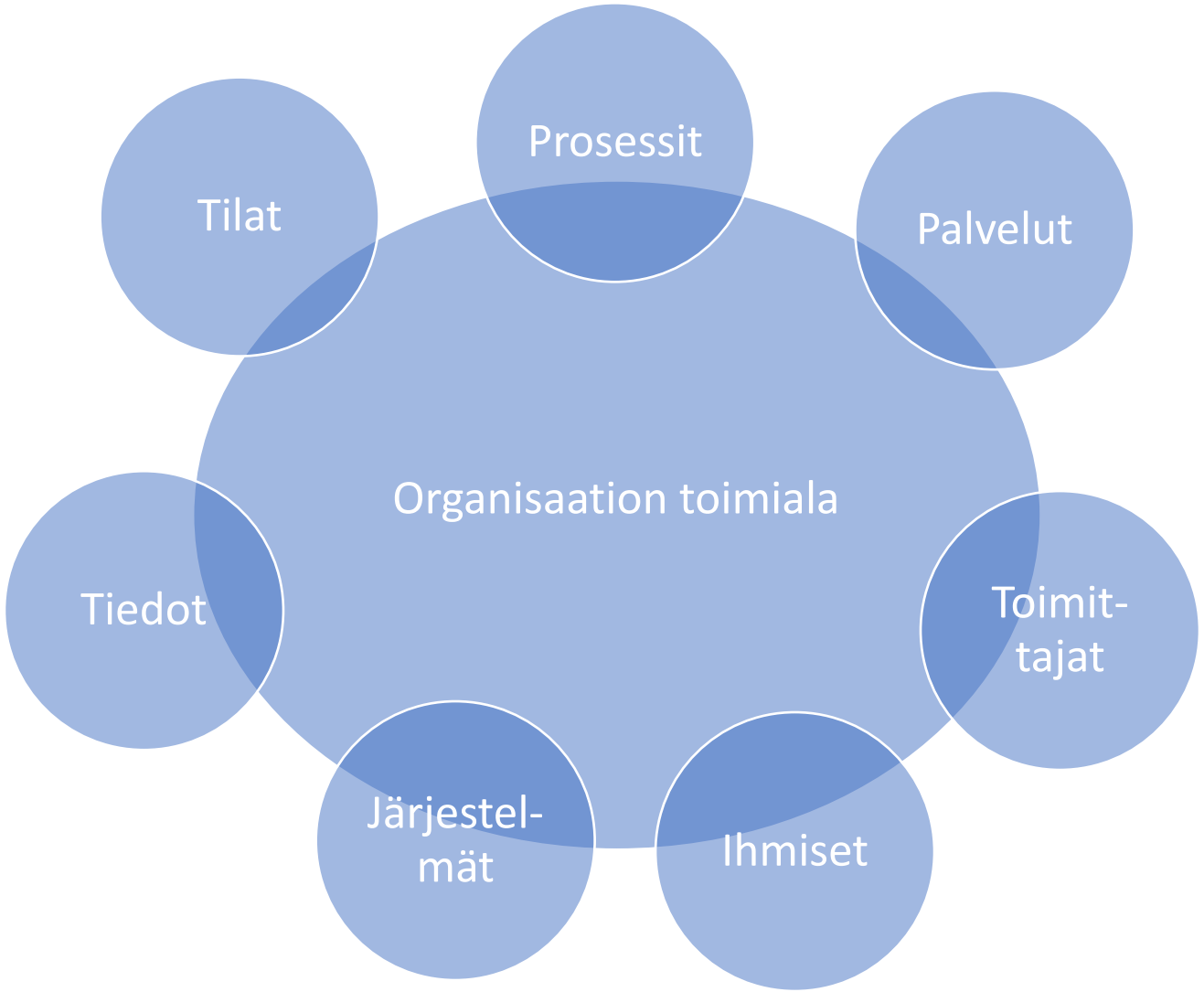
1. Tietoturvan hallinnan ympäristön määrittely

#tuki2018 #stöd2018

1. Organisaation toimintaympäristö
2. Lakisääteiset vaatimukset
3. Riskienhallinta
4. Tietoturvapolitiikka ja -ohjeet
5. Tietoturvaorganisaatio

2. Suojattavien kohteiden tunnistaminen

#tuki2018 #stöd2018



3. Riskien tunnistaminen ja analysointi

#tuki2018 #stöd2018

1. Uhkien tunnistaminen
2. Riskien vaikutusten analysointi
3. Riskien hallintakeinojen valinta
4. Riskitason määritys

4. Suojauskeinojen valinta ja käyttöönotto

#tuki2018 #stöd2018

A.5: Tietoturvapolitiikat (2 hallintakeinoa)

A.6: Tietoturvallisuuden organisointi (7 hallintakeinoa)

