SENAATTI

# Tietoturvallisen työskentelyn pelisäännöt yhteisissä työympäristöissä

11.10.2024

Yhteisten työympäristöjen kiinteistö- ja toimitilaturvallisuuskonsepti

# Sisältö

- Termistö, määritelmät
- Turvallisuuden hallinta valtion työympäristöissä
- Työympäristön suunnittelu- ja toteutusperiaatteita
- Tietoturvallisen työskentelyn periaatteita
- Toimintaperiaatteet -  tietojen turvallinen käsittely käytännössä

# Turvallisuuden hallinta valtion työympäristöissä

- Valtion työympäristöjen turvallisuuden hallinta painottuu tietoturvan ja tietosuojan lisäksi henkilöturvallisuuden, palo- ja pelastusturvallisuuden sekä jatkuvuudenhallinnan ympärille.
- Valtion työympäristöjen turvallisuus varmistetaan rakenteellisten, turvateknisten, hallinnollisten sekä toiminnallisten keinojen yhdistelmällä.

# Säädöspohja

- Tiedonhallintalaissa ja turvallisuusluokitusasetuksessa ei aseteta yksityiskohtaisia vaatimuksia tilojen turvallisuudelle.
  - *”Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.”* (Laki julkisen hallinnon tiedonhallinnasta)
  - *”Tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia.”* (Laki julkisen hallinnon tiedonhallinnasta)
- Tiedonhallintalautakunnan julkaisemat suositukset tarjoavat suosituksia säädettyjen vaatimusten toteuttamista varten.

1. Turvallisuusalueen vähimmäisvaatimusten toteuttaminen
2. Riskien arviointi
3. Turvatoimien valinta (monitasoinen suojaus)
4. Alueen turvatoimien tavoitteiden saavuttaminen

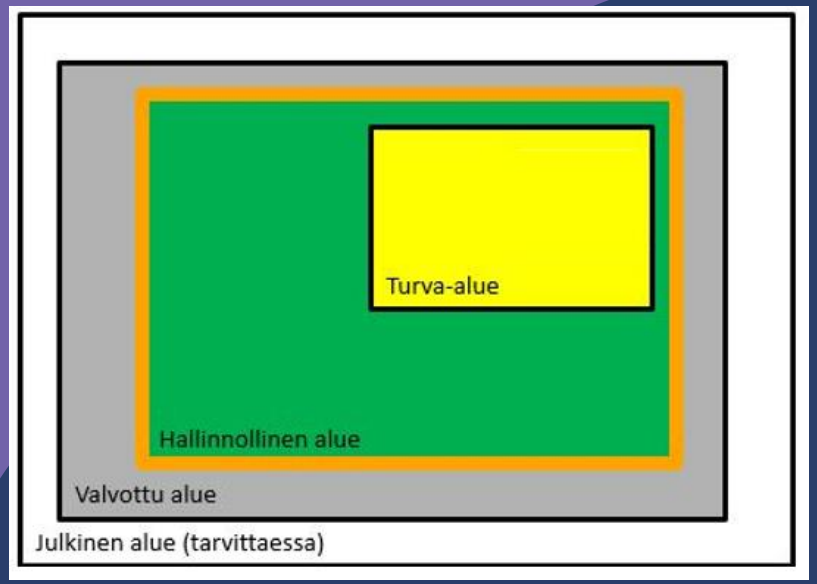
# Suunnittelu- ja toteutusperiaatteita

# Tilojen suunnittelu ja toteutus tietoturvallisuuden näkökulmasta

- Työympäristön ja –välineiden on tuettava tietoturvallista työskentelyä.
- Työympäristöjen suunnittelussa tulee tunnistaa ja arvioida olennaiset riskit, joita tietojen käsittely-ympäristö voi aiheuttaa salassa pidettävien tietojen ja henkilötietojen suojalle.
- Suunnittelussa ja toteutuksessa huomioidaan toiminnan tarpeet:
  - salassa pidettävien sekä henkilötietoja sisältävien aineistojen suojaustarpeet- ja vaatimukset, aineiston käsittelyn laajuus, käsittelytapa- ja muoto, säilytystarve ja mahdolliset erityispiirteet- ja vaatimukset.
- Suunnittelussa määritellään tilavyöhykkeet, fyysisesti suojatut turvallisuusalueet sekä muut tilaturvajärjestelyt tietojen käsittelyn ja tietojärjestelmien suojaamiseksi riskienarvioinnin mukaisesti.

