VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Rekommendation om behandling av sekretessbelagda handlingar

Nämnder

Finansministeriets publikationer – 2023:19

Finansministeriets publikationer 2023:19

Rekommendation om behandling av sekretessbelagda handlingar

Finansministeriet Helsingfors 2023

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

Finansministeriet

ISBN pdf: 978-952-367-094-5
ISSN pdf: 1797-9714

Layout: Statsrådets förvaltningsenhet, publikationsverksamheten

Helsingfors 2023

Presentationsblad
24.3.2023

Rekommendation om behandling av sekretessbelagda handlingar

Finansministeriets publikationer 2023:19		**Tema**	Nämnder
Utgivare	Finansministeriet		
Utarbetad av	Informationshanteringsnämnden		
Språk	svenska	**Sidantal**	52

Referat

I lagen om informationshantering inom den offentliga förvaltningen (906/2019) finns bestämmelser om ansvar i fråga om informationssäkerhetsåtgärder som gäller informationshanteringsenheter och myndigheter inom den offentliga förvaltningen samt privatpersoner, privaträttsliga sammanslutningar och sådana offentligrättsliga samfund som inte är myndigheter till den del dessa sköter offentliga förvaltningsuppgifter.

Denna rekommendation av informationshanteringsnämnden redogör för behandlingen av sekretessbelagda handlingar (uppgifter) och uppfyllandet av de krav som gäller behandlingen. Publikationen innehåller de krav som ställs i lagstiftningen, rekommendationer och praktiska exempel som gäller behandlingen av sekretessbelagda handlingar. Bilaga 1 är en sammanställning av rekommendationerna och den rättsliga grund som hänför sig till dem.

Informationshanteringsnämndens tidigare rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet (FM 2021:72) fastställer de minimikrav på informationssäkerhet som ska iakttas inom den offentliga förvaltningen. Det rekommenderas att dessa minimikrav också ska tillämpas på behandlingen av sekretessbelagda handlingar.

Rekommendationen är i första hand avsedd för myndigheter, men utöver dem kan även aktörer inom näringslivet och andra som behandlar handlingar som myndigheterna klassat som sekretessbelagda ha nytta av rekommendationen.

Informationshanteringsnämnden godkände rekommendationen den 15 december 2022.

Nyckelord	informationssäkerhet, nämnder, datasekretess, informationshanteringsnämnden, beredskap, lokaler, informationshanteringslagen, offentlig förvaltning, sekretessbelagda handlingar, sekretessbelagda uppgifter		
ISBN PDF	978-952-367-094-5	**ISSN PDF**	1797-9714
URN-adress	https://urn.fi/URN:ISBN:978-952-367-094-5		

Kuvailulehti
24.3.2023

Suositus salassa pidettävien asiakirjojen käsittelystä

Valtiovarainministeriön julkaisuja 2023:19		**Teema**	Lautakunnat
Julkaisija	Valtiovarainministeriö		
Yhteisötekijä	Tiedonhallintalautakunta		
Kieli	ruotsi	**Sivumäärä**	52

Tiivistelmä

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019) on säädetty tietoturvallisuustoimenpiteisiin liittyviä vastuita julkisen hallinnon tiedonhallintayksiköille ja viranomaisille sekä yksityisille henkilöille ja yhteisöille taikka muille kuin viranomaisena toimiville julkisoikeudellisille yhteisöille, siltä osin kuin ne hoitavat julkista hallintotehtävää.

Tässä tiedonhallintolautakunnan antamassa suosituksessa kuvataan salassa pidettävien asiakirjojen (tietojen) käsittelyssä sekä käsittelyä koskevien vaatimusten täyttämisessä. Suositus sisältää lainsäädännön vaatimuksia, suosituksia sekä käytännön esimerkkejä salassa pidettävien asiakirjojen käsittelystä. Liitteeseen 1 on koostettu dokumentissa olevat suositukset ja niihin liittyvät lakiperusteet.

Aikaisemmin julkaistu tiedonhallintalautakunnan suosituskokoelma tiettyjen turvallisuussääntöjen soveltamisesta (VM 2021:65) sisältää julkisessa hallinnossa noudatettavat tietoturvallisuuden vähimmäisvaatimukset. Näitä vähimmäisvaatimuksia suositellaan sovellettavaksi myös salassa pidettävien asiakirjojen käsittelyssä.

Suositus on tarkoitettu ensisijaisesti viranomaisille, mutta niiden lisäksi suositusta voivat hyödyntää elinkeinoelämän toimijat ja kaikki muutkin, jotka käsittelevät viranomaisten salassa pidettäväksi määrittelemiä asiakirjoja.

Tiedonhallintalautakunta hyväksyi suosituksen 15.12.2022.

Asiasanat	tietoturva, lautakunnat, tietosuoja, tiedonhallintalautakunta, varautuminen, toimitilat, tiedonhallintalaki, julkinen hallinto, salassa pidettävä asiakirja, salassa pidettävä tieto		
ISBN PDF	978-952-367-094-5	**ISSN PDF**	1797-9714
Julkaisun osoite	https://urn.fi/URN:ISBN:978-952-367-094-5		

Description sheet
24 March 2023

Recommendation for the processing of non-disclosable documents

Publications of the Ministry of Finance 2023:19		**Subject**	Board
Publisher	Ministry of Finance		
Group author	Information Management Board		
Language	Swedish	**Pages**	52

Abstract

The Act on Information Management in Public Administration (906/2019) lays down obligations relating to information security measures that apply to information management units and authorities as well as to private individuals or corporations or to corporations subject to public law other than those serving as authorities insofar as they perform public administrative tasks.

This recommendation issued by the Information Management Board describes the recommendations and practices to be applied when processing non-disclosable documents (data) and fulfilling the requirements for processing. The recommendation includes legislative requirements, recommendations and practical examples of the processing of non-disclosable documents. The recommendation in the documents and the related legal grounds have been compiled in Appendix 1.

The previously published Collection of recommendations on the application of certain security regulations (VM 2021:65) includes the minimum data security requirements to be complied with in public administration. These minimum requirements are also recommended to be applied to the processing of non-disclosable documents.

The recommendation is primarily intended for authorities, but can also be used by business and industry and any other parties that process documents that have been classified as non-disclosable by the authorities.

The Information Management Board approved the recommendation on 15 December 2022

Keywords data security, board, data privacy, Information Management Board, precautionary measures, business premises, Act on Information Management in Public Administration, public administration, non-disclosable document, non-disclosable information

ISBN PDF	978-952-367-094-5	**ISSN PDF**	1797-9714
URN address	https://urn.fi/URN:ISBN:978-952-367-094-5		

Innehåll

1 Inledning

Denna rekommendation om behandling av sekretessbelagda handlingar har utarbetats av den offentliga förvaltningens informationshanteringsnämnd, nedan *informationshanteringsnämnden*, i syfte att hjälpa och instruera informationshanteringsenheter och myndigheter i uppfyllandet av de krav som ställs på behandlingen av sekretessbelagda handlingar (information/uppgifter). Rekommendationen behandlar utöver de krav som lagstiftningen ställer på behandlingen av information även goda förfaranden som myndigheterna kan använda när de vidtar åtgärder som gäller behandling av information och utarbetar anvisningar om behandlingen.

I 22 § 1 mom. i lagen om offentlighet i myndigheternas verksamhet (621/1999), nedan *offentlighetslagen* eller *OffL*, föreskrivs följande: ”En myndighetshandling skall sekretessbeläggas, om det i denna lag eller någon annan lag föreskrivs eller en myndighet med stöd av lag har föreskrivit att den skall vara sekretessbelagd eller om handlingen innehåller uppgifter för vilka tystnadsplikt föreskrivs genom lag”.

Med sekretessbelagd avses enligt 22 § 2 mom. i offentlighetslagen att en myndighetshandling eller en kopia eller utskrift av en sådan handling inte får företes för eller lämnas ut till utomstående eller med hjälp av en teknisk anslutning eller på något annat sätt företes för eller lämnas ut till utomstående. Syftet är att skydda sekretessbelagd information oavsett var eller hur den visas. I 23 § offentlighetslagen föreskrivs om tystnadsplikt och förbud mot utnyttjande av sekretessbelagd information.

Denna rekommendation är i första hand avsedd för myndigheter, men även aktörer inom näringslivet och andra som hanterar handlingar som myndigheter har sekretessbelagt kan ha nytta av den. Nedan används termen *organisation* om dessa aktörer som är föremål för bestämmelser om informationssäkerhet.

Utöver rekommendationen behövs det i organisationerna fortfarande egna anvisningar om behandlingen samt utbildning för både ansvariga personer och hela personalen. För detta ska det enligt 4 § 2 mom. 2 punkten i lagen om informationshantering inom den offentliga förvaltningen (906/2019), nedan *informationshanteringslagen* eller *InfL*, användas eget preciserande material om de praktiska åtgärderna i samband med behandling av sekretessbelagd information.

Rekommendationen har utarbetats i den informationssäkerhetssektion som tillsattes av informationshanteringsnämnden för 1 januari–31 december 2022. Rådgivande tjänsteman Mika Kuronen från finansministeriet var ordförande för sektionen och ledande expert Tuula Seppo från Myndigheten för digitalisering och befolkningsdata var sekreterare. Informationshanteringsnämnden utnämnde experter från olika informationshanteringsenheter till medlemmar i sektionen. Dessutom hörde sektionen även många olika experter utanför sektionen på sina möten, verkstäder och seminarier. Utkastet till rekommendation kunde kommenteras i den offentliga utlåtandetjänsten 30 augusti–21 september 2022.

1.1 Grunder i lagstiftningen

I 10 § i informationshanteringslagen föreskrivs om den uppgift som informationshanteringsnämnden för den offentliga förvaltningen har när det gäller att främja de i denna lag föreskrivna förfarandena i fråga om informationshantering och informationssäkerhet samt genomförandet av lagens krav. För att genomföra denna uppgift utarbetar och upprätthåller informationshanteringsnämnden rekommendationer vars syfte är att vägleda informationshanteringsenheter och myndigheter i uppfyllandet av kraven i informationshanteringslagen baserat på goda förfaranden.

I 4 § 2 mom. i informationshanteringslagen föreskrivs att en informationshanteringsenhets ledning ska ombesörja att den har uppdaterade anvisningar om hantering av informationsmaterial, om användning av informationssystem, om databehandlingsrättigheter, om informationshanteringsansvar, om informationsrättigheter, om informationssäkerhetsåtgärder samt om beredskap för undantagsförhållanden. Enligt detta moment har ledningen också ansvar för att det kan erbjudas utbildning varmed det säkerställs att de anställda och personer som arbetar för informationshanteringsenhetens räkning är tillräckligt förtrogna med gällande författningar, föreskrifter och med informationshanteringsenhetens anvisningar om informationshantering och databehandling samt om offentlighet och sekretess i fråga om handlingar. Anvisningarna om behandling av sekretessbelagd information är i hög grad kopplade till fullgörandet av det ansvar som informationshanteringslagen ålägger ledningen vid informationshanteringsenheter.

Kraven som gäller behandling av sekretessbelagd information är ett viktigt bedömningsobjekt när informationshanteringsenheten i enlighet med 13 § 1 mom. i informationshanteringslagen identifierar relevanta risker förenade med informationsbehandling och dimensionerar informationssäkerhetsåtgärderna utifrån riskbedömningen. På grundval av riskbedömningen kan informationshanteringsenheterna och de myndigheter som är verksamma inom dessa genom adekvata säkerhetsåtgärder i fråga om sina informationsmaterial trygga säkerheten för informationsmaterial som innehåller sekretessbelagd information (informationshanteringslagen 15 §) och de användarrättigheter för

informationssystemen som krävs för behandling av information (informationshanteringslagen 16 §). Dessutom finns det i 14 § i informationshanteringslagen krav på överföring av sekretessbelagd information i det allmänna datanätet.

Vid behandling av sekretessbelagd information ska informationshanteringsenheter och myndigheter utöver informationshanteringslagen även tillämpa bland annat offentlighetslagen. Av denna anledning behandlar rekommendationen även kraven i offentlighetslagen i samband med och vid sidan av kraven i informationshanteringslagen. Syftet med detta är att de som använder rekommendationen ska få tillräckligt med information om den allmänna lagstiftning som har väsentlig inverkan på behandlingen av information.

I 18 § i informationshanteringslagen och i statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019), nedan *säkerhetsklassificeringsförordningen* eller *SKF*, som kompletterar informationshanteringslagen, finns bestämmelser om säkerhetsklassificering, klassificeringsanteckningar och behandling av säkerhetsklassificerade handlingar.

