ULKOMINISTERIÖ PÄÄTÖS PC0UC1LR-48

19.12.2019

Asia

Ulkoasiainhallinnon tietoturvapolitiikka

Tietoturvatoiminta on ulkoasiainhallinnon kokonaisturvallisuuden hallinnan keskeinen osa-alue. Tämä asiakirja toimii perustana, jonka varaan ulkoasiainhallinnon tietoturvatoiminta rakentuu. Tämä asiakirja on vahvistettu ulkoministeriön johtoryhmän (virkamieskokoonpano) kokouksessa 5.11.2019 ja sillä kumotaan päätös ”Tietoturvallisuus ulkoasiainhallinnossa” (HELK305-8, 15.4.2009).

Vastuullisuus ja vaatimustenmukaisuus

Ulkoasiainhallinnossa suhtaudutaan vastuullisesti tietoturvallisuudesta huolehtimiseen. Samalla jokaisen toimintaan osallistuvan henkilön edellytetään toimivan vastuullisesti. Ulkoasiainhallinnon toiminnassa noudatetaan sitä koskevia säädöksiä, määräyksiä ja muita velvoitteita ottaen huomioon toimialan erityisvaatimukset.

Suojattavat kohteet ja hyväksyttävä käyttö

Tärkeimmät ulkoasiainhallinnon tietoturvatoiminnalla suojattavat kohteet ovat tiedot ja varsinaiseen toimintaan liittyvät prosessit, toiminnot, palvelut ja tietojärjestelmät sekä näitä tukevat resurssit ja infrastruktuuri. Tietoturvajärjestelyillä huolehditaan ulkoasiainhallinnon omien ja sen hallussa olevien tietojen ja niiden käsittelyn hallinnollisesta, teknisestä ja fyysisestä tietoturvallisuudesta (eheys, saatavuus, luottamuksellisuus, kiistämättömyys) tietojen olomuodosta ja sijainnista riippumatta.

Tietoturvajärjestelyillä tuetaan myös tietosuojanäkökohtien toteutumista.

Tietoturvallisuuteen liittyvät prosessit, menettelyt ja mekanismit on vakioitava ja dokumentoitava. Toimintaan liittyviä suojattavia tietoaineistoja, tietojärjestelmiä, työvälineitä ja muuta suojattavaa omaisuutta käytetään työtehtävien mukaisiin hyväksyttyjä tarpeita palveleviin tarkoituksiin.

Lähtökohtana on työtehtäviin perustuva tarve esim. käsitellä tietoja, päästä suojattuihin tietojärjestelmiin tai päästä luokiteltuihin toimitiloihin.

Politiikan kattavuus

Tietoturvatoiminta kattaa koko ulkoasiainhallinnon toiminnan, kaikki osastot ja yksiköt ml. erillisyksiköt sekä ulkomaan edustukseen kuuluvat edustustot ja avustavat toimielimet, kaikissa tilanteissa.

Tietoturvallisuuden kehittäminen sovitetaan yhteen palveluprosessien, toimintatapojen, henkilöstön koulutuksen ja teknisten ratkaisujen kehittämisen kanssa.

Tietoturvavaatimukset koskevat kaikkia ulkoasiainhallinnon henkilökuntaan kuuluvia ja ulkoasiainhallinnon kanssa yhteistyössä tai toimeksiannosta työskenteleviä henkilöitä sekä yhteistoimintaan liittyvin osin heidän taustaorganisaatioitaan.

Tietoturvatoiminnan päämäärät ja tavoitteet

Tietoturvatoiminnan tulee tukea ulkoasiainhallinnon tavoitteiden saavuttamista ja päivittäisen työn tekemistä, hallita tiedon käsittelyä uhkaavia riskejä ja pyrkiä osaltaan mahdollistamaan uusia, tehokkaampia toimintatapoja.