# Tilavyöhykkeet ja turvallisuusalueet - suunnitteluperiaatteet

- Valtion työympäristökonseptin mukaisesti kiinteistön tilat jaetaan käyttötarkoituksen mukaisiin tilavyöhykkeisiin, joita ovat julkinen ja sisäinen tilavyöhyke.
- Turvallisuusalueiden suunnittelu aloitetaan kiinteistön tai toimitilan ulkoalueista.
- Turvallisuuden kannalta kriittisimmät tilat pyritään sijoittamaan kiinteistön sisäosien tiloihin ja mahdollisimman keskelle kiinteistöä.
- Toimitilaturvallisuuden perusperiaatteet on kuvattu dokumentissa *Toimitilaturvallisuuden periaatteet yhteisissä työympäristöissä*



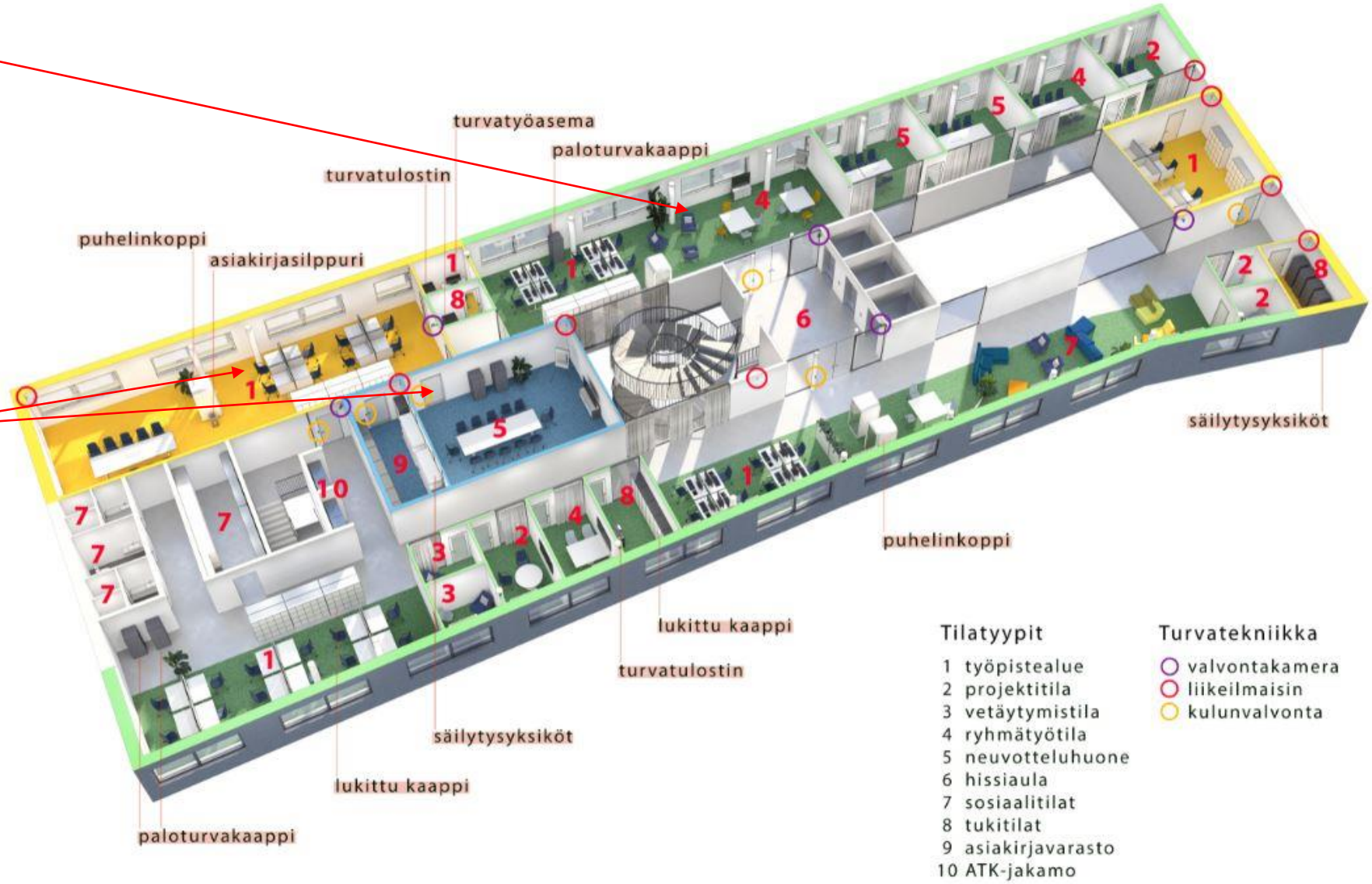

Turvallisuusalueiden välisten kulkureittien tulisi johtaa yhtä luokkaa ylemmälle tai alemmalle turvallisuusalueelle. Aina tämä kuitenkaan ei ole mahdollista ja tietyissä tapauksissa turva-alue voi rajautua esimerkiksi julkiseen alueeseen (huomioitava riskiarviointia):

**Esimerkki: *(julkinen alue) < >valvottu alue < > hallinnollinen alue < > turva-alue.***

# Toimitilan turvallisuusalueet ja käsittelyperiaatteet - esimerkki

**Hallinnollinen alue**
- Käsittely
  - Salassa pidettävä
  - TL IV – II * ja **
- Säilytys
  - Salassa pidettävä ja TL IV soveltuvissa lukituissa toimistokalusteissa.

**Turva-alue**
- Käsittely
  - Salassa pidettävä
  - TL IV – I **
- Säilytys:
  - Salassa pidettävä ja TLIV kuten edellä
  - TL III – I soveltuvaksi arvioidussa säilytysratkaisussa.