En organisations sekretessbelagda information kan innehålla personuppgifter, och då måste man också beakta kraven på behandling av personuppgifter. Den allmänna lagstiftningen om behandling av personuppgifter består av EU:s allmänna dataskyddsförordning ((EU) 2016/679), nedan *dataskyddsförordningen,* och dataskyddslagen (1050/2018). Om behandling av personuppgifter i brottmål och i samband med upprätthållande av den nationella säkerheten finns bestämmelser i lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018). Närmare anvisningar om behandling av personuppgifter ges av Dataombudsmannens byrå.

1.2 Förhållande till andra rekommendationer

Denna rekommendation och andra rekommendationer från informationshanteringsnämnden bildar tillsammans en helhet som kan användas för att planera de åtgärder som behandling av sekretessbelagd information kräver, bland annat när det gäller skydd av information. Strävan vid utarbetande av rekommendationen var att undvika överlappning med andra rekommendationer. Bilaga 1 innehåller en sammanfattning av rekommendationerna i detta dokument och av deras rättsliga grund. I tabellen nedan listas rekommendationer som informationshanteringsnämnden tagit fram och som man gärna ska sätta sig in i.

Taulukko 1. **Tabell 1.** Rekommendationer av informationshanteringsnämnden som kan rekommenderas.

Publikation	Innehåll
Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet (2021:72)	Rekommendationen innehåller minimikrav på informationssäkerhet som ska uppfyllas inom den offentliga förvaltningen samt detaljerade rekommendationer om tillämpningen av informationshanteringslagens paragrafer om informationssäkerhet. Utgångspunkten är att dessa rekommendationer ska tillämpas även vid behandling av sekretessbelagd information.
Rekommendation om behandling av säkerhetsklassificerade handlingar (2021:10) och Hantering av säkerhetsklassificerade handlingar i molntjänster (2022:6)	Dessa publikationer innehåller rekommendationer om behandling av säkerhetsklassificerade handlingar, och det rekommenderas att dessa tillämpas riskbaserat och utifrån en situationsbedömning även vid hantering av sekretessbelagd information.
Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen, Julkri (2022:65)	Kriterierna stöder organisationerna vid planering, genomförande och bedömning av informationssäkerheten och skyddet av personuppgifter. De kan användas vid bedömning av lagenlighet och som en del av ansvarsskyldigheten enligt dataskyddsförordningen.
Rekommendation om metadata för ärendehantering (2021:43) och Rekommendation om metadata för myndigheternas handlingar i samband med tjänsteproduktion (2022:70)	Publikationerna innehåller rekommendationer om registrering och rekommenderade metadata vid ärendehantering och tjänsteproduktion.
Rekommendation om tekniska gränssnitt och elektroniska förbindelser (2021:38)	Rekommendationen innehåller preciseringar av de sätt att överföra information elektroniskt som det föreskrivs om i informationshanteringslagen.
Rekommendation för en informationshanteringsmodell (2020:41)	Rekommendationen innehåller anvisningar och goda förfaranden för framtagning av en informationshanteringsmodell som definierar och beskriver informationshanteringen i informationshanteringsenhetens verksamhetsmiljö.
Rekommendation om bedömning av förändringar i informationshanteringen (2020:65)	Rekommendationen innehåller anvisningar och goda förfaranden för den bedömning av konsekvenserna av förändringar som föreskrivs i 5 § 3 mom. i informationshanteringslagen, bland annat i förhållande till informationssäkerhetskraven och informationssäkerhetsåtgärderna enligt 4 kap.

1.3 Avgränsningar

Denna rekommendation gäller tillämpningen av informationshanteringslagen på behandling av sekretessbelagd information. I rekommendationen beaktas inte:

- kraven på behandling av säkerhetsklassificerade uppgifter,
- branschspecifik lagstiftning, till exempel social- och hälsovårdslagstiftningens krav i fråga om sekretessbelagd information,
- bestämmelserna om behandling av personuppgifter,
- de krav som grundar sig på internationella förpliktelser i fråga om informationssäkerhet och som inte särskilt beaktas i lagen om tjänster inom elektronisk kommunikation (917/2014), som föreskriver om bland annat sekretessbeläggning och behandling av information i samband med elektronisk kommunikation.

Även om denna rekommendation inte innehåller de ovan nämnda kraven ska organisationen identifiera och beakta dessa krav i sin verksamhet och sina anvisningar.

2 Grunder för behandling av sekretessbelagda handlingar

2.1 Sekretessbelagda myndighetshandlingar

Organisationen ska identifiera när den behandlar sekretessbelagd information.

Information hos myndigheter delas i regel in i offentlig och sekretessbelagd information. Om det är frågan om personuppgifter ska man beakta även den lagstiftning och de anvisningar som gäller behandling av personuppgifter. Sekretessbelagd information kan också vara säkerhetsklassificerad[1] information, som är indelad i olika säkerhetsklasser. När det gäller utlämnande av uppgifter ska man beakta att en del av de uppgifter som inte är sekretessbelagda kan vara uppgifter som kan uppges enligt prövning[2].

I 22 §[3] i offentlighetslagen föreskrivs om handlingssekretess. 24 § 1 mom. i offentlighetslagen innehåller 32 punkter som anger vilka myndighetshandlingar som är sekretessbelagda. Bland annat följande:

> 17) handlingar som innehåller uppgifter om statens, välfärdsområdets, kommuners eller något annat offentligt samfunds eller i 4 § 2 mom. (offentlighetslagen) avsedda sammanslutningars, inrättningars eller stiftelsers företagshemligheter,
>
> 20) handlingar som innehåller uppgifter om en privat företagshemlighet samt sådana handlingar som innehåller uppgifter om någon annan motsvarande omständighet som har samband med privat näringsverksamhet,

1 InfL 18 § ”Handlingar som ska säkerhetsklassificeras inom statsförvaltningen” och säkerhetsklassificeringsförordningen 3 § ”Säkerhetsklassificering och märkning av säkerhetsklass”.

2 OffL 16 a § ”Anteckningar som ska göras i andra än sekretessbelagda handlingar”, 9 § ”Rätt att ta del av en offentlig handling” och 17 § ”Beaktande av rätten till information vid beslutsfattande”.

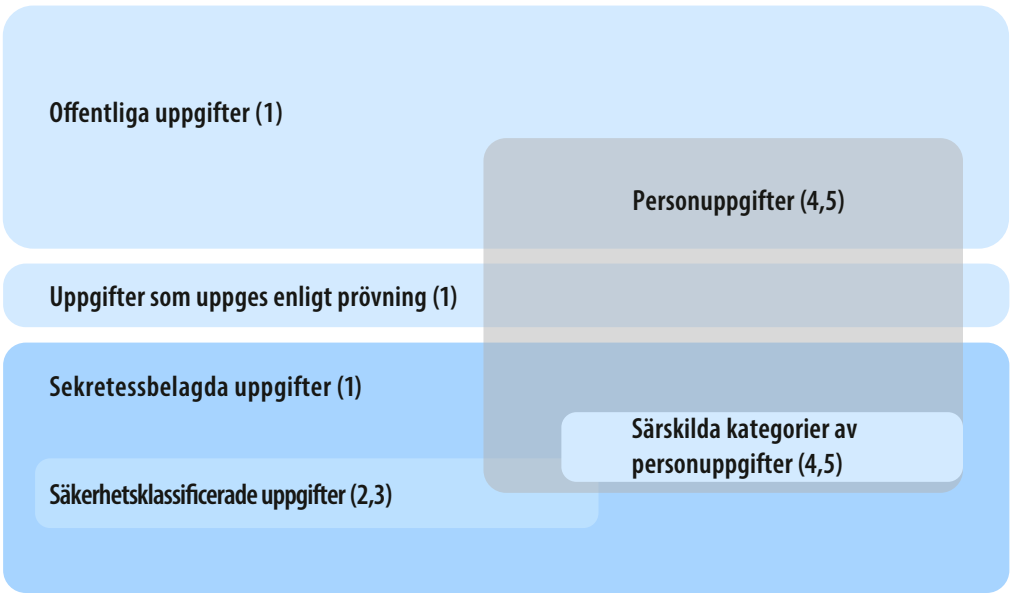
3 OffL 22 § ”Handlingssekretess”.

25) handlingar som innehåller uppgifter om en klient hos socialvården eller en enskild kund hos arbetsförvaltningen samt de förmåner eller stödåtgärder eller den socialvårdsservice eller den service för arbetsförvaltningens enskilda kunder denne erhållit eller uppgifter om en persons hälsotillstånd eller handikapp, den hälsovård eller rehabilitering som denne har erhållit eller uppgifter om någons sexuella beteende eller inriktning.

Det har föreskrivits om sekretess även i annan lagstiftning, men dessa grunder för sekretess har inte särskilt beaktats i denna rekommendation.

Den riktgivande figuren nedan klargör förhållandet mellan offentliga, sekretessbelagda och säkerhetsklassificerade uppgifter samt personuppgifter och uppgifter som hör till särskilda kategorier av personuppgifter. De uppgifter som uppges enligt prövning har placerats mellan de offentliga och sekretessbelagda uppgifterna. Dessa uppgifter behandlas närmare i kapitel 2.8.

Figur 1. Olika uppgifters förhållande till varandra



1) Offentlighetslagen 621/1999
2) Informationshanteringslagen 906/2019
3) Säkerhetsklassificeringsförordningen 1101/2019
4) EU:s allmänna dataskyddsförordning (EU) 2016/679
5) Dataskyddslagen 1050/2018

Personuppgifter är inte sekretessbelagda såvida det inte i en lag eller förordning särskilt föreskrivs att de ska sekretessbeläggas. Det bör dock beaktas att det i dataskyddslagstiftningen finns ytterligare krav i fråga om skydd av personuppgifter. En del av de uppgifter som hör till särskilda kategorier av personuppgifter ska enligt 24 § 1 mom. i offentlighetslagen sekretessbeläggas.

Organisationen ska identifiera vilka uppgifter den behandlar och vilka författningar som gäller dessa uppgifter. Om man identifierar och klassificerar uppgifter blir det lättare att prioritera investeringar som gäller informationssäkerhet. Jämfört med offentliga uppgifter kräver sekretessbelagda uppgifter ytterligare skyddsåtgärder.

2.2 Minimikrav och riskbaserad komplettering av dem

Organisationen ska uppfylla vissa minimikrav som grundar sig på lagstiftningen om behandling av sekretessbelagd information. Dessutom rekommenderas att organisationen kompletterar minimikraven genom att riskbaserat tillämpa informationssäkerhetskrav på en högre nivå än miniminivån.

Informationshanteringslagen innehåller inte särskilt detaljerade krav på informationssäkerhetsåtgärder för sekretessbelagd information. Med stöd av 13 § 1 mom. i informationshanteringslagen, som föreskriver att ”Informationshanteringsenheten ska identifiera relevanta risker som är förenade med informationsbehandlingen och dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen”, kan de nödvändiga åtgärderna i många fall fastställas utifrån en fallspecifik riskbedömning. Till exempel mängden sekretessbelagda uppgifter och följderna av ett obehörigt avslöjande påverkar valet av åtgärder.

Man bör dock komma ihåg att ingen sekretessbelagd information får hamna i fel händer. All sekretessbelagd information måste skyddas mycket väl.

Rekommendationssamlingen om tillämpningen av vissa bestämmelser om informationssäkerhet (2021:72) innehåller minimikraven på informationssäkerhet som den offentliga förvaltningen måste uppfylla. Det är bra att tillämpa denna rekommendation även vid behandling av sekretessbelagd information. Dessutom rekommenderas att organisationer som behandlar sekretessbelagd information kompletterar informationssäkerhetsåtgärderna för behandling av sekretessbelagd information genom att riskbaserat tillämpa rekommendationerna för informationsbehandling på en högre säkerhetsnivå samt

i nödvändig omfattning åtgärder som beskrivs i informationssäkerhetsstandarder[4]. Resultatet av riskbedömningen påverkar vilka säkerhetsåtgärder som bör väljas för att målen för dem ska uppnås. Om risken bedöms vara liten, till exempel utifrån det skyddade intressets och den eventuella skadans begränsade omfattning och den låga sannolikheten för att skadan uppstår, kan säkerhetsåtgärderna vara lättare än i situationer där det skyddade intresset och den eventuella skadan är betydande och risken för att skadan uppstår är större än liten.

Vid val av informationssäkerhetsåtgärder utifrån risker bör man beakta både de potentiella konsekvenserna av ett obehörigt avslöjande av information och kostnaderna för att minska dem. För att man ska hitta rätt nivå krävs en systematisk riskbedömning.