Tarkoituksena on, että:

- Tietoturvatoiminta on ammattitaitoista ja luotettavaa
- Ulkoasiainhallinnon omat ja muiden sidosryhmien asettamat tietoturvallisuutta koskevat vaatimukset ja odotukset täytetään
- Tietoturvariskit ovat hallinnassa
- Tietoturvallisuuden hallinnan järjestelyt edustavat hyvää kansainvälisten ja kansallisten standardien määrittämää tasoa
- Tietoturvallisuus täyttää käsittelyprosesseja koskevat vaatimukset
- Tietojärjestelmien tekninen turvallisuus täyttää tietojärjestelmiä koskevat erityisvaatimukset

Täsmällisemmät tavoitteet asetetaan toiminnan ja talouden suunnittelun sekä strategiatyön yhteydessä.

Tietoturvariskien hallinta

Tietoturvallisuudesta huolehtiminen on osa normaalia toiminnan ylläpitämistä, kehittämistä, riskienhallintaa ja tulosohjausta. Tietoturvatoiminnan avulla on otettava hallintaan tietoturvariskit ja pidettävä ne tasolla, joka turvaa edellytykset varsinaisen toiminnan jatkuvuudelle, tehokkuudelle ja laadulle.

Organisointi ja vastuut

Tietoturvallisuudesta vastaavat kaikki ulkoasiainhallinnossa työskentelevät, kukin oman vastuu- ja tehtäväalueensa osalta. Vastuustaan huolehtimiseksi jokaiselle tarjotaan koulutusta, ohjeistusta ja turvallinen toimintaympäristö. Jokaisen velvollisuutena on perehtyä itseään ja vastuualuettaan koskeviin ulkoasiainhallinnon tietoturvallisuutta koskeviin kuvauksiin ja ohjeisiin, noudattaa niitä.

Kokonaisvastuu organisaation tietoturvallisuudesta sekä tietoturvapolitiikan toteuttamisedellytyksistä on ulkoministeriön johdolla.

Tietoturvallisuuden hallintajärjestelmän kehittämisen ja valvonnan koordinoinnista vastaa tietoturvapäällikkö. Tietoturvatoimintaa tukemaan ja kehittämään voidaan perustaa tarvittavia työryhmiä. Tietoturvatoimintaa kehitetään yhteistyössä ministeriön turvallisuuden ja riskienhallinnan eri osa-alueiden vastuutahojen ja -henkilöiden kanssa.

Tämän päätöksen ja sitä täydentävien kuvausten ja ohjeiden vastaiseen toimintaan puututaan korjaavilla tai kehittävillä toimenpiteillä ja seuraamusmenettelyillä.

Resursointi

Resurssit suunnataan tietoturvallisuuden kannalta keskeisiin kohteisiin. Tietoturvallisuuden edellyttämät resurssitarpeet otetaan huomioon toiminta- ja taloussuunnitelmissa sekä tulosohjaus- ja kehysprosesseissa.

Seuranta ja arviointi

Määritettyjen tietoturvavaatimusten toteutumista sekä menettelyiden ja ohjeiden noudattamista seurataan, mitataan, arvioidaan ja auditoidaan.

Jokaisen toimintaan osallistuvan velvollisuutena on ilmoittaa havaitsemistaan tietoturvapuutteista ja heikkouksista sekä tapahtuneista häiriöistä tai niiden epäilyistä ja läheltä piti tilanteista ao. vastuutaholle, jonka velvollisuutena on ryhtyä tarvittaviin toimenpiteisiin ilman aiheetonta viivettä.

Vaatimusten, menettelyiden ja ohjeiden vastaiseen toimintaan puututaan korjaavilla ja kehittävillä toimenpiteillä ja tarvittavilla seuraamusmenettelyillä.

Jatkuva parantaminen

Tietoturvallisuuteen liittyvien prosessien, menettelyiden ja mekanismien on edustettava hyvää hallintokäytäntöä ja oltava jatkuvan parantamisen kohteena.