Turvallisuusluokiteltuja ja salassa pidettäviä asiakirjoja on käsiteltävä siten, että **pääsy tietoihin suojataan sivullisilta**. Fyysisten turvatoimien valinta tehdään viranomaisen **riskien arvioinnin** perusteella. **Monitasoista suojausperiaatetta** soveltaen määritellään asianmukainen ja riittävä **turvatoimien yhdistelmä** (hallinnolliset, toiminnalliset ja fyysiset keinot).
*Turvallisuusluokan II tai III asiakirjoja sisältävät tietovarannot ja näiden asiakirjojen käsittelyyn käytetyt tietojärjestelmät sijoitettava turva-alueelle
**Tiloihin, joissa käsitellään TL I tai II tietoja, saa tuoda ainoastaan viranomaisen hyväksymiä elektronisia laitteita. Jos tarkastaminen tai hyväksyntä ei mahdollista, tulee em. jättää tilan ulkopuolelle esim. tähän varattuun säilytyslokeroon. Tila tai alue tarkastettava säännöllisesti fyysisesti tai teknisesti luvattomien laitteiden tai yhteyksien havaitsemiseksi

# Työpisteet

- Työpisteen valinta riskiperusteisesti, ympäristö, toiminnan tarpeet ja kokonaisratkaisu huomioiden.
- Työpisteiden sijoittelulla ja valinnalla pyritään estämään suoran näköyhteyden syntyminen ulkopuolisista tiloista työpisteelle, tarvittaessa työpisteet varustetaan näkösuojasermeillä ja/tai näytöt näytönsuojakalvoilla näytönsuojakalvoilla

# Tietoturvallisen työskentelyn periaatteet

# Tietoturvallisen työskentelyn periaatteet

1) **Kulkujärjestelyt ja vieraiden hallinta** *(kulunvalvonta, pääsyoikeudet, julkinen – sisäinen tilavyöhyke)*

2) **Työskentelyalueen ja työpisteen valinta** *(käsiteltävän aineiston suojaustarve huomioiden)*

3) **Tiedon käsittelyn suojaaminen** *(tiedonsaantioikeus,"need to know", sähköinen käsittely, ohjeistus)*