Med stöd av ovanstående rekommenderas att organisationerna använder en riskbedömningsmetod[5] som är lämplig för bedömning av informationssäkerhetsrisker och tillämpar metoden systematiskt vid planering av hur informationssäkerheten för behandling av sekretessbelagd information ska ombesörjas. Organisationen kan till exempel använda Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen, nedan *Julkri-kriterierna*, på så sätt att man bedömer vilka av informationssäkerhetsåtgärderna för information av säkerhetsklass TL IV som är nödvändiga även för organisationens sekretessbelagda information. I vissa fall, till exempel i samband med ackumulering av information som innehåller mycket sekretessbelagda uppgifter, kan man även överväga att tillämpa åtgärderna i säkerhetsklass TL III.

En kumulativ effekt är ett fenomen som handlar om att en stor mängd information kan öka riskerna och utgöra en viktigare helhet än enstaka uppgifter. För den kumulativa effekten finns ingen allmän definition som är lämplig för alla situationer. En kumulativ effekt kan orsakas av både en stor mängd uppgifter och sammanslagning av informationskällor. Den potentiella kumulativa effekten bör beaktas när information skyddas och eventuellt klassificeras.

4 Exempelvis SFS-ISO/IEC 27002:2022. Tietoturvallisuuden hallintakeinojen menettelyohjeet.

5 Till exempel: SFS-ISO/IEC:27001:2022. Tietoturvallisuuden hallintajärjestelmä, Kapitel 6, eller SFS-ISO 31000:2018 Riskienhallinta och SFS-ISO/IEC:27005:2018 Tietoturvariskien hallinta.

Exempel på en åtgärd som organisationen kan vidta:

- Till exempel i en organisations ärendehanteringsregister och ett välfärdsområdes patientdataregister kan det finnas stora mängder sekretessbelagda uppgifter, varför man vid skydd av dessa utifrån riskerna bör överväga användning av de hanteringsmetoder som används vid skydd av säkerhetsklassificerade uppgifter.

2.3 Informationens livscykel och sekretess

Organisationen ska identifiera de processer och informationssystem som är kopplade till behandlingen av sekretessbelagd information och riskbaserat säkerställa att de är tillräckligt informationssäkra under informationens hela livscykel.

I 13 § 1 mom. i informationshanteringslagen föreskrivs följande: ”En informationshanteringsenhet ska följa upp informationssäkerhetens tillstånd i sin verksamhetsmiljö och säkerställa informationsmaterialens och informationssystemens informationssäkerhet under hela deras livscykel.” Dessutom föreskrivs i 13 § 4 mom. följande: ”Myndigheten ska vid sina upphandlingar säkerställa att de aktuella informationssystemen har lämpliga säkerhetsåtgärder.” I kapitel 8 i informationshanteringsnämndens rekommendation (FM 2021:72) behandlas informationssäkerhet vid upphandling av informationssystem ingående.

Baserat på dessa rekommenderas att organisationerna vidtar följande åtgärder för att säkerställa informationssäkerhet vid behandling av sekretessbelagd information:

- identifiera alla sekretessbelagda uppgifter som de har ansvar för och de personer som behandlar dem samt de informationssystem som används vid behandlingen under informationens hela livscykel,
- definiera informationssäkerhetskraven för de informationssystem och tjänster som används i behandlingen, med hänsyn till de risker som är förknippade med behandlingen av de sekretessbelagda uppgifterna,
- säkerställa att informationssäkerhetskraven för informationssystem och tjänster uppfylls i samband med upphandlingar samt regelbundet under hela systemets livscykel genom att systematiskt tillämpa förfaranden för förändringshantering,

- planera och ge anvisningar för processerna för behandling av sekretessbelagd information så att behandlingen är tillräckligt säker, samt
- genom tillräcklig övervakning säkerställa att de rekommendationer som beskrivs ovan följs och upprätthålla en informationshanteringsmodell för hantering av informationssäkerheten.

För att säkerställa att rekommendationerna ovan följs kan organisationen för informationssäkerheten införa ett lednings- och hanteringssystem av lämplig omfattning.

Exempel på åtgärder som organisationen kan vidta:

- definiera och ge anvisningar om de system som är tillåtna för behandling av sekretessbelagd information,
- fastställa informationssäkerhetskrav som gör systemen tillräckligt säkra för behandling av sekretessbelagd information och se till att kraven hålls uppdaterade,
- behandla och förvara informationsmaterial i verksamhetslokaler som är tillräckligt säkra enligt kraven på tillförlitlighet, integritet och tillgänglighet,
- kontrollera att kraven uppfylls, samt
- använda programvaror vars säkerhet har påvisats genom en inspektion utförd av en extern inspektionsinrättning.

2.4 Anteckningar om sekretess

Organisationerna rekommenderas att planera och genomföra antecknandet om sekretess på ett sådant sätt att alla som behandlar och alla som får sekretessbelagd information är medvetna om sekretesskravet.

Det rekommenderas att man säkerställer konfidentialiteten för sekretessbelagda uppgifter genom att på ett systematiskt sätt ta reda på i vilka situationer och med vilka informationssystem sekretessbelagda uppgifter behandlas och för dessa planera förfaranden

genom vilka det säkerställs att personer som hanterar sekretessbelagda uppgifter i alla situationer informeras om sekretessen.

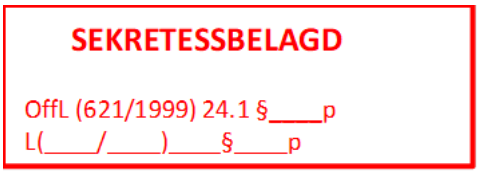
I 25 § 1 mom. i offentlighetslagen föreskrivs följande: ”Anteckning om sekretess skall göras i en myndighetshandling som en myndighet ger ut till en part och som skall vara sekretessbelagd på grund av någon annans eller allmänt intresse. Parten ska informeras om sin sekretessplikt också när sekretessbelagda uppgifter lämnas ut muntligen.”

Enligt den första meningen i 25 § 2 mom. i offentlighetslagen får anteckning göras också i andra handlingar än de som avses i 1 mom., det vill säga en anteckning kan göras även vid andra tillfällen än när myndigheten ger ut en handling till en part.

Den allmänna principen är att den som utarbetat informationen bestämmer vilka uppgifter som ska sekretessbeläggas och gör nödvändiga anteckningar. Av anteckningen ska det framgå till vilka delar informationen är sekretessbelagd och vad sekretessen grundar sig på.

En anteckning om sekretess görs genom att i handlingar på finska anteckna ”SALASSA PIDETTÄVÄ” och på svenska ”SEKRETESSBELAGD”. Någon mer specifik enhetlig rekommendation har inte getts om sekretessanteckningarna, men bilden nedan visar hur en anteckning på en handling kan se ut. Anteckningen kan användas i både manuella och elektroniska handlingar.

Figur 2. Bild som visar hur en anteckning om sekretess kan se ut.



Anteckningen om sekretess kan göras i handlingar till exempel per stycke eller kapitel på så sätt att man framför ett stycke eller kapitel som är offentligt använder förkortningen O och framför ett stycke eller kapitel som är sekretessbelagt förkortningen SEKBEL. Om sekretessen grundar sig på en bestämmelse som innehåller en klausul om skaderekvisit, får anteckningen dock göras så att bara den bestämmelse som sekretessen grundar sig på framgår av anteckningen.

I informationssystem kan uppgiften om sekretess anges med metadata, till exempel med en uppgift om grunden för sekretessen och sekretesstiden.[6] Dessutom bör det noteras att om metadata är synliga för andra än de som har rätt att behandla sekretessbelagd information får metadata inte innehålla sekretessbelagd information. Mer detaljerad information om metadata och registrering finns i informationshanteringsnämndens rekommendationer om metadata vid ärendehantering och i samband med tjänster.[7]

Exempel på åtgärder som kan vidtas för att säkerställa konfidentialitet:

- de som utarbetar sekretessbelagda handlingar ges anvisningar om att anteckningarna om sekretess ska göras genast i samband med att handlingen utarbetas,
- för antecknandet av metadata ges anvisningar om att metadata inte får innehålla sekretessbelagd information eller identifieringsuppgifter om personer,
- de som lämnar ut uppgifter ges anvisningar om att de ska informera om sekretessen, även då uppgifter lämnas ut muntligt,
- informationssystem som innehåller sekretessbelagd information utformas så att de som utarbetar information är tvungna att genast när utarbetandet inleds ta ställning till om informationen ska sekretessbeläggas,
- i informationssystem inkluderas visualiseringar eller varningar som visas för användaren när denne börjar behandla sekretessbelagd information,
- för utskrift och kopiering av sekretessbelagd information på olika sätt ges sådana anvisningar att även den som behandlar en kopia av informationen känner till sekretessen,
- det kontrolleras och bedöms regelbundet om sekretesskraven uppfylls.

6 OffL 25 §

7 Rekommendation om metadata för ärendehantering FM 2021:43 och Rekommendation om metadata för myndigheternas handlingar i samband med tjänsteproduktion FM 2022:70

2.5 Sekretessens giltighet och upphörande

Organisationerna rekommenderas att planera och ge anvisningar om att alla som behandlar eller lämnar ut sekretessbelagda uppgifter ska kontrollera sekretessens giltighet så att inte uppgifter utan grund hålls hemliga och så att anteckningarna om sekretess är uppdaterade.

Enligt 25 § 2 mom. i offentlighetslagen: ”När det inte längre finns grunder för att sekretessbelägga en handling eller informationen i den ska det på den handling i vilken den ursprungliga anteckningen har införts antecknas att anteckningen har avlägsnats eller ändrats. Senast när handlingen lämnas ut till utomstående ska anteckningens korrekthet kontrolleras.” Sekretesstiden kan ha löpt ut eller så kanske inte informationsinnehållet längre behöver vara sekretessbelagt vid tidpunkten för utlämnandet av det. När klassificeringen av en handling ändras vidtas följande åtgärder:

- om handlingen har behandlats i pappersform stryks sekretesstämpeln över,
- under stämpeln skrivs ”sekretessen har upphört”, datum och den behöriga tjänstemannens underskrift,
- det antecknas också i ärenderegistret att handlingen har blivit offentlig,
- i elektroniska handlingar görs anteckningarna genom att ändra metadata,
- handlingar som är föremål för en begäran om information förses med ett separat följebrev som anger när sekretessen upphör,
- ändringar av metadata införs bland handlingens logguppgifter.

Enligt 31 § 1 mom. i offentlighetslagen: ”En myndighetshandling får inte hållas hemlig, när den sekretesstid som föreskrivs i lag eller med stöd av en lag har förflutit eller när den myndighet som förordnat om sekretess återkallar sitt förordnande.”

2.6 Sekretess- och tystnadsplikt

Organisationen ska med tillräcklig vägledning, kommunikation och övervakning säkerställa att alla som hanterar sekretessbelagd information känner till skyldigheten att sekretessbelägga handlingar, tystnadsplikten och förbudet mot att skaffa fördelar.

Enligt 22 § 1 mom. i offentlighetslagen ska en myndighetshandling sekretessbeläggas, om det i den lagen eller någon annan lag föreskrivs eller en myndighet med stöd av lag har föreskrivit att den ska vara sekretessbelagd eller om handlingen innehåller uppgifter för vilka tystnadsplikt föreskrivs genom lag.

Enligt 23 § i offentlighetslagen har personer som är anställda hos en myndighet eller personer som på andra grunder behandlar sekretessbelagda uppgifter tystnadsplikt och får inte använda sekretessbelagda uppgifter för att skaffa sig själv eller någon annan en fördel.

Enligt 4 § 2 mom. 2, 3 och 5 punkten i informationshanteringslagen ska en informationshanteringsenhets ledning ombesörja att det finns uppdaterade anvisningar, erbjuda utbildning om författningar, föreskrifter och informationshanteringsenhetens anvisningar om informationshantering, databehandling samt om offentlighet och sekretess i fråga om handlingar och ordna tillräcklig övervakning av att dessa iakttas.