A.7: Henkilöstöturvallisuus (6 hallintakeinoa, joita sovelletaan ennen työsuhdetta, sen aikana ja sen jälkeen)

A.8: Suojattavan omaisuuden hallinta (10 hallintakeinoa)

A.9: Pääsynhallinta (14 hallintakeinoa)

A.10: Salaus (2 hallintakeinoa)

A.11: Fyysinen turvallisuus ja ympäristön turvallisuus (15 hallintakeinoa)

A.12: Käyttöturvallisuus (14 hallintakeinoa)

A.13: Viestintäturvallisuus (7 hallintakeinoa)

A.14: Järjestelmien hankkiminen, kehittäminen ja ylläpito (13 hallintakeinoa)

A.15: Suhteet toimittajiin (5 hallintakeinoa)

A.16: Tietoturvahäiriöiden hallinta (7 hallintakeinoa)

A.17: Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia (4 hallintakeinoa)

A.18: Vaatimustenmukaisuus (8 hallintakeinoa, sisältäen sisäiset vaatimukset kuten politiikat ja ulkoiset vaatimukset, kuten lainsäädäntö)

5. Riskien ja tietoturvallisuuden valvonta

#tuki2018 #stöd2018

1. Tietoturvan ja riskien valvonta ja raportointi
2. Sisäiset ja ulkoiset auditoinnit
3. Tekninen valvonta
4. Toimittajien valvonta

Tekninen valvonta *

- Lokien keräys
- SIEM
- IDS/IPS
- Antivirus
- Roskapostisuodatus
- Salatun liikenteen avaaminen
- Data Loss Prevention – teknologiat (”DLP”)

* Huom! YT-menettely

6. Riskien ja tietoturvan hallinnan kehittäminen

#tuki2018 #stöd2018

1. Tietoturvatason nostaminen
2. Järjestelmien tason vastaavuus tietosisällön vaatimuksiin
3. Riskien vähentäminen
4. Kustannusten optimointi
5. Vaatimusten kohdentaminen

6. Riskien ja tietoturvan hallinnan kehittäminen

#tuki2018 #stöd2018

- Tietoturvaa ja tietoturvariskien hallintaa kehitetään jatkuvasti valvontatiedon ja tilannekuvan perusteella → Uusien teknologioiden käyttöönotto automaattisessa valvonnassa lisää tietoisuutta ja pienentää tietoturvariskejä
- Tietoturvavaatimuksia parannetaan ja kohdennetaan hankintoihin aktiivisesti tietoturvaorganisaation toimesta → Tietoturva on mukana kaikissa uusien järjestelmien hankinnoissa sekä sopimusneuvotteluissa
- Tietoturvan tasoa optimoidaan jatkuvasti, tavoitteena että mitään järjestelmää / tietoa ei suojata yli sen vaatimusten→ kustannukset järjestelmien vaatimustenmukaisuudesta pienenevät

Tietoturvapolitiikka

Tietoturvapolitiikka

#tuki2018 #stöd2018

- Organisaation johdon tulee osoittaa tukensa ja sitoutumisensa tietoturvallisuuden kehittämiseen julkaisemalla ja ylläpitämällä tietoturvallisuuspolitiikka
- Politiikka pyrkii osoittamaan tietoturvallisuuden merkityksen organisaation toimintaan ja johdon tahtotilan tietoturvallisuuden ylläpitämiseksi ja kehittämiseksi
- Politiikan tulee olla johdon hyväksymä ja allekirjoittama. Se tulee olla kaikkien työntekijöiden ja relevanttien kolmansien osapuolien saatavilla ja tiedossa.

Tietoturvapolitiikka

#tuki2018 #stöd2018

- Politiikassa tulisi olla määritetty mm. seuraavat asiat:
  - Tietoturvallisuuden määritelmä, sen kokonaistavoitteet ja kattama alue
  - Tietoturvallisuuden merkitys liiketoiminnan edistäjänä ja tiedon jaon mahdollistajana
  - Organisaation johdon tahto ja tavoitteet
  - Tietoturvallisuuden kontrollitavoitteiden ja kontrollien viitekehys / implementointitapa
  - Tietoturvapolitiikan, periaatteiden, standardien ja vaatimusten määritelmä ja vaatimukset
  - Lainsäädännöllisten ja muiden säännösten asettamat vaatimukset
  - Tietoturvakoulutukset ja tietoisuuden lisäämisen periaatteet
  - Viittaus liiketoiminnan jatkuvuussuunnitteluun
  - Tietoturvarikkomusten seuranta ja sanktiot
  - Tietoturvallisuuteen liittyvät vastuut ja velvollisuudet sekä raportointikanavat
  - Viittaukset täydentäviin dokumentteihin ja muihin tietolähteisiin