4) **Tyhjän pöydän periaate** *(aineistoa ei jätetä pöydälle, kone lukitaan)*

5) **Tiedon säilyttäminen, tulostus, tuhoaminen** *(suojaustarpeen mukainen säilytys, turvatulostus, tietosuoja-astiat)*

6) **Poikkeamien hallinta** *(proaktiivisuus, ilmoita puutteista ja havainnoista)*

SENAATTI

# Pääsynhallinta

## Kulkujärjestelyt ja vieraidenhallinta

# Pääsynhallinta - kulkujärjestelyt

- Asiaton pääsy tiloihin tulee estää, itsenäinen pääsy vain valtuutetuilla henkilöillä.
- Henkilökunnalle ja palveluntuottajille työtehtävien mukaiset kulkuoikeudet.
- Nimetty vastuullinen, joka huolehtii pääsyoikeuksien, kulkutunnisteiden ja avainten hallinnasta ja ohjeistamisesta.
- Kaikilla kuvallinen henkilökortti näkyvillä tiloissa asioinnin aikana.
- Kaikki huolehtivat osaltaan kulunvalvonnasta, puuttuvat mahdollisiin poikkeamiin ja ilmoittavat niistä.

## Vieraidenhallinnan yleiset periaatteet

- Tapaa vieraat julkisen vyöhykkeen tiloissa
- Vieras tunnistetaan ja kirjataan, vierailijatunniste näkyvillä vierailun ajan
- Vastuuhenkilö huolehtii vieraistaan (ennakoi, ilmoita, saata, valvo ja ohjeista)
- Puutu rohkeasti poikkeamiin

# Toimintaperiaatteet – tietojen käsittely

# Yleiset käsittelyperiaatteet

- **Elinkaariajattelu**
  - Käsittelijän tulee huolehtia, että suojattavan tiedon turvallisuus ja suojaustoimet varmistetaan koko käsittelyketjun ajan.
- **Puhtaan pöydän – periaate**
  - Suojattavien tietojen (asiakirjat, myös päätelaitteet) tulee olla riittävällä tavalla käsittelijän henkilökohtaisessa valvonnassa, huomioitava erityisesti yhteisissä työympäristöissä.
  - Yhteisessä työympäristössä suositaan salassa pidettävän tietoaineiston käsittelyä sähköisenä, vältetään paperiaineiston turhaa käsittelyä ja säilyttämistä.

# Yleiset periaatteet

- **Need-to-know -periaate**
  - Salassa pidettäviä tietoja tai henkilötietoja käsittelevän velvollisuus suojata aineiston päätymistä sivullisille. Sivullinen on henkilö jolla ei ole tiedonsaantitarvetta- tai oikeutta käsiteltävään tietoaineistoon, työympäristöratkaisu ei muuta tätä huolehtimisvelvollisuutta.
    - Tiedon käsittelyn näkökulmasta sivullinen voi olla esimerkiksi oman organisaation henkilö, toisen organisaation henkilö tai täysin ulkopuolinen henkilö
  - Jokaisen tulee huomioida, että yhteisessä työympäristössä voi olla samaan aikaan henkilöitä joilla ei ole tiedonsaantitarvetta- tai oikeutta aineistoon jota olet käsittelemässä.
  - Jokaisella on järjestetty oikeudet ja pääsy vain sellaiseen aineistoon johon henkilöllä on käsittelytarve tai/ja erikseen myönnetty käsittelyoikeus (korostuu TL-aineistojen osalta).

# Yleiset periaatteet

- **Yhteiset pelisäännöt / ohjeistus**
  - *Asiakirjan käsittelijän* vastuulla on huolehtia riittävistä tietoturvallisuustoimista, varmistamalla etteivät sivulliset saa tarpeettomasti tietoonsa tai haltuunsa suojattavaa aineistoa joka ei ole heille tarkoitettua, vahingossa / tahattomasti tapahtuvat tilanteet mukaan lukien.
  - *Jokainen* huolehtii siitä, ettei toiminnallaan vaaranna tiloissa käsiteltävien tietojen turvallisuutta. Jokaisen tulee huolehtia, ettei tarkoituksellisesti pyri saamaan tietoonsa suojattavaa aineistoa johon hänellä ei ole tarvetta tai oikeutta käsittelyyn.
  - Yhteiset käsittelysäännöt ja ohjeet koskevat jokaista. Jokainen sitoutuu noudattamaan ohjeita ja on velvollinen puuttumaan poikkeamiin sekä ilmoittamaan niistä.