Exempel på åtgärder som organisationen kan vidta:

- ge tydliga anvisningar om frågor som rör sekretessplikten, tystnadsplikten och förbudet mot att skaffa fördelar,
- genom kommunikation, introduktion och utbildning säkerställa att personalen har tillräcklig kännedom om frågor som rör sekretess, tystnadsplikt och förbudet mot att skaffa fördelar,
- informera personer som behandlar sekretessbelagd information om påföljderna för brott mot sekretessplikten, tystnadsplikten och förbudet mot att skaffa fördelar,
- aktivt övervaka fullgörandet av tystnadsplikten i organisationen, samt
- i samband med att anställnings- och tjänsteförhållanden samt praktiktid upphör säkerställa att de som lämnar organisationen är medvetna om att tystnadsplikten fortsätter även efter att anställnings- och tjänsteförhållandet eller praktiktiden har upphört.

2.7 Utlämnande av sekretessbelagd information

Organisationerna rekommenderas att tydligt bestämma och ge anvisningar om i vilka situationer, på vilka grunder och hur sekretessbelagd information får lämnas ut.

Organisationerna rekommenderas att säkerställa att offentlighetsprincipen i fråga om myndigheters handlingar förverkligas och att sekretessbelagd information inte röjs genom att identifiera och ge anvisningar[8] om de situationer där sekretessbelagd information får lämnas ut.

I 26–32 § i offentlighetslagen föreskrivs om de allmänna grunderna för utlämnande av sekretessbelagda uppgifter, det vill säga om grunderna för undantag från och upphörande av sekretess. I 17–21 § i offentlighetslagen beskrivs myndigheternas skyldighet att främja tillgången till information, och i paragraferna ingår även preciseringar om utlämnandet av sekretessbelagda uppgifter.[9] Anvisningarna bör ta hänsyn till dessa och eventuell speciallagstiftning.

Exempel på åtgärder som organisationen kan vidta:

- gå igenom de för den egna verksamheten relevanta allmänna grunderna för utlämnande av information samt grunderna för utlämnande i speciallagstiftning,
- utifrån dessa ge anvisningar om hur och på vilka grunder sekretessbelagd information får lämnas ut,
- definiera ansvar och beslutsförfaranden för utlämnande av sekretessbelagd information,
- ge anvisningar om att kontrollera sekretessens giltighet, bland annat för att säkerställa att det inte finns ogrundade sekretessanteckningar i de handlingar som ska lämnas ut, samt
- se till att den som mottar sekretessbelagd information är medveten om sekretess- och tystnadsplikten och om förbudet mot att skaffa fördelar.

8 InfL 4 § 2 mom. 2 punkten

9 Handlingar som ska hållas hemliga för allmänheten kan till exempel lämnas ut till en på förhand bestämd mottagare inom ramen för en bestämmelse som innehåller en offentlighets- eller sekretesspresumtion (OffL 17 § 2 och 3 mom. och 23 § 2 mom.).

2.8 Uppgifter som uppges enligt prövning

Organisationerna rekommenderas att identifiera de uppgifter som ska uppges enligt prövning, göra en anteckning på dem i den omfattning som det behövs och skydda dem genom att riskbaserat använda de hanteringsmetoder som används för att skydda sekretessbelagda uppgifter.

Enligt 16 a § 1 mom. kan det på en handling antecknas ”HARKINNANVARAISESTI ANNETTAVA” och på svenska ”UPPGES ENLIGT PRÖVNING”, om utlämnande av handlingen enligt lag är beroende av en myndighetsprövning eller om uppgifterna i handlingen enligt lag får användas eller lämnas ut endast för det ändamål som angetts och om obehörigt avslöjande av uppgifterna kan orsaka olägenheter för allmänna eller enskilda intressen eller försämra en myndighets verksamhetsförutsättningar.

Uppgifter som kan uppges enligt prövning kan till exempel vara uppgifter om ärenden vars beredning fortfarande pågår och som ännu inte är offentliga.[10] Bilden nedan visar en anteckning på en handling som kan lämnas ut enligt prövning. Anteckningen kan användas i både manuella och elektroniska handlingar.

Figur 3. Bild som visar en anteckning på en handling som kan lämnas ut enligt prövning.

UPPGES ENLIGT PRÖVNING

OffL (621/1999) 16 a §

Syftet med anteckningen är att informera den som behandlar handlingen om att handlingen innehåller information som får lämnas ut endast under särskilda förutsättningar, på grund av att handlingen inte ännu är offentlig eller på grund av att den, trots att den är offentlig, får lämnas ut endast under vissa förutsättningar. Enligt 16 § 3 mom. i offentlighetslagen: ”Personuppgifter ur en myndighets personregister får, om inte något annat särskilt bestäms i lag, lämnas ut i form av en kopia eller en utskrift eller i elektronisk form om mottagaren enligt bestämmelserna om skydd för personuppgifter har rätt att registrera och använda sådana personuppgifter. För direktmarknadsföring och för opinions- eller marknadsundersökningar får personuppgifter dock lämnas ut endast om det särskilt föreskrivs eller om den registrerade har samtyckt till detta.”

10 OffL 6 §, 7 §, 9 § 2 mom.

Exempel på åtgärder som organisationen kan vidta:

- ge anvisningar om de behörigheter, förfaranden och principer enligt vilka uppgifter som kan uppges enligt prövning lämnas ut,
- skydda uppgifter som kan uppges enligt prövning genom att riskbaserat använda de metoder för hantering av informationssäkerhet som används vid behandling av sekretessbelagda uppgifter, samt
- säkerställa att dataskyddslagstiftningen har beaktats i behandlingen av personuppgifter som kan lämnas ut enligt prövning.

3 Rekommendationer för skydd av sekretessbelagd information

3.1 Behandling och anvisningar

3.1.1 Skydd av information från utomstående

Organisationen ska ordna behandlingen av sekretessbelagd information så att utomstående inte får kännedom om informationen av misstag eller avsiktligen.

Organisationerna rekommenderas att säkerställa att sekretessbelagd information är skyddad från utomstående genom att använda tillräckligt säkra lokaler för behandling av informationen och genom att vidta andra åtgärder som minskar risken för att utomstående får kännedom om informationen.[11]

Exempel på åtgärder som organisationen kan vidta:

- placera informationssystem och informationslager som innehåller sekretessbelagda uppgifter i ett tillräckligt skyddat område. Vid bedömningen kan man använda de krav på säkerhetsområden som beskrivs i säkerhetsklassificeringsförordningen,[12]
- ge anvisningar om att lokaler med adekvat ljudisolering ska användas när sekretessbelagd information diskuteras,
- skaffa sekretessfilter för datorer och ordna arbetsplatserna så att den information som behandlas inte av misstag kan ses av utomstående,
- ge anvisningar om hur sekretessbelagd information ska behandlas särskilt i situationer där informationen måste behandlas eller transporteras utanför säkra lokaler,
- säkerställa att sekretessbelagd information förstörs på ett tillräckligt säkert sätt.

11 InfL 13 § 1 mom., 15 § 2 mom., OffL 22 §

12 SKF 9 § 1 punkten och Rekommendation om behandling av säkerhetsklassificerade handlingar FM 2021:10

3.1.2 Lokalsäkerhet

> Organisationerna ska behandla och förvara informationsmaterial i verksamhetslokaler som är tillräckligt säkra enligt kraven på tillförlitlighet, integritet och tillgänglighet.[13]

Organisationerna rekommenderas att säkerställa lokalsäkerheten genom att vidta förebyggande, förhindrande och begränsande åtgärder för att upptäcka och spåra gärningar som äventyrar skyddet samt åtgärder för att återställa säkerhetsnivån.

Bedömningen av fysiska säkerhetsåtgärder grundar sig på riskbedömning och den helhet som flernivåskyddet bildar. Det är således i vissa situationer möjligt att utifrån en riskbedömning antingen godta brister i enskilda skyddsåtgärder eller kräva säkerhetsåtgärder på en högre nivå än den normala målnivån. Genom tillämpning av principen om skydd på flera nivåer kan en lämplig och i förhållande till riskbedömningen tillräcklig kombination av säkerhetsåtgärder fastställas, en kombination bestående av administrativa, funktionella och fysiska metoder.

När det gäller det fysiska skyddet av sekretessbelagda handlingar rekommenderas att man använder de i säkerhetsklassificeringsförordningen[14] definierade begreppen som gäller säkerhetsområden på olika nivåer och att man drar nytta av Julkri-kriterierna vid definition av detaljerade fysiska skydd (FYY-05, FYY-06 och FYY-07).

Informationslager som innehåller sekretessbelagda uppgifter och handlingar samt informationssystem som används vid behandling av dem bör placeras i ett område som myndigheten utsett för detta ändamål – till exempel ett sådant administrativt område som beskrivs i säkerhetsklassificeringsförordningen – eller så måste informationen skyddas riskbaserat med andra säkerhetskontroller.

De områden som definieras i säkerhetsklassificeringsförordningen är:

1. ”*administrativa områden* som har tydligt bestämda synliga gränser och till vilka endast personer som har auktoriserats av en statsförvaltningsmyndighet har tillträde utan följeslagare,
2. *skyddsområden* som har tydligt bestämda och skyddade gränser till vilka allas inträde och utträde övervakas genom identifiering med passerkort eller

13 InfL 15 § 2 mom

14 SKF 9 §

personligen och till vilka endast personer vilkas pålitlighet har fastställts har tillträde utan följeslagare och som har ett särskilt tillstånd att få komma in på området."

När det gäller verksamhetslokaler som används för flera ändamål är det nödvändigt att i förväg säkerställa att lokalernas säkerhetslösningar är adekvata för behandling av sekretessbelagd information. Dessutom ska det beaktas att även personer som är anställda av andra organisationer kan arbeta i lokalerna.

Mer information om frågor som rör lokalsäkerhet finns i informationshanteringsnämndens rekommendation (FM 2021:72).[15] Riksarkivet utfärdar närmare föreskrifter om krav på arkivutrymmen.[16]

Exempel på åtgärder för att förbättra lokalsäkerheten:

- sköta om låsningen av lokalerna och nyckelhanteringen,
- placera arbetsplatserna på ett sådant sätt att smygtittande inte är möjligt,
- sköta om hanteringen av åtkomsträttigheterna,
- se till att besökare har följeslagare,
- införa ett passersystem.

3.1.3 Tillåtna databehandlingsmiljöer

Organisationen rekommenderas att definiera och ge tydliga anvisningar om i vilka system, tjänster, förvaringslösningar och terminalenheter sekretessbelagd information får behandlas och lagras.[17]

15 Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet, FM 2021:72, kapitel 12.

16 Riksarkivet Föreskrift och anvisningar angående arkivutrymmen. AL/19699/07.01.01.00/2012

17 InfL 4 § 2 mom. 2 punkten

Förutom att skydda informationssystemen ska man se till att användarna vet vilka uppgifter som får behandlas i vilka miljöer; det behövs således anvisningar om vilka behandlingsmiljöer som är tillåtna.

Exempel på åtgärder som organisationen kan vidta:

- ge anvisningar om i vilka system det är tillåtet att behandla och förvara sekretessbelagd information, inklusive verktyg för grupparbete,
- ge anvisningar om i vilka system det inte är tillåtet att behandla eller förvara sekretessbelagd information,
- ge anvisningar om förvaringslösningar för sekretessbelagd information i pappersdokument och för annan, icke-elektronisk sekretessbelagd information,
- förbjuda behandling av sekretessbelagd information i sociala medier,
- ge anvisningar om hur sekretessbelagd information får behandlas i mobila enheter,
- ange systemspecifika begränsningar och andra eventuella krav som måste beaktas vid behandling av sekretessbelagd information med hjälp av systemet i fråga,
- övervaka att endast tillåtna system används vid behandling av sekretessbelagd information.

3.1.4 Behandling av information i molntjänster

Den allmänna utgångspunkten vid planering av behandling av sekretessbelagd information i molntjänster är att säkerheten bör säkerställas på ett heltäckande och riskbaserat sätt, på samma sätt som i tjänster som produceras med annan teknik.

Vid planering av användningen av molntjänster och vid bedömning av riskerna förenade med användningen bör man också ta hänsyn till molntjänsternas egenskaper, såsom de olika genomförandemodellerna för tjänsterna, fördelningen av säkerhetsansvaret mellan kunden och leverantören, aspekterna relaterade till informationens fysiska plats samt den snabba tekniska utvecklingen av molntjänsterna och de utmaningar i förändringshanteringen som är kopplade till denna utveckling.

Det finns i princip inga rättsliga hinder för behandling av sekretessbelagd information i molntjänster. När man bedömer molntjänsternas lämplighet ska organisationen dock ta reda på riskerna i fråga om molntjänstens säkerhet och tjänstens lämplighet för det planerade användningsändamålet, med beaktande av särskilt följande aspekter:

- säkerheten och riskerna i samband med överföring av informationsmaterial i datanät,[18]
- riskerna förknippade med användning och administrering av molntjänsten,
- organisationens interna kompetens i att använda molntjänster,
- risker relaterade till lagstiftningen och till bestämmanderätt,
- kan tillgången till uppgifter säkerställas tillräckligt bra även i allvarliga störningssituationer och eventuellt även under exceptionella omständigheter, samt
- risker förknippade med informationens fysiska plats.