- Kaikkea ei välttämättä dokumentoida kokonaisuudessaan politiikkaan, koska se pyritään pitämään mahdollisimman yleisellä tasolla ja riittävän lyhyenä

Ulkoistuskumppanit ja tietoturva (käsitellään laajemmin erillisissä työpajoissa)

Tiedonkäsittelyn ulkoistuskumppaneita koskevat vaatimukset

#tuki2018 #stöd2018

- Ulkoistussopimuksessa on sovittava vastuista ja erityisesti siitä, että henkilötietojen käsittelijä mm.
  - käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti, mikä koskee myös henkilötietojen siirtoja kolmanteen maahan tai kansainväliselle järjestölle (poikkeuksia);
  - varmistaa, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus;
  - toteuttaa kaikki 32 artiklassa vaaditut toimenpiteet;
  - ottaen huomioon käsittelytoimen luonteen auttaa rekisterinpitäjää asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä mahdollisuuksien mukaan täyttämään rekisterinpitäjän velvollisuuden vastata rekisteröityjen pyyntöihin;

Tiedonkäsittelyn ulkoistuskumppaneita koskevat vaatimukset (jatkuu)

#tuki2018 #stöd2018

- Ulkoistussopimuksessa on säädettävä erityisesti, että henkilötietojen käsittelijä mm.
  - auttaa rekisterinpitäjää varmistamaan, että 32–36 artiklassa säädettyjä velvollisuuksia noudatetaan ottaen huomioon käsittelyn luonteen ja henkilötietojen käsittelijän saatavilla olevat tiedot (→ tietoturvaloukkaukset ja tietosuojan vaikutustenarvioinnit);
  - rekisterinpitäjän valinnan mukaan poistaa tai palauttaa käsittelyyn liittyvien palveluiden tarjoamisen päätyttyä kaikki henkilötiedot rekisterinpitäjälle ja poistaa olemassa olevat jäljennökset, paitsi jos unionin oikeudessa tai jäsenvaltion lainsäädännössä vaaditaan säilyttämään henkilötiedot;
  - saattaa rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen tässä artiklassa säädettyjen velvollisuuksien noudattamisen osoittamista varten, ja sallii rekisterinpitäjän tai muun rekisterinpitäjän valtuuttaman auditoijan suorittamat auditoinnit, kuten tarkastukset, sekä osallistuu niihin.

Tietoturvaloukkaukset ja ilmoitusvelvollisuus

(käsitellään laajemmin erillisissä työpajoissa)

Artikla 33-34 - Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle ja rekisteröidyille

#tuki2018 #stöd2018

- Henkilötietojen tietoturvaloukkauksella tarkoitetaan tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.
  - Jos järjestelmään, jossa henkilötietoja käsitellään tai siirretään, kohdistuu palvelunestohyökkäys, kohdistuuko siihen henkilötietojen tietoturvaloukkaus?

Artikla 33-34 - Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle ja rekisteröidyille

#tuki2018 #stöd2018

- Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta toimivaltaiselle valvontaviranomaiselle, paitsi jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä.
- Jos ilmoitusta ei anneta 72 tunnin kuluessa, rekisterinpitäjän on toimitettava valvontaviranomaiselle perusteltu selitys.
- Jos tapahtuman seurauksena saattaa olla korkeita riskejä rekisteröityjen kannalta, ilmoitus on tehtävä myös rekisteröidyille.

Artikla 33-34 - Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle ja rekisteröidyille

#tuki2018 #stöd2018

- Henkilötietojen käsittelijän on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa.
- Tiedonannossa viranomaiselle/rekisteröidyille on vähintään
  a. kuvattava henkilötietojen tietoturvaloukkaus, mukaan lukien mahdollisuuksien mukaan asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät;
  b. ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa;
  c. kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset;
  d. kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.

→ **Suunniteltava prosessi ja valmis lomake, saatava käsittelijältä riittävät tiedot**

Esimerkki ISO 27001 kontrolleista

Kontrollitavoitteet

#tuki2018 #stöd2018

Tietojen luokittelu

- Kontrollitavoite: Varmistaa, että kaikki tieto tulee asianmukaisella ja riittävällä tavalla suojatuksi
  - Luokittelu tulisi tehdä niin, että se osoittaa tarpeen, prioriteetit ja odotetun suojaustason
  - Tietojenluokittelu käytäntö tulisi ottaa käyttöön ja sen tulisi osoittaa tarvittavat suojaustasot sekä tavat, joilla eri luokkiin kuuluvia tietoja saadaan käsitellä

Käytännön keinot – kontrollit

#tuki2018 #stöd2018

Luokitteluohjeet:

- Kontrolli: Tiedon luokittelussa tulisi huomioida tiedon arvo, lainsäädännön asettamat vaatimukset, tiedon luottamuksellisuuden taso sekä kriittisyys organisaation toiminnalle

Tiedon merkitseminen ja käsittely

- Kontrolli: Tietojen luokittelun mukaiseen merkitsemiseen ja käsittelyyn tulisi olla riittävät ja asianmukaiset tavat ja käytännöt

RYHMÄTEHTÄVÄ

Ryhmätehtävä 1

#tuki2018 #stöd2018

1. Mitä organisaationne tietoturvan hallinnassa tulee muuttaa, jotta tietosuoja-asetuksen vaatimukset voidaan täyttää? (ks. erityisesti 32 artikla)

(Tukikysymyksiä:

- Millaisia xxx kontrolleja tunnistat olevan teillä jo käytössä?
- Mitkä xxx kontrolleista jossain tietyssä (ei tarvitse sanoa missä) järjestelmässä on mielestäsi riittävällä tasolla? Miksi?
- Mitkä kontrollit vaativat korjaamista ensiksi?
- Kuinka tärkeimmät korjaukset saadaan aikaan – mitä pitää olla olemassa, jotta korjaaminen voi onnistua?)

Käytännön tietoturvakontrolleja

Työkalu tietojärjestelmien arviointiin / GDPR & tietoturva

#tuki2018 #stöd2018

		Kyselyyn vastaaja:									
		Järjestelmän nimi:									
Tietoturvan osa-alue	**Järjestelmän ylläpito**	**Suostumus-ten hallinta** *Luottamuksellisuus*	**Käyttäjien-hallinta** *Luottamuksellisuus*	**Pääsyn-valvonta** *Luottamuksellisuus*	**Lokitus** *Luottamuksellisuus*	**Lokitus** *Luottamuksellisuus*	**Lokitus** *Luottamuksellisuus*	**Lokitus** *Luottamuksellisuus*	**Varmuus-kopiointi** *Eheys, saatavuus*	**Varmuus-kopiointi** *Eheys, saatavuus*	**Tietoturv päivityks** *Luottamu lisuus, eh saatavuu*
Vaatimus	Vastaako järjestelmän ylläpidosta organisaatio vai onko se ulkoistettu?	Tukeeko tietokanta suostumusten ja kieltojen hallintaa?	Onko kaikilla käyttäjillä yksilölliset käyttäjätunnukset?	Onko salasanoilla laatuvaatimukset? Millaiset?	Lokitetaanko järjestelmään kirjautuminen?	Lokitetaanko henkilötietojen käyttö?	Lokitetaanko admin-käyttäjien toimet?	Onko järjestelmän tuottamien lokien muuttaminen tai poistaminen estetty?	Onko järjestelmän ja sen tietojen varmuuskopioinnista suunnitelma, joka huomioi erilaiset tietojen palautustarpeet?	Testataanko varmuuskopioiden palautuksia?	Onko järjestelm automatis (tietoturva vitysten jakelu?
Vastaus											

KOTITEHTÄVÄ

Kotitehtävä – tietoturvallisuuden toteuttaminen

#tuki2018 #stöd2018

1. Laadi suunnitelma tietosuojan huomioonottamisesta tietoturvan hallinnassa organisaatiossasi
2. Sovella työpajassa esiteltyä työkalua yhteen valinnaiseen järjestelmään ja sen tietoturvaan

Lopuksi

Kertaus

#tuki2018 #stöd2018

1. Toimitamme linkin tilaisuuden palautekyselyyn ja materiaaleihin
2. Tee kotitehtävät – varmista että työpajassa käsitellyt asiat etenevät organisaatiossasi
3. Ilmoittaudu seuraavaan työpajaan kun laitamme sinulle linkin
4. Vastaa viikkoa ennen seuraavaa työpajaa toimittamaamme kyselyyn koskien kotitehtävien suorittamista
5. Katso Arjen tietosuoja-videot ja suorita nettitesti – huolehdi, että organisaatiosi huolehtii sen levittämisestä henkilöstölle viimeistään syksyn aikana – sekä kerää tiedot ja varmistaa, että henkilöstö katsoo sen ja suorittaa nettitestin hyväksytysti

#tuki2018 #stöd2018

Kysymykset materiaaliin liittyen voi osoittaa:

Mikko Viemerö (CIPP/E, CIPM, CIPT, CISA, CISM)
KPMG Cyber Security Services
+358 20 760 3530
mikko.viemero@kpmg.fi

Kuntaliitto
Kommunförbundet

TIETOSUOJAVALTUUTETUN TOIMISTO

Valtori | Valtion tieto- ja viestintäteknikkakeskus

OIKEUSMINISTERIÖ
JUSTITIEMINISTERIET

VALTIOVARAINMINISTERIÖ

Viestintävirasto