# Yleiset periaatteet

- **Salassapitovelvollisuus koskee kaikkia**
  - Julkisuuslaki säätelee viranomaisen salassa pidettävien asiakirjojen vaitiolovelvollisuudesta ja hyväksikäyttökiellosta
  - Virkamieslaki säätelee virkasuhteisten virkavelvollisuuksista sis. korostetun salassapitovelvollisuuden
  - Turvallisuussopimukset ja vaitiolositoumukset sitovat palveluntuottajia
  - Rikoslaki määrittää salassapitovelvollisuuden rikkomiseen liittyvistä rikosoikeudellisista seurauksista

# Miten suojaan salassa pidettävää tietoa?

# YLEISIMMÄT RISKITILANTEET - KÄYTÄNNÖSSÄ

# TIETOAINEISTON SUOJAAMINEN – KÄYTÄNNÖSSÄ

1. **Huomioi jo työpisteen valinnassa** aineiston suojaamisen edellytykset

2. **Käy luottamukselliset keskustelut, puhelut ja palaverit** (tarvittaessa) vetäytymistilassa, neuvotteluhuoneessa tai puhelinkopissa

3. **Käytä** kannettavalla tietokoneella ja ulkoisilla näytöillä **näytönsuojaa.**

4. **Noudata puhtaan pöydän -periaatetta**
Aineistoa ei voi jättää työpisteille **valvomatta** lyhyt-aikaisestikaan

5. **Lukitse työasema** aina poistuessasi työpisteeltä:
⊞ - painike + L
Valttikoneilla→ kortti ulos

6. **Laita** asiakirjat / päätelaite **poistuessasi lukittuun kappiin** tai kanna ne mukana

7. **Vältä tarpeetonta tulostamista, jos pakko niin käytä** suojattavan aineiston tulostamisessa vain **turvatulostusta tai oheistulostimia.**

8. **Tuhoa tarpeettomat** luottamukselliset paperiasiakirjat laittamalla ne **tietosuoja-astiaan** tai käyttämällä silppuria