I denna rekommendation ingår ingen analys eller några närmare anvisningar om frågor som rör användningen av molntjänster, men följande rekommendationer om användningen av molntjänster ska organisationen gärna använda:

- kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen (Julkri) och användningsfallet ”Bedömning av SaaS-molntjänsten”[19], som ingår i denna publikation,
- hantering av säkerhetsklassificerade handlingar i molntjänster (FM 2022:6)
- säkerhetskriterier för molntjänster (PiTuKri).

18 InfL 14 §

19 Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen (Julkri), bilaga 3, kapitel 2.1.2 Bedömning av SaaS-molntjänsten

3.1.5 Distansanvändning

Organisationerna rekommenderas att definiera och ge anvisningar om förfaranden för behandling av sekretessbelagd information vid arbete utanför de säkerhetsområden som organisationerna definierat.[20]

Lagstiftningen ställer inga hinder i vägen för behandling av sekretessbelagd information utanför säkerhetsområden[21], såsom i offentliga lokaler eller i distansarbete [22]. Behandlingen av sekretessbelagd information i sådana lokaler är förenad med olika risker, som bör beaktas vid planering av behandlingen. På grund av detta rekommenderas att organisationerna bedömer dessa risker och utifrån denna bedömning avgör var och på vilket sätt sekretessbelagd information får behandlas.[23]

Exempel på åtgärder som organisationen kan vidta:

- ge anvisningar om i vilken omfattning sekretessbelagd information får behandlas utanför säkerhetsområdena,
- lista informationssystem och dataöverföringssätt som får användas vid distansbehandling av sekretessbelagd information,
- fastställa krav på de terminalenheter som används för behandling av information,
- utarbeta anvisningar om förhindrande av olovlig observation och avlyssning,
- utarbeta anvisningar om förvaring av information och datamedier i olika former utanför säkerhetsområdena,
- ge anvisningar om goda förfaranden för förbättring av säkerheten vid hantering i en icke-säker miljö, samt
- utarbeta anvisningar om behandling av sekretessbelagd information utomlands.

20 InfL 4 § 2 mom.
21 Se kapitel 3.1.2 Lokalsäkerhet
22 SKF 10 §
23 InfL 13 § 1 mom.

3.1.6 Anvisningar

Det rekommenderas att organisationerna för behandlingen av sekretessbelagd information utarbetar anvisningar som är så lättanvända som möjligt.

Enligt 4 § 2 mom. 2 punkten i informationshanteringslagen ska en informationshanteringsenhets ledning ha ”uppdaterade anvisningar om hantering av informationsmaterial, om användning av informationssystem, om databehandlingsrättigheter, om informationshanteringsansvar, om informationsrättigheter, om informationssäkerhetsåtgärder samt om beredskap för undantagsförhållanden”. Förutom att anvisningarna är heltäckande, korrekta, konsekventa och uppdaterade är det viktigt att de är lätta att använda och tillgängliga.

Exempel på åtgärder som organisationen kan vidta:

- säkerställa att anvisningarna är begripliga för personer som inte är experter på informationssäkerhet,
- dela upp anvisningarna i tillräckligt små helheter, i vilka det är möjligt att snabbt hitta det huvudsakliga innehållet,
- använda effekter för att framhäva det huvudsakliga innehållet,
- se till att anvisningarnas rubriker och innehåll överensstämmer med varandra,
- skapa en söktjänst som gör det lätt att hitta anvisningar,
- koppla anvisningarna till situationer där de sannolikt kommer att behövas,
- samla gällande anvisningar om informationssäkerhet på ett ställe, där det är lätt för organisationens användare att hitta dem, samt
- informera om anvisningarna och om ändringar som gjorts i dem.

3.2 Processer

3.2.1 Säkerhet i upphandlingar och system

> I processer för upphandling och underhåll av informationssystem och tjänster som har anknytning till behandling av sekretessbelagd information ska organisationerna inkludera fastställande av informationssäkerhetskrav och säkerställande av att kraven uppfylls.

I 13 § 4 mom. i informationshanteringslagen föreskrivs följande: ”Myndigheten ska vid sina upphandlingar säkerställa att de aktuella informationssystemen har lämpliga säkerhetsåtgärder”. För att det lagstadgade kravet ska bli uppfyllt rekommenderas att det i processerna för upphandling av informationssystem och tjänster som har anknytning till sekretessbelagd information ingår steg där man definierar informationssäkerhetskrav för upphandlingen och säkerställer att kraven uppfylls.

I samband med att man definierar informationssäkerhetskraven för en tjänst är det bra att också bedöma nödvändigheten och omfattningen av informationssäkerhetskrav på tjänsteproducentens verksamhet. Dessutom rekommenderas organisationerna att i samband med upphandlingar bedöma lagstiftningsrelaterade[24] risker och beakta dem i kraven på tjänsteproducenten och den fysiska platsen för informationen.

Det rekommenderas att underhållsprocesserna planeras så att man i samband med dem tillräckligt ofta säkerställer att informationssäkerhetskraven är uppdaterade, att informationssäkerhetskraven är uppfyllda i samband med versionsuppdateringar och att allmänt identifierade sårbarheter åtgärdas.

Upphandlingarna och deras säkerhet behandlas i kapitel 8 i informationshanteringsnämndens rekommendation ”Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet (FM 2021:72)” och i Julkri-kriteriet Upphandlingarnas säkerhet (HAL-16).

Med vissa undantag ska statliga ämbetsverk och inrättningar använda gemensamma grundläggande informationsteknik- och informationssystemtjänster[25]. För produktionen

24 Med lagstiftningsrelaterad risk avses i detta sammanhang till exempel en situation där lagstiftning som gäller tjänsteproducenten kräver att denne överlämnar sekretessbelagd information till myndigheter i en annan stat.

25 Lag om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (1226/2013)

av dessa tjänster ansvarar Statens center för informations- och kommunikationsteknik Valtori[26], och i vissa fall andra statsägda producenter, såsom Suomen erillisverkot Oy.[27]

När det gäller att säkerställa säkerheten vid behandling av sekretessbelagd information rekommenderas att de organisationer som använder tjänster beaktar informationssäkerhetskraven för gemensamma tjänster i sina serviceavtal och att de i samarbete med tjänsteproducenten kontrollerar dem i samband med revideringar av avtalen.

I offentliga upphandlingar använder organisationerna i stor utsträckning också gemensamma inköpscentraler och anknutna enheter. Med tanke på säkerheten för sekretessbelagd information rekommenderas att organisationerna säkerställer att krav som gäller sekretessbelagd information inkluderas i de upphandlingskontrakt som upprättas med inköpscentraler och anknutna enheter och, om möjligt, även i de ramavtal som ingås med dem.

Exempel på åtgärder som organisationen kan vidta:

- säkerställa att det i de obligatoriska stegen i upphandlingsprocessen ingår definition, kontroll och godkännande av informationssäkerhetskrav innan anbudsförfrågan skickas,
- säkerställa att alla ovan nämnda steg dokumenteras skriftligt,
- kräva att tjänsteproducenten uppfyller minimikraven i fråga om sekretessbelagd information,
- kräva att tjänsteproducenten på ett trovärdigt sätt visar att de tjänster som används uppfyller minimikraven på dem,
- säkerställa att processerna för implementering och förändringshantering inkluderar kontroll av att informationssäkerhetskraven uppfylls innan nya versioner börjar användas, samt
- säkerställa att sekretesskraven beaktas i både kontrakt och ramavtal.

26 Statsrådets förordning om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (132/2014)

27 Lag om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015)

3.2.2 Uppdatering av användarrättigheter

För att säkerställa att användarrättigheterna för informationssystemen är korrekta och uppdaterade rekommenderas att organisationerna definierar processer för hur användarrättigheter uppdateras i samband med uppgiftsändringar.

I 16 § i informationshanteringslagen föreskrivs följande: ”Den systemansvariga myndigheten ska definiera användarrättigheterna för informationssystem. Användarrättigheterna ska definieras och uppdateras utifrån användarens uppgiftsrelaterade användningsbehov”.

För att säkerställa att användarrättigheterna är korrekta och uppdaterade rekommenderas organisationen att koppla kontrollen av detta till processer som alltid genomförs i samband med ändringar av personers uppgifter. Detta säkerställer att de nödvändiga ändringarna av användarrättigheter blir utförda.

Dessutom rekommenderas att processen för underhåll av användarrättigheter utformas så att de egentliga besluten om rättigheterna fattas av personer som är ansvariga för den sekretessbelagda informationen och som har förutsättningar att bedöma användarens behov av att få denna rättighet. Mer information finns i Julkri-kriteriernas delområde teknisk säkerhet (TEK) under punkten ”Administration av åtkomsträtt” (TEK-07).

Exempel på åtgärder som organisationen kan vidta:

- identifiera de system som innehåller sekretessbelagd information,
- definiera processer för säkerställande av att användarrättigheterna uppdateras när anställningsförhållanden och externa tjänster inleds, avslutas och ändras,
- separera godkännandet av användarrättigheter från det praktiska genomförandet av dem, samt
- kontrollera minst en gång om året att användarrättigheterna till sekretessbelagd information är uppdaterade.

3.2.3 Verifiering och övervakning av användarna

Organisationen rekommenderas att verifiera användarna av sekretessbelagd information med tillräckligt tillförlitliga individuella användar-ID:n och att säkerställa säkerheten vid behandlingen med tillräcklig övervakning.

Det rekommenderas att man säkerställer säkerheten för sekretessbelagd information genom att för verifiering av användarna använda tillräckligt tillförlitliga metoder, till exempel:

- individuella personliga användar-ID:n,
- åtminstone en metod som baserar sig på lösenord, samt
- låsning av användar-ID:n efter för många felaktiga försök.

Starkare verifieringsmetoder, till exempel flerstegsverifiering baserad på en mobil enhet eller ett certifikatkort, rekommenderas särskilt för situationer där användningen sker i en mindre säker miljö. Mer information finns i Julkri-kriteriernas delområde teknisk säkerhet (TEK) under punkten ”Administration av åtkomsträtt” (TEK-07).

Dessutom rekommenderas att organisationen säkerställer säkerheten vid behandling av sekretessbelagd information genom tillräcklig övervakning baserad på logguppgifter. Enligt 17 § i informationshanteringslagen: ”En myndighet ska ombesörja att logginformation insamlas om användning av dess informationssystem och om utlämnande av information från dem, om användningen förutsätter identifiering eller annan registrering. Syftet med logginformationen är uppföljning av användningen och utlämnandet av information från informationssystem samt utredning av tekniska systemfel”.

Exempel på åtgärder som en organisation kan vidta för att förbättra verifieringen av användare och övervakning av användningen:

- definiera en policy enligt vilken alla användare har individuella användar-ID:n,
- separera inloggningsuppgifter som är kopplade till underhåll av systemen från normala personliga inloggningsuppgifter,
- fastställa minimikrav i fråga om lösenord och se till att de uppfylls programmatiskt,

- införa ett förfarande där det av användare som loggar in i ett system utanför organisationen krävs en ytterligare bekräftelse med en mobilapplikation, samt
- för system som innehåller sekretessbelagd information definiera loggövervakning bestående av flera övervakningsmetoder som kompletterar varandra, såsom regelbaserade larm i samband med eventuella missbruk och manuella loggkontroller som kompletterar dessa.

3.2.4 Kontinuitetshantering för sekretessbelagd information

Organisationerna rekommenderas att planera och genomföra adekvata skydd för att säkerställa konfidentialiteten för sekretessbelagd information även i störningssituationer.[28]

Som en del av beredskap och kontinuitetshantering planerar organisationerna åtgärder för att säkerställa kontinuiteten i verksamheten och för att återhämta sig från störningssituationer. Dessa åtgärder, som vanligtvis är inriktade på information som är viktig eller kritisk med tanke på organisationens verksamhet, beskrivs i Julkri-kriteriernas delområde Beredskap och kontinuitetshantering (VAR).