Toimeenpano

Kullakin vastuualueella on ryhdyttävä tarvittaviin toimenpiteisiin tämän tietoturvapolitiikan saattamiseksi osaksi käytännön toimintaa. Toiminnasta, palveluista ja tietojärjestelmistä vastaavien ja niiden kehittäjien velvollisuutena on ottaa tietoturvallisuus ja tietosuoja huomioon jo palvelujen ja järjestelmien suunnitteluvaiheessa.

Ministeriön ja edustustojen johto ja esimiehet luovat toimintaedellytykset toiminnan tietoturvallisuudelle sekä toimivat esimerkkinä ja kannustavat tietoturvallisiin toimintatapoihin. Esimiesten velvollisuutena on puuttua havaitsemiinsa tai heidän tietoonsa saatettuihin tietoturvahäiriöihin ja -poikkeamiin.

Tätä politiikkaa täsmennetään ja täydennetään esim. osa-aluekohtaisilla linjauksilla sekä suunnitelmilla, menettelytapakuvauksilla ja ohjeilla.

Lisätietoja: UM Tietoturva

Päätöksentekijä:

Matti Anttonen
Valtiosihteeri

Esittelijä:

Ari Uusikartano
Tietohallintojohtaja

Viite

Ministeriön johtoryhmän (virkamieskokoonpano) 5.11.2019, PC0TQ390-78

Liitteet

-

Videeraus:

LKP
-
TAKP:
-
TU:
-
TE:
-
PROJ:
-
KUMP:
-
TEHTÄVÄNUMERO:
-

Hallintopalvelut
HAL-40 Antti Savolainen

Asiasanat	TIETOTURVALLISUUS
Hoitaa	**HAL-40**
Hoitaa UE	
Koordinoi	
Tiedoksi	ALI-01; ALI-02; ALI-10; ALI-20; ALI-30; ALI-40; ASA-01; ASA-02; ASA-10; ASA-20; ASA-30; ASA-40; AVS-KEO; AVS-PAL; AVS-POL; AVS-TUO; EUR-01; EUR-02; EUR-10; EUR-20; EUR-30; EUR-40; EVA-11; HAL-01; HAL-10; HAL-11; HAL-13; HAL-41_VNHY; HAL-44; HAL-45; HAL-60; HAL-70; ITÄ-01; ITÄ-02; ITÄ-10; ITÄ-20; KEO-01; KEO-02; KEO-10; KEO-20; KEO-30; KEO-50; KEO-70; KEO-80; KEO-90; KPA-01; KPA-02; KPA-10; KPA-20; KPA-30; KPA-40; NSA-00; OIK-01; OIK-02; OIK-09; OIK-10; OIK-20; OIK-30; OIK-40; POL-01; POL-02; POL-10; POL-20; POL-30; POL-40; POL-50; PRO-00; STU-00; STY-00; TAS-10; TUO-01; TUO-02; TUO-10; TUO-20; TUO-30; UKKMI-00; UMI-00; VIE-01; VIE-02; VIE-10; VIE-20; VIE-30; VIE-40; VIE-50; VSI-00 ABA; ABO; ADD; ALG; ANK; ATE; BAN; BEI; BEO; BER; BOG; BRA; BRN; BRY; BUD; BUE; BUK; CAN; DAR; DUB; ENE; EUE; GEN; HAA; HAN; HNG; JAK; KAB; KAI; KAT; KIO; KOB; KUL; LIM; LIS; LON; LOS; LUS; MAD; MAP; MEX; MIN; MOS; MSK; NAE; NAI; NDE; NIC; NUR; NYC; OEC; OSL; OTT; PAR; PEK; PET; PIE; PRA; PRE; PRI; RAB; RAM; REY; RIA; RII; ROO; SAO; SEO; SIN; SNG; SNT; SOF; TAL; TEH; TEL; TOK; TUK; TUN; VAR; WAS; WIE; VIL; WIN; YAN; YKE; ZAG

Laatija jakanut