# Työpisteen valinta

SENAATTI

# Työpisteen valinta – käytännön toimenpiteitä ja ohjeistus

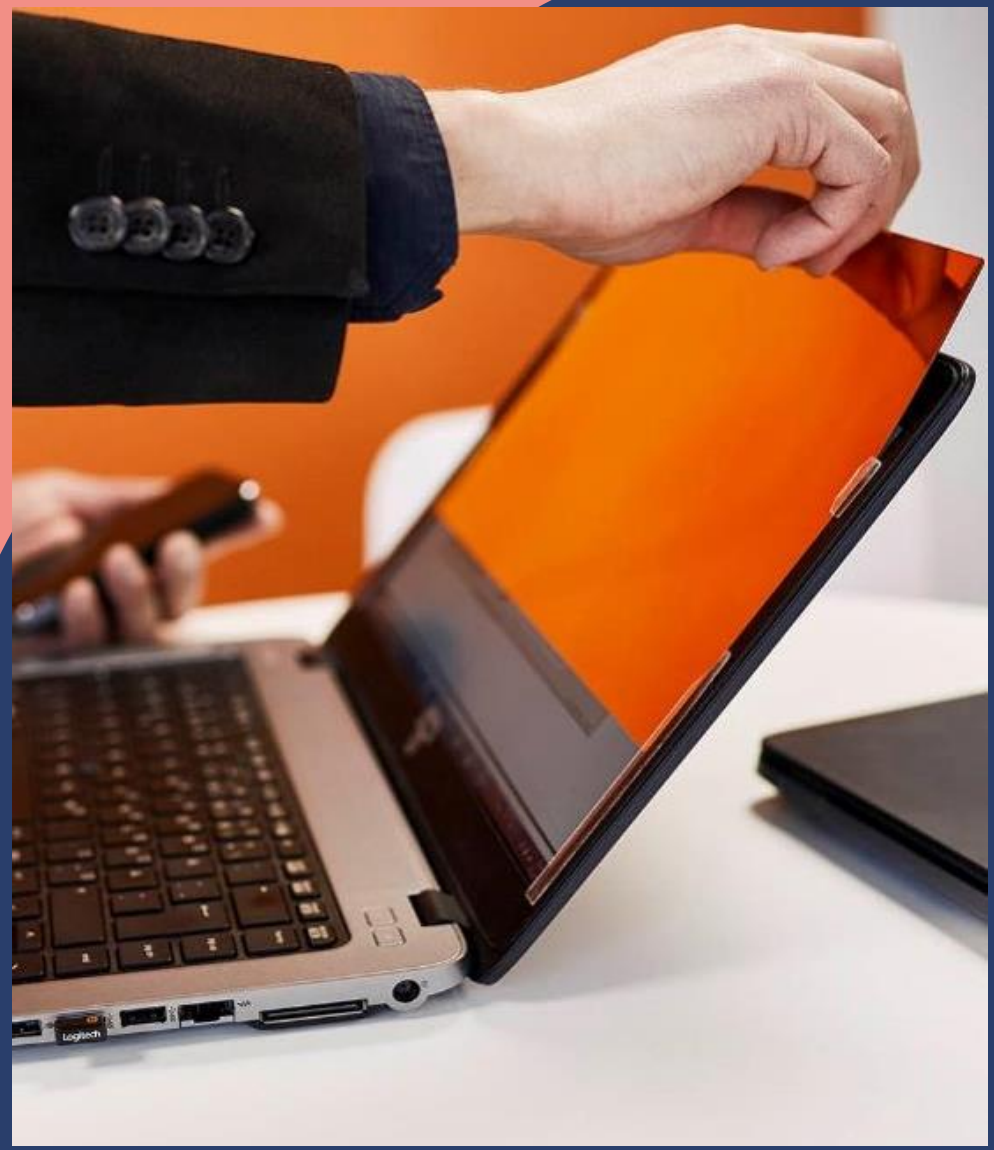
- Käsittelijä valitsee tilan ja työpisteen kulloiseen käsittelytilanteeseen sopivaksi (paperiaineisto, sähköinen, keskustelu) huomioiden riittävällä tavalla, että salassa pidettävän aineiston luottamuksellisuus ei vaarannu. Käsittelijä tekee riskiperusteisen arvioinnin ja valinnan.
- Mikäli tilassa on samaan aikaan muita henkilöitä joilla ei ole tiedonsaantioikeutta käsiteltävään tietoon ja kokonaisuus arvioiden käsittelytilanteen turvaaminen vaatii käytännön toimenpiteitä, käsittelijä voi esim.
  - valita käsittelyn ajaksi vetäytymistilan, puhelinkopin, kokoustilan tai
  - työpisteen jossa on valmiina näkösuojan tarjoava sermi tai
  - työpisteen jolla on syrjäinen sijainti, eikä esim. selän takana ole toista työpistettä ja henkilöä
  - keskeyttää salassa pidettävän tietoaineiston käsittelyn esim. kollegan kanssa käytävän keskustelun tai tilassa tapahtuvan huolto- tai siivoustoimenpiteiden ajaksi

# Näkösuoja

SENAATTI

# Näkösuoja – käytännön toimenpiteitä ja ohjeistus

- Käsitellään siten, että alueella olevat sivulliset eivät näe hallitsemattomasti ja selkokielisesti suojattavaa tietoa tai pääse perehtymään niihin.
- Ikkuna- ja tai lasipinnat voidaan tarvittaessa suojata (sälekaihtimet, verhot, maitokalvot)
- Näytön voi suunnata siten, ettei ulkopuoliset näe käsiteltävää aineistoa. Ulkoisiin näyttöihin on tiettyyn kokoluokkaan asti saatavissa myös kalvoja.
- Käytännön toimenpiteitä:
  - Käytetään tarvittaessa näytön suojaa (erillistä tietoturvakalvoa tai koneeseen integroitua turvakalvoa.)
  - Näyttöpäätteen voi suojata tilapäisesti sammuttamalla sen.
  - Paperiasiakirjan voi suojata tilapäisesti esim. kääntämällä sen ympäri, peittämällä sen tai sijoittamalla asiakirjamappiin, laukkuun tai kirjekuoreen.