Exempel på åtgärder som organisationen kan vidta för att säkerställa att information förblir sekretessbelagd under störningssituationer:

- säkerställa att personal som hanterar störningssituationer, inklusive tjänsteleverantörernas personal, har kunnande och är medvetna om sekretesskraven i fråga om information som behandlas,
- utföra riskbedömning under tjänstens hela livscykel,
- planera tillräckliga skydd för processerna för kontinuitetshantering för att säkerställa konfidentialiteten för information,

28 InfL 13 § 1 mom.

- planera metoder som kan ersätta de hanteringsmetoder som används i normala situationer och som inte kan genomföras under en störningssituation, samt
- regelbundet öva verksamheten i samband med störningssituationer i enlighet med kontinuitetsplanerna, och då särskilt fästa uppmärksamhet vid sekretessen.

3.3 Tekniska rekommendationer

3.3.1 Avskiljning av behandlingsmiljön

Organisationerna rekommenderas att avskilja de miljöer där sekretessbelagd information behandlas från offentliga datanät och andra miljöer med lägre säkerhetsnivå.

Avskiljning av informationssystem är en av de effektivaste faktorerna vid skydd av sekretessbelagd information. Målet med avskiljningen är att begränsa den miljö där sekretessbelagd information behandlas så att den blir en hanterbar helhet och att se till att informationen behandlas endast i tillräckligt säkra miljöer. I praktiken har man i den offentliga förvaltningens organisationer vanligtvis avskilt hela den miljö där information behandlas, både offentlig och sekretessbelagd information, från de offentliga datanäten.

Vid koppling av databehandlingsmiljön till andra miljöer rekommenderas att åtminstone en brandväggslösning används. Mer information finns i Julkri-kriteriernas delområde teknisk säkerhet (TEK) under punkterna ”Nätets strukturella säkerhet” (TEK-01) och ”Nätets strukturella säkerhet – avskiljning av behandlingsmiljöer” (TEK-01.3).

Exempel på en åtgärd som organisationen kan vidta:

- avskilja organisationens databehandlingsmiljö från andra miljöer med brandvägg.

3.3.2 Datakryptering och verifiering av mottagare

Organisationerna rekommenderas att kryptera sekretessbelagd information i allmänna datanät med krypteringslösningar som stöder modern krypteringsstyrka och inte har några kända sårbarheter.

Enligt 14 § 1 mom. i informationshanteringslagen: ”Om en myndighet överför sekretessbelagd information i det allmänna datanätet ska informationen överföras i ett krypterat eller på annat sätt skyddat format. Dessutom ska överföringen ordnas så att mottagaren verifieras eller identifieras på ett tillräckligt informationssäkert sätt, innan mottagaren kommer åt att behandla den överförda sekretessbelagda informationen”.

Krypteringskravet kan uppfyllas antingen med en separat kryptering av datakommunikationen eller de data som ska överföras. Krypteringslösningar som inte har några kända sårbarheter och som stöder moderna krypteringsstyrkor kan anses vara tillräckligt säkra för de flesta sekretessbelagda uppgifter. Mer information finns i Julkri-kriteriernas delområde teknisk säkerhet (TEK) under punkten ”Kryptering av information” (TEK-16), i de krypteringslösningar som godkänts av Cybersäkerhetscentrets NCSA-verksamhet och i dokumentet om hantering av hårddiskarnas livscykel.

Exempel på åtgärder som organisationen kan vidta:

- se till att organisationen har en planerad nyckelhantering,
- använda servercertifikat i dataöverföring mellan informationssystem, samt
- identifiera personer med en stark elektronisk identifieringsmetod eller på något annat tillräckligt säkert sätt.

3.3.3 Systemhärdningar

Organisationerna rekommenderas att införa ett förfarande där system som innehåller sekretessbelagd information installeras systematiskt så att slutresultatet blir en så kallad härdad installation.

System har ofta många funktionaliteter som är förinställt aktiverade. Om onödiga egenskaper inte inaktiveras ökar risken för obehörig användning av sekretessbelagd information i systemen.

På grund av detta rekommenderas att system som innehåller sekretessbelagd information härdas med hjälp av ett systematiskt förfarande där förinställda lösenord ändras, icke-nödvändiga tjänster inaktiveras och anslutningar och egenskaper begränsas i enlighet med principen om lägsta behörighet. Mer information finns i Julkri-kriteriernas delområde teknisk säkerhet (TEK) under punkten ”Systemhärdning” (TEK-07).

Exempel på åtgärder som organisationen kan vidta:

- identifiera de objekt som ska härdas,
- definiera sättet att genomföra härdningen,
- härda objekten enligt definitionerna, samt
- regelbundet säkerställa att härdningarna är aktiva, särskilt efter uppdateringar, under hela informationssystemets livscykel.

3.3.4 Skydd mot skadeprogram

Organisationerna rekommenderas att planera och genomföra tillförlitliga metoder för förebyggande och upptäckt av hot från skadlig programvara och för åtgärdande av situationer.

Systemen kan skyddas mot skadeprogram till exempel genom härdning, avgränsningar av användarrättigheter, säkerhetsuppdateringar, kapacitet att observera avvikelser, säkerställande av personalens säkerhetsmedvetenhet och användning av program för bekämpning

av skadliga program. Mer information finns i Julkri-kriteriernas delområde teknisk säkerhet (TEK) under punkten ”Skydd mot skadeprogram” (TEK-11).

3.3.5 Hantering av sårbarheter i program

Organisationerna rekommenderas att förse databehandlingsmiljön med tillförlitliga metoder för hantering av programsårbarheter under miljöns hela livscykel.

Programsårbarheter utnyttjas i många olika typer av attacker i något skede. Ansvarsfulla leverantörer korrigerar sårbarheter som upptäcks i deras programvaror. Organisationen kan minska riskerna förknippade med sårbarheter i programvaror genom att systematiskt övervaka sårbarheter och installera säkerhetsuppdateringar utan dröjsmål. Mer information finns i Julkri-kriterierna under punkten ”Hantering av sårbarheter i program” (TEK-19).

Exempel på åtgärder som organisationen kan vidta:

- följa information om informationssäkerhet från myndigheter, tillverkare av utrustning och programvaror samt andra liknande aktörer,
- installera säkerhetsuppdateringar som bedömts vara nödvändiga och kontrollera att de lyckats,
- i upphandlingskrav och kontrakt ålägga leverantörerna att systematiskt övervaka sårbarheter i programvaran och leverera säkerhetsuppdateringar utan dröjsmål,
- kontrollera nätet och dess tjänster och servrar samt till nätet kopplade arbetsstationer, bärbara datorer, skrivare, mobila enheter och motsvarande på ett heltäckande sätt genom sårbarhetsskanning, en gång om året och alltid efter betydande ändringar,
- ordna behandlingen av sårbarheter samt brister som upptäcks i uppdateringsförfarandena så att svagheter som väsentligt påverkar skyddet av databehandlingsmiljön tas bort, korrigeras eller på annat sätt begränsas så att behandlingen av sekretessbelagda uppgifter inte äventyras.

Ordlista

Term	Definition	Källa
handling	en framställning i skrift, en bild eller ett meddelande som avser ett visst objekt eller ärende och uttrycks i form av tecken som på grund av användningen är avsedda att höra samman och vilket kan uppfattas endast med hjälp av automatisk databehandling eller en ljud- eller bildåtergivningsanordning eller något annat hjälpmedel Begreppet handling är vittomfattande; till handlingar hör till exempel pappersdokument, bilder, ljud, videor och meddelanden.	OffL 5 § 1 mom.
personuppgift som hör till särskilda kategorier av personuppgifter	en personuppgift som avslöjar ras eller etniskt ursprung, politiska åsikter, religion eller övertygelse, medlemskap i fackförening, en genetisk eller biometrisk uppgift, en uppgift om hälsa eller en uppgift om en fysisk persons sexualliv eller sexuella läggning	Dataskyddsförordningen artikel 9
sårbarhet	brist, fel eller tillvägagångssätt som ökar risken för hot mot säkerheten Sårbarheter kan förekomma i till exempel datasystem, mjukvara, hårdvara, processer eller människors verksamhet. En sårbarhet kan till exempel vara ett fel i ett program som gör det möjligt att kringgå begränsningar som förhindrar missbruk.	VAHTI-ordlista om riskhantering i digital verksamhetsmiljö – presentation och introduktion till riskkommunikation; 15.11.2022 (Myndigheten för digitalisering och befolkningsdata)
skadligt program	ett program som avsiktligt orsakar händelser som är oönskade för användaren i ett informationssystem eller en del av ett sådant Skadliga program är till exempel virus, maskar och trojanska hästar samt kombinationer av dessa.	Ordlista om cybersäkerhet (TSK 52, 2018)
administrativt område	områden eller lokaler som är avsedda för myndighetens normala arbete och till vilka endast personer som myndigheten i förväg auktoriserat har självständigt tillträde, vilket den aktör som har ansvar för lokalerna säkerställer Ett administrativt område eller en administrativ lokal kan till exempel vara en kontorslokal, flera olika kontorslokaler som bildar en helhet, ett serverutrymme, en datahall eller en lokal där ett företag eller en annan sammanslutning har verksamhet. I säkerhetsklassificeringsförordningen avses med administrativa områden sådana områden som har tydligt bestämda synliga gränser och till vilka endast personer som har auktoriserats av en statsförvaltningsmyndighet har tillträde utan följeslagare.	Rekommendation om behandling av sekretessbelagda handlingar (FM 2023:4) SKF 9 § 1 punkten

Term	Definition	Källa
hanteringsmetod, hanteringsåtgärd **synonym: kontroll**	en åtgärd genom vilken man strävar efter att ändra eller bevara en risk Termen hanteringsmetod används ibland som synonym till kontroll, men ofta avses med hanteringsmetod en helhetslösning (till exempel identifiering eller god förvaltningssed) som kan innehålla flera konkreta kontroller. Kontrollerna kan vara processer, verksamhetsprinciper, utrustning, praxis, engångsåtgärder eller annan typ av verksamhet.	VAHTI-ordlista om riskhantering i digital verksamhetsmiljö – presentation och introduktion till riskkommunikation; 15.11.2022 (Myndigheten för digitalisering och befolkningsdata)
personuppgift	en uppgift utifrån vilken en person kan identifieras direkt eller indirekt till exempel genom att kombinera en enskild uppgift till en annan uppgift som möjliggör identifiering En person kan identifieras till exempel utifrån namn, personbeteckning eller någon faktor som är kännetecknande för personen i fråga.	Dataskyddsförordningen artikel 4.1 Lag om behandling av personuppgifter i brottmål 3 § 1 mom. 1 punkten
offentlig handling	en myndighetshandling som det inte i någon bestämmelse har fastställts att ska vara sekretessbelagd	OffL 1 § och 9 §
offentlighetsprincipen	en princip enligt vilken myndighetshandlingar är offentliga, om inte något annat föreskrivs särskilt i offentlighetslagen eller någon annan lag	OffL 1 §
härdning	en process där ett system säkras genom att minska dess sårbarhetsyta Till vanliga sätt att minska antalet tillgängliga attackmetoder hör att ändra förinställda lösenord och att ta bort onödiga program, inloggningar och tjänster.	Rekommendation om behandling av sekretessbelagda handlingar (FM 2023:X)
logg	en fil där händelser och orsaker till händelser registreras i kronologisk ordning Händelser och ändringar i datasystem, applikationer, datanät och datainnehåll registreras i loggen, dvs. loggas. Logginformation används för övervakning av användning och av utlämnande av information från informationssystem och för utredning av tekniska systemfel.	Traficom – Så här samlar du in och använder loggdata InfL 17 §
metadata	information som beskriver kontext, innehåll eller struktur för ett material och som styr och dokumenterar behandlingen och hanteringen av materialet Metadata kan användas bland annat för att söka, lokalisera och identifiera ett material. Metadata är väsentliga när det gäller att hitta, lista och använda material. Metadata innehåller både uppgifter som beskriver materialet och tekniska metadata om systemet.	Tietotermit (2018)