# Luottamukselliset keskustelut

SENAATTI

# Luottamukselliset keskustelut – käytännön toimenpiteitä ja ohjeistus

- Tiloissa on huomioituna riittävä äänieritys (normaali puheääni ei vuoda ympäröiviin tiloihin)
- Käsittelijän on kuitenkin aina huolehdittava myös itse tarvittavasta suojauksesta käsittelyn aikana.
- Käsittelyssä huomioidaan, ettei keskustelusta syntyvä puheääni vuoda
  - tilojen ulkopuolelle tai käytettävän tilan sisällä sivullisille
  - huomioitava että samoissa tiloissa voi olla samaan aikaan henkilöitä joilla ei tarvetta/oikeutta käsiteltävään tietoon
- Luottamukselliset keskustelut (palaverit, puhelut, neuvottelut) hoidetaan tarvittaessa näihin varatuissa vetäytymistiloissa, puhelinkopeissa, neuvottelutiloissa tai projektityötiloissa.
  - Tilan ovet suljetaan tarvittaessa käsittelyn ajaksi tai äänenvoimakkuus huomioidaan riittävällä tavalla.
  - Huomioidaan että ääni voi vuotaa myös avoimen ikkunan kautta, ikkunat suljetaan käsittelyn ajaksi.
  - Videoneuvottelulaitteiden äänenvoimakkuus voi ylittää ”normaalin ääneneristävyysrajan”.

# Puhtaan pöydän periaate

SENAATTI

# Puhtaan pöydän periaate – käytännön toimenpiteitä ja ohjeistus

- Salassa pidettäviä tietoja sisältäviä asiakirjoja kuten papereita, mappeja, sähköisiä muistivälineitä ei jätetä työpistealueille vapaasti ja valvomatta, esim. työpisteen, neuvotteluhuoneen tai vetäytymistilan pöydälle poistuessa ruokatauolle.
- Työpaikalla, päivän aikana asiakirjat säilytetään niihin varatuissa lukituissa kaapeissa tai kannetaan mukana. Päivän päätteeksi asiakirjat laitetaan lukittuihin kaappeihin.
- Työasema lukitaan aina kun poistutaan työpisteeltä, lyhytaikaisestikin.
- Mobiilityössä tulee noudattaa työnantajan käsittelyohjeita.

# Tietoaineiston, säilytys, tulostaminen ja tulostaminen

SENAATTI

# Tietoaineiston säilytys, tulostus ja tuhoaminen – käytännön toimenpiteitä ja ohjeistus

- Tulostus:
  - Vältä ylimääräistä tulostamista, kysy itseltäsi onko tulostaminen välttämätöntä!
  - Salassa pidettävien asiakirjojen tai henkilötietojen tulostamisessa käytetään aina turvatulostusta, jolla vältetään asiakirjan unohtuminen monitoimilaitteelle sekä ”ristiintulostus”.
- Säilytys:
  - Kannettavat työasemat ja asiakirjat sisäisellä työpistealueella lukitussa lokerossa, kaapissa, asiakirjavarastossa tai vaihtoehtoisesti kannetaan mukana.
  - Salassa pidettävä ja korkeintaan TLIV aineisto hallinnollisella alueella lukitussa kaapissa. TL III-II asiakirjat turva-alueella kassakaapissa.
- Tuhoaminen:
  - Paperiaineisto ja sähköiset muistivälineet (muistitikut ja CD-levyt jne.) tuhotaan laittamalla ne käyttöön tarkoitettuihin tietosuoja-astioihin. Astiat tulee merkitä selvästi käyttötarkoituksen mukaisesti, esim. ”vain julkinen tieto”, ”vain salassa pidettävä tieto”. TL- tiedon tuhoaminen organisaation ohjeiden ja turvatason mukaisesti, esim. erillinen asiakirjasilppuri.


SENAATTI