Term	Definition	Källa
brandvägg	ett program eller utrustning vars syfte är att förhindra otillåten eller obehörig åtkomst från ett nätverk eller från en del av ett nätverk till en annan del Brandväggar används ofta mellan internet och lokala nät. Brandväggstekniken bygger på filtrering av datakommunikation som passerar genom brandväggen i båda riktningarna enligt fördefinierade regler. Brandväggen släpper igenom endast tillåten kommunikation.	Ordlista om cybersäkerhet (TSK 52, 2018)
risk	effekt av osäkerhet på mål Effekten utgör en avvikelse från det som förväntats. Den kan vara positiv, negativ eller både positiv och negativ, och den kan hantera, skapa eller åstadkomma möjligheter och hot. Risk uttrycks vanligtvis som en kombination av riskkällor, möjliga händelser, deras konsekvenser och deras sannolikhet. Risker kan påverka till exempel människor, djur, egendom, informationssystem, miljön eller kollektiva värden.	Ordlista om cybersäkerhet (TSK 52, 2018)
sekretessbelagd handling	en myndighetshandling som enligt offentlighetslagen eller någon annan lag ska sekretessbeläggas eller som en myndighet med stöd av lag har föreskrivit att ska vara sekretessbelagd, eller en handling som innehåller uppgifter för vilka tystnadsplikt föreskrivs genom lag	OffL 22 § och 24 §
sekretessbelagd information	information som finns i en handling och som på grund av sin beskaffenhet ska sekretessbeläggas	Rekommendation om behandling av sekretessbelagda handlingar (FM 2023:X)
informationsmaterial	datauppsättning som består av handlingar och annan motsvarande information och har samband med en viss myndighetsuppgift eller myndighetstjänst	InfL 2 §
informationshanteringsenhet	en myndighet eller administrativ helhet som består av flera myndigheter vars uppgift är att ordna informationshanteringen i enlighet med kraven i informationshanteringslagen Informationshanteringsenheter är statliga ämbetsverk och inrättningar; domstolar och nämnder som har inrättats för att behandla besvärsärenden; riksdagens ämbetsverk; statliga affärsverk; välfärdsområden; välfärdssammanslutningar; kommuner; samkommuner; självständiga offentligrättsliga inrättningar; universitet som avses i universitetslagen och yrkeshögskolor som avses i yrkeshögskolelagen.	VAHTI-ordlista om riskhantering i digital verksamhetsmiljö – presentation och introduktion till riskkommunikation; 15.11.2022 (Myndigheten för digitalisering och befolkningsdata) InfL 2 och 4 §

Term	Definition	Källa
informations-system	ett helhetsarrangemang som består av databehandlingsutrustning, programvara och annan databehandling Till exempel de lika molntjänsterna och terminalenheter som används vid behandling av data är informationssystem.	InfL 2 §
lednings- och hanteringssystem för informations-säkerhet	ett system som ingår i ett allmänt verksamhetssystem som skapas och genomförs baserat på bedömningar av riskerna i verksamheten och som används, övervakas, granskas, underhålls och förbättras för att uppnå en god informationssäkerhet Det innefattar organisationsstruktur, policyer, planerings- och utvecklingsåtgärder, ansvar, förfaranden, metoder, processer, indikatorer och resurser.	Valtiohallinnon tietoturvasanasto (VAHTI 8/2002)
informations-säkerhetsrisk	sannolikheten för att ett informationssäkerhetshot blir verklighet och den potentiella skadans storlek Riskens storlek beror på storleken på den potentiella skadan och sannolikheten för skadehändelsen.	Tiivis tietoturvasanasto (TSK 31, 2004)
skyddsområde	ett område som har tydligt bestämda och skyddade gränser till vilka allas inträde och utträde övervakas genom identifiering med passerkort eller personligen och till vilka endast personer vilkas pålitlighet har fastställts har tillträde utan följeslagare och som har ett särskilt tillstånd att få komma in på området	SKF 9 § 2 punkten
säkerhetsklass-ificerad handling	en handling som en statlig myndighet försett med en anteckning om säkerhetsklass En handling ska säkerhetsklassificeras om handlingen eller informationen i den är sekretessbelagd enligt 24 § 1 mom. 2, 5 eller 7–11 punkten i lagen om offentlighet i myndigheternas verksamhet och om obehörigt avslöjande eller obehörig användning av handlingen kan orsaka skada för försvaret, för förberedelser inför undantagsförhållanden, för internationella relationer, för brottsbekämpningen, för den allmänna säkerheten eller för stats- och samhällsekonomins funktion, eller på något annat jämförbart sätt för Finlands säkerhet.	InfL 18 § OffL 24 §
säkerhetsområde	ett begrepp som innefattar både administrativa områden och skyddsområden	SKF 9 §

Term	Definition	Källa
myndighets-handling	en handling som innehas av en myndighet och som har upprättats av myndigheten eller av någon som är anställd hos en myndighet eller som har inkommit till en myndighet för behandling av ett visst ärende eller i övrigt inkommit i samband med ett ärende som hör till myndighetens verksamhetsområde eller uppgifter En handling anses ha blivit upprättad av en myndighet även när den har upprättats på uppdrag av myndigheten. En handling anses ha inkommit till en myndighet även när den har inkommit till den som verkar på uppdrag av myndigheten eller i övrigt för myndighetens räkning, för att denne skall kunna utföra sitt uppdrag.	OffL 5 § 2 mom.[29]

29 I 5 § 3–5 mom. i OffL föreskrivs om vilka handlingar som inte ska betraktas som myndighetshandlingar och om hur lagen tillämpas på exempelvis handlingar som upprättats för myndigheters interna arbete.

Bilaga: Sammanställning av rekommendationerna och deras rättsliga grund

Kapitel	Rekommendation och rättslig grund
2.1 Sekretessbelagda myndighetshandlingar	Organisationen ska identifiera när den behandlar sekretessbelagd information. InfL 4 § 2 mom. 2 punkten.
2.2. Minimikrav och riskbaserad komplettering av dem	Organisationen ska uppfylla vissa minimikrav som grundar sig på lagstiftningen om behandling av sekretessbelagd information. InfL 13 §. Organisationerna rekommenderas att komplettera minimikraven genom att riskbaserat tillämpa informationssäkerhetskrav på en högre nivå. InfL 13 § 1 mom. Organisationerna rekommenderas att använda en riskbedömningsmetod som är lämplig för bedömning av informationssäkerhetsrisker och att tillämpa metoden systematiskt vid planering av hur informationssäkerheten för behandling av sekretessbelagd information ska ombesörjas. InfL 13 § 1 mom. Den potentiella kumulativa effekten bör beaktas när information skyddas och eventuellt klassificeras. InfL 13 §.
2.3 Informationens livscykel och sekretess	Organisationen ska identifiera de processer och informationssystem som är kopplade till behandlingen av sekretessbelagd information och riskbaserat säkerställa att de är tillräckligt informationssäkra under informationens hela livscykel. InfL 13 § 1 och 4 mom. Myndigheten ska vid sina upphandlingar säkerställa att de aktuella informationssystemen har lämpliga säkerhetsåtgärder. InfL 13 § 4 mom. Organisationerna rekommenderas att: identifiera alla sekretessbelagda uppgifter som de har ansvar för och de personer som behandlar dem samt de informationssystem som används vid behandlingen under informationens hela livscykel, definiera informationssäkerhetskrav för de informationssystem och tjänster som används i behandlingen, med hänsyn till de risker som är förknippade med behandlingen av de sekretessbelagda uppgifterna, säkerställa att informationssäkerhetskraven för informationssystem och tjänster uppfylls i samband med upphandlingar samt regelbundet under hela systemets livscykel genom att systematiskt tillämpa förfaranden för förändringshantering, planera och ge anvisningar för processerna vid behandling av sekretessbelagd information så att behandlingen är tillräckligt säker, genom tillräcklig övervakning säkerställa att de ovan beskrivna rekommendationerna följs, upprätthålla en informationshanteringsmodell för hantering av informationssäkerheten. InfL 4 § 2 mom., 5 § och 13 §.

Kapitel	Rekommendation och rättslig grund
2.4. Anteckningar om sekretess	Organisationerna rekommenderas att planera och genomföra antecknandet om sekretess på ett sådant sätt att alla som behandlar och alla som får sekretessbelagd information är medvetna om sekretesskravet. InfL 4 § 2 mom. och 13 § 1 mom., OffL 25 §. Det rekommenderas att man säkerställer konfidentialiteten för sekretessbelagda uppgifter genom att på ett systematiskt sätt ta reda på i vilka situationer och med vilka informationssystem sekretessbelagda uppgifter behandlas och för dessa planera förfaranden genom vilka det säkerställs att personer som hanterar sekretessbelagda uppgifter i alla situationer informeras om sekretessen. InfL 4 § 2 mom. och 13 § 1 mom., OffL 22 §.
2.5 Sekretessens giltighet och upphörande	Organisationerna rekommenderas att planera och ge anvisningar om att alla som behandlar eller lämnar ut sekretessbelagda uppgifter ska kontrollera sekretessens giltighet så att inte uppgifter utan grund hålls hemliga och så att anteckningarna om sekretess är uppdaterade. InfL 4 § 2 mom. 2 punkten och OffL 25 § 2 mom. och 31 §.
2.6 Sekretess- och tystnadsplikt	Organisationen ska med tillräcklig vägledning, kommunikation och övervakning säkerställa att alla som hanterar sekretessbelagd information känner till skyldigheten att sekretessbelägga handlingar, tystnadsplikten och förbudet mot att skaffa fördelar. InfL 4 § 2 mom. 2 och 3 punkten, OffL 22 § 1 mom. och 23 §.
2.7 Utlämnande av sekretessbelagd information	Organisationerna rekommenderas att tydligt bestämma och ge anvisningar om i vilka situationer, på vilka grunder och hur sekretessbelagd information får lämnas ut. InfL 4 § 2 mom. 2 punkten, OffL 7 kap.
2.8 Uppgifter som uppges enligt prövning	Organisationerna rekommenderas att identifiera de uppgifter som kan uppges enligt prövning och göra en anteckning på dem i den omfattning som det behövs. InfL 4 § 2 mom., 13 § 1 mom. och OffL 16 a §. Organisationerna rekommenderas att skydda uppgifter som kan uppges enligt prövning genom att riskbaserat använda de hanteringsmetoder som används för att skydda sekretessbelagda uppgifter. InfL 13 § 1 mom.
3.1.1 Skydd av personuppgifter från utomstående	Organisationen ska ordna behandlingen av sekretessbelagd information så att utomstående inte får kännedom om informationen av misstag eller avsiktligen. InfL 4 § 2 mom. 2 och 5 punkten, 15 § 2 mom., OffL 22 §. Organisationerna rekommenderas att säkerställa att sekretessbelagd information är skyddad från utomstående genom att använda tillräckligt säkra lokaler för behandling av informationen eller genom att vidta andra åtgärder som minskar risken för att utomstående får kännedom om informationen. InfL 13 § 1 mom., 15 § 2 mom.

Kapitel	Rekommendation och rättslig grund
3.1.2 Lokalsäkerhet	Organisationerna ska behandla och förvara informationsmaterial i verksamhetslokaler som är tillräckligt säkra enligt kraven på tillförlitlighet, integritet och tillgänglighet. InfL 15 § 2 mom. Organisationerna rekommenderas att säkerställa lokalsäkerheten genom att vidta förebyggande, förhindrande och begränsande åtgärder för att upptäcka och spåra gärningar som äventyrar skyddet samt åtgärder för att återställa säkerhetsnivån. InfL 13 § 1 mom., 15 § 2 mom. Organisationerna rekommenderas att använda de i säkerhetsklassificeringsförordningen definierade begreppen som gäller säkerhetsområden på olika nivåer och att dra nytta av Julkri-kriterierna vid definition av detaljerade fysiska skydd (FYY-05, FYY-06 och FYY-07). InfL 13 § 1 mom., 15 § 2 mom., SKF 9 §.
3.1.3 Tillåtna databehandlingsmiljöer	Organisationen rekommenderas att definiera och ge tydliga anvisningar om i vilka system, tjänster, förvaringslösningar och terminalenheter sekretessbelagd information får behandlas och lagras. InfL 4 § 2 mom. 2 punkten.
3.1.4 Distansanvändning	Organisationerna rekommenderas att definiera och ge anvisningar om förfaranden för behandling av sekretessbelagd information vid arbete utanför de säkerhetsområden som organisationerna definierat. InfL 4 § 2 mom. 2 punkten, 13 § 1 mom., SKF 10 §. Organisationerna rekommenderas att bedöma dessa risker och utifrån denna bedömning avgöra var och på vilket sätt sekretessbelagd information får behandlas. InfL 13 § 1 mom.
3.1.6 Anvisningar	Det rekommenderas att organisationerna för behandlingen av sekretessbelagd information utarbetar anvisningar som är så lättanvända som möjligt. InfL 4 § 2 mom. 2 punkten.
3.2.1 Säkerhet i upphandlingar och system	I processer för upphandling och underhåll av informationssystem och tjänster som har anknytning till behandling av sekretessbelagd information ska organisationerna inkludera definitioner av informationssäkerhetskrav och säkerställande av att kraven uppfylls. InfL 13 § 4 mom. I samband med att man definierar informationssäkerhetskraven för en tjänst är det bra att också bedöma nödvändigheten och omfattningen av informationssäkerhetskrav på tjänsteproducentens verksamhet. InfL 13 § 4 mom. Organisationerna rekommenderas att i samband med upphandlingar bedöma lagstiftningsrelaterade risker och beakta dem i kraven på tjänsteproducenten och den fysiska platsen för informationen. InfL 13 § 1 mom. Det rekommenderas att underhållsprocesserna planeras så att man i samband med dem tillräckligt ofta säkerställer att informationssäkerhetskraven är uppdaterade, att informationssäkerhetskraven är uppfyllda i samband med versionsuppdateringar och att allmänt identifierade sårbarheter åtgärdas. InfL 13 § 1 mom.

Kapitel	Rekommendation och rättslig grund
	När det gäller att säkerställa säkerheten vid behandling av sekretessbelagd information rekommenderas att de organisationer som använder tjänster beaktar informationssäkerhetskraven för gemensamma tjänster i sina serviceavtal och att de i samarbete med tjänsteproducenten kontrollerar dem i samband med revideringar av avtalen. InfL 13 § 1 och 4 mom. Med tanke på säkerheten för sekretessbelagd information rekommenderas att organisationerna säkerställer att krav som gäller sekretessbelagd information inkluderas i de upphandlingskontrakt som upprättas med inköpscentraler och anknutna enheter och, om möjligt, även i de ramavtal som ingås med dem. InfL 13 § 4 mom.
3.2.2 Uppdatering av användarrättigheter	För att säkerställa att användarrättigheterna för informationssystem är korrekta och uppdaterade rekommenderas att organisationen definierar processer för hur användarrättigheter uppdateras i samband med uppgiftsändringar. InfL 16 §. För att säkerställa att användarrättigheterna är korrekta och uppdaterade rekommenderas organisationen att koppla kontrollen av detta till processer som alltid genomförs i samband med ändringar av personers uppgifter. Detta säkerställer att de nödvändiga ändringarna av användarrättigheter blir utförda. InfL 16 §. Det rekommenderas att processen för underhåll av användarrättigheter utformas så att de egentliga besluten om rättigheterna fattas av personer som är ansvariga för den sekretessbelagda informationen och som har förutsättningar att bedöma användarens behov av att få denna rättighet. InfL 16 §.
3.2.3 Verifiering och övervakning av användarna	Organisationerna rekommenderas att verifiera användarna av sekretessbelagd information med tillräckligt tillförlitliga individuella användar-ID:n och att säkerställa säkerheten vid behandlingen med tillräcklig övervakning. InfL 4 § 2mom. 5 punkten, 13 § 4 mom., InfL 16 §. Det rekommenderas att man säkerställer säkerheten för sekretessbelagd information genom att för verifiering av användarna använda tillräckligt tillförlitliga metoder, till exempel individuella personliga användar-ID:n, åtminstone en metod som baserar sig på lösenord och låsning av användar-ID:n efter för många felaktiga försök. InfL 13 § 1 mom. Starkare verifieringsmetoder, till exempel flerstegsverifiering baserad på en mobil enhet eller ett certifikatkort, rekommenderas särskilt för situationer där användningen sker i en mindre säker miljö. InfL 13 § 1 mom., 14 §. Dessutom rekommenderas att organisationen säkerställer säkerheten vid behandling av sekretessbelagd information genom tillräcklig övervakning baserad på logguppgifter. InfL 17 §.
3.2.4 Kontinuitetshantering för sekretessbelagd information	Organisationerna rekommenderas att planera och genomföra adekvata skydd för att säkerställa konfidentialiteten för sekretessbelagd information även i störningssituationer. InfL 13 § 1 mom.

Kapitel	Rekommendation och rättslig grund
3.3.1 Avskiljning av behandlingsmiljön	Organisationerna rekommenderas att avskilja de miljöer där sekretessbelagd information behandlas från offentliga datanät och andra miljöer med lägre säkerhetsnivå. InfL 13 § 1 mom. Vid koppling av databehandlingsmiljön till andra miljöer rekommenderas att åtminstone en brandväggslösning används. InfL 13 § 1 mom.
3.3.2 Datakryptering och verifiering av mottagare	Organisationerna rekommenderas att kryptera sekretessbelagd information i allmänna datanät med krypteringslösningar som stöder modern krypteringsstyrka och inte har några kända sårbarheter. InfL 14 § 1 mom.
3.3.3 Systemhärdningar	Organisationerna rekommenderas att införa ett förfarande där system som innehåller sekretessbelagd information installeras systematiskt så att slutresultatet blir en så kallad härdad installation. InfL 13 § 1 mom. Organisationerna rekommenderas att härda system som innehåller sekretessbelagd information med hjälp av ett systematiskt förfarande där förinställda lösenord ändras, icke-nödvändiga tjänster inaktiveras och anslutningar och egenskaper begränsas i enlighet med principen om lägsta behörighet. InfL 13 § 1 mom.
3.3.4 Skydd mot skadeprogram	Organisationerna rekommenderas att planera och genomföra tillförlitliga metoder för förebyggande och upptäckt av hot från skadlig programvara och för åtgärdande av situationer. InfL 13 § 1 mom.
3.3.5 Hantering av sårbarheter i program	Organisationerna rekommenderas att förse databehandlingsmiljön med tillförlitliga metoder för hantering av programsårbarheter under miljöns hela livscykel. InfL 13 § 1 mom.

Källor

Författningar

Dataskyddslag (1050/2018). https://www.finlex.fi/sv/laki/ajantasa/2018/20181050
Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning). https://eur-lex.europa.eu/legal-content/SV/TXT/ https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&from=FI.
Lag om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (1226/2013). https://www.finlex.fi/sv/laki/ajantasa/2013/20131226
Lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018). https://www.finlex.fi/sv/laki/ajantasa/2018/20181054.
Lag om informationshantering inom den offentliga förvaltningen. https://www.finlex.fi/sv/laki/ajantasa/2019/20190906.
Lag om offentlighet i myndigheternas verksamhet (621/1999). https://www.finlex.fi/sv/laki/ajantasa/1999/19990621.
Lag om tjänster inom elektronisk kommunikation (917/2014). https://www.finlex.fi/sv/laki/ajantasa/2014/20140917.
Lag om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015). https://www.finlex.fi/sv/laki/ajantasa/2015/20150010.
Statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019). https://www.finlex.fi/sv/laki/ajantasa/2019/20191101.
Statsrådets förordning om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster (132/2014). https://www.finlex.fi/sv/laki/ajantasa/2014/20140132.

Informationshanteringsnämndens rekommendationer

Informationshanteringsnämndens rekommendation - Finansministeriet (2021:43). Rekommendation om metadata för ärendehantering. https://julkaisut.valtioneuvosto.fi/handle/10024/163359.
Informationshanteringsnämndens rekommendation - Finansministeriet (2022:65). Kriterier för bedömning av informationssäkerheten i den offentliga förvaltningen (Julkri): Rekommendation och kriterier. https://julkaisut.valtioneuvosto.fi/handle/10024/164418.
Informationshanteringsnämndens rekommendation - Finansministeriet (2021:72). Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet. https://julkaisut.valtioneuvosto.fi/handle/10024/163694.
Informationshanteringsnämndens rekommendation - Finansministeriet (2021:38). Rekommendation om tekniska gränssnitt och elektroniska förbindelser. https://julkaisut.valtioneuvosto.fi/handle/10024/163311.
Informationshanteringsnämndens rekommendation - Finansministeriet (2020:41). Rekommendation för en informationshanteringsmodell. https://julkaisut.valtioneuvosto.fi/handle/10024/162238.
Informationshanteringsnämndens rekommendation - Finansministeriet (2020:65). Rekommendation om bedömning av förändringar i informationshanteringen. https://julkaisut.valtioneuvosto.fi/handle/10024/162432.
Informationshanteringsnämndens rekommendation - Finansministeriet (2021:10). Rekommendation om behandling av säkerhetsklassificerade handlingar. https://julkaisut.valtioneuvosto.fi/handle/10024/162868.
Informationshanteringsnämndens rekommendation - Finansministeriet (2022:6). Hantering av säkerhetsklassificerade handlingar i molntjänster. https://julkaisut.valtioneuvosto.fi/handle/10024/163823.
Informationshanteringsnämndens rekommendation - Finansministeriet (2022:70). Rekommendation om metadata för myndigheternas handlingar i samband med tjänsteproduktion. https://julkaisut.valtioneuvosto.fi/handle/10024/164380.

Anvisningar och annat material

Dataombudsmannens byrå. https://tietosuoja.fi/sv/framsida. Hämtad 16.5.2022.
Myndigheten för digitalisering och befolkningsdata 2022. VAHTI-ordlista om riskhantering i digital verksamhetsmiljö – presentation och introduktion till riskkommunikation 9.6.2022. https://dvv.fi/documents/16079645/110675816/VAHTI-ordlista+om+riskhantering+i+digital+verksamhetsmilj%C3%B6.pdf/aec58883-3c7c-430d-8d3c-658b98bed212/VAHTI-ordlista+om+riskhantering+i+digital+verksamhetsmilj%C3%B6.pdf?t=1674484460823
Riksarkivet 2013. Föreskrifter och anvisningar angående arkivutrymmen. AL/19699/07.01.01.00/2012. https://arkisto.fi/uploads/normit/kunnallishallinto/seulontapaatokset/Foreskrifter%20och%20anvisningar%20om%20arkivutrymmen.pdf. Hämtad 16.5.2022.
Suomen standardisoimisliitto SFS ry 2018. SFS-ISO 27005:2018. Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskien hallinta. SFS - Tietoturvariskit hallintaan standardin ohjeilla. Hämtad 17.10.2022.
Suomen standardisoimisliitto SFS ry 2022. ISO/IEC 27001:2022 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. ISO/IEC 27000 Tietoturvallisuuden standardisarja | SFS. Hämtad 17.10.2022.
Suomen standardisoimisliitto SFS ry 2022. ISO/IEC 27002:2022 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. ISO/IEC 27000 Tietoturvallisuuden standardisarja | SFS. Hämtad 17.10.2022.
Suomen standardisoimisliitto SFS ry 2018. SFS-ISO 31000:2018. Riskienhallinta. Ohjeet. ISO 31000 Riskienhallinta | SFS. Hämtad 17.10.2022.
Terminologicentralen 2018. Kyberturvallisuuden sanasto. Ordlista om cybersäkerhet (TSK 52). Kyberturvallisuuden sanasto (TSK 52) | Sanastokeskus. Hämtad 29.9.2022.
Terminologicentralen 2004. Tiivis tietoturvasanasto. Koncis informationssäkerhetsordlista (TSK 31). Tiivis tietoturvasanasto (TSK 31) | Sanastokeskus. Hämtad 29.9.2022.
Tietotermit 2018. http://urn.fi/URN:NBN:fi:au:tt:t41. Hämtad 2.11.2022.
Traficom. Transport- och kommunikationsverket. Cybersäkerhetscentret. 2022. Krypteringslösningar som godkänns av Traficoms NCSA-verksamhet. https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/ncsa/krypteringslosningar-som-godkanns-av-transport-och-kommunikationsverket | Cybersäkerhetscentret. Hämtad 10.8.2022.
Traficom. Trafik- och kommunikationsverket. Cybersäkerhetscentret 2020. Så här samlar du in och använder loggdata. https://www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/sa-har-samlar-du-och-anvander-loggdata | Cybersäkerhetscentret. Hämtad 17.10.2022.
Traficom. Trafik- och kommunikationsministeriet. Cybersäkerhetscentret 2020. Säkerhetskriterier för molntjänster (PiTuKri). https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Traficom_PiTuKri_2020_SE_210506_WEB.pdf (kyberturvallisuuskeskus.fi). Hämtad 17.10.2022.
Valtiovarainministeriö. Valtiohallinnon tietoturvallisuuden johtoryhmä 2008. Valtiohallinnon tietoturvallisuussanasto. VAHTI 8/2008 Valtionhallinnon tietoturvasanasto | Suomidigi. Hämtad 19.10.2022.
Viestintävirasto. Kyberturvallisuuskeskus 2016. Kiintolevyjen elinkaaren hallinta. Ylikirjoitus ja uusiokäyttö. Ohje-ylikirjoitus.pdf (kyberturvallisuuskeskus.fi). Hämtad 16.5.2022.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

FINANSMINISTERIET
Snellmansgatan 1 A
PB 28, 00023 STATSRÅDET
Telefon 0295 160 01
finansministeriet.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-094-5 (pdf)

Mars 2023