UPPSALA
UNIVERSITET

EXTERN

Att genomföra en informationsklassificering

Vägledning från Säkerhetsavdelningen

Fastställd av Veronika Berglund 2024-12-12

Om Säkerhetsavdelningens råd och rekommendationer

När Säkerhetsavdelningen ger råd och rekommendationer följer dessa i normalfallet allmänna råd/motsv. publicerade av MSB, Säkerhetspolisen, Försvarsmakten eller annan, i sammanhanget relevant, expertmyndighet.
I enskilda sakfrågor kan avdelningens personal också ge råd utifrån egen erfarenhet inom området relaterad till universitetets behov.

Innehåll

Inledning 5
Vilka ska göra informationsklassning och varför? 5
Modell och nivåer för informationsklassificering 6
Att identifiera datatyper/informationstyper 7
Att välja rätt klassningsnivå 7
Angående personuppgifters klassificering 9

Vad används mina KRT-värden till? 10
Referenstabell – standardvärden för olika datatyper/informationstyper 12
Mall för dokumentation och hur den används 15
Exempel på ett forskningsprojekt: 15

Särskilda noteringar (lagrum mm) 17
Information som är av betydelse för Sveriges säkerhet 19
Offentlighets- och sekretesslagen (2009:400) 19
Hantering av strategiska produkter 20
Skyldigheter som följer av avtal 20

Larmkedjan vid Uppsala universitet 21
Larma vid behov 21
Incidentrapportering 21

Säkerhetsavdelningens råd och stöd 23
Webbutbildningar och vägledningar 23

Dokumenthistorik ____ **24**

Inledning

Grunden för en säker hantering av information/data läggs genom att en informationsklassificering genomförs. Det är en aktivitet där skyddsvärdet för informationen/datat bestäms med utgångspunkt från aspekterna konfidentialitet, riktighet och tillgänglighet.

Konfidentialitet	Informationen ska inte göras tillgänglig eller avslöjas för obehöriga personer, system eller processer.
Riktighet	Informationen ska inte förvanskas, manipuleras eller ändras – varken obehörigen, av misstag eller på grund av funktionsstörningar
Tillgänglighet	Informationen ska vara åtkomlig och användbar på förväntat sätt och inom önskad tid.

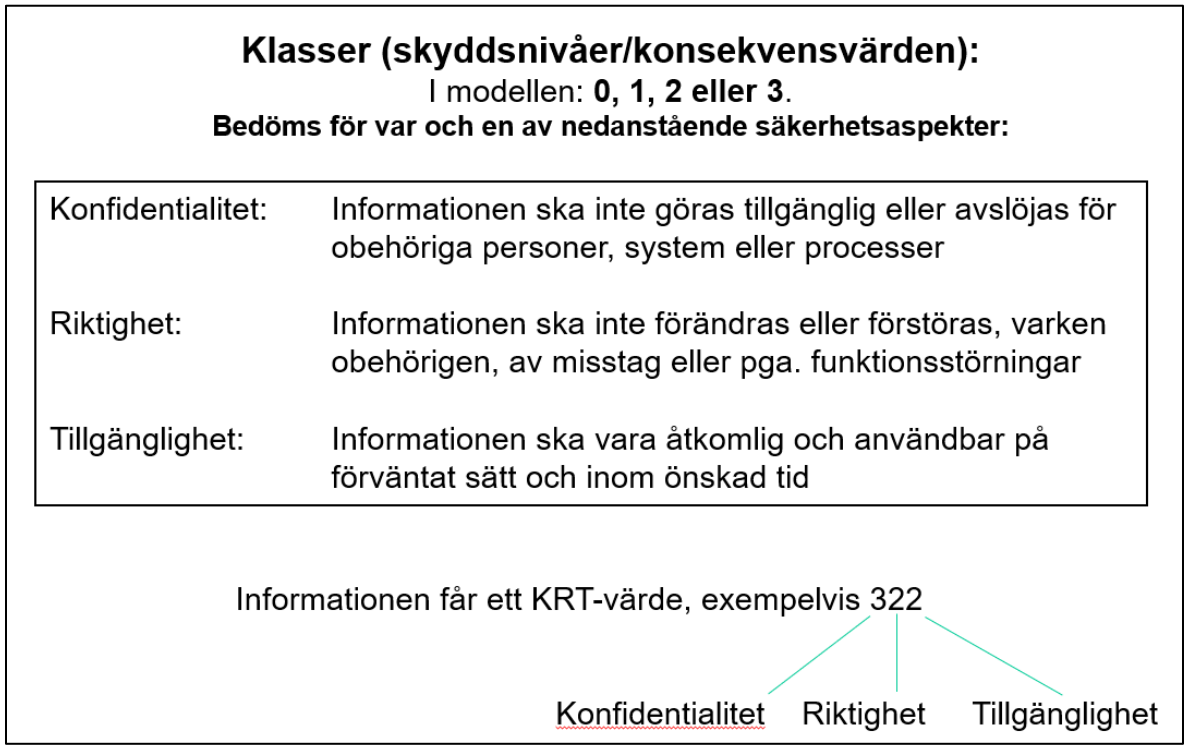
Data/information kan bland annat vara personuppgifter, forskningsdata, ekonomidata eller information som inte är digital, som till exempel papper. Ytterligare exempel kan hämtas ur referenstabellen med standardklassificeringar med olika datatyper/informationstyper i slutet av dokumentet.

Vilka ska göra informationsklassning och varför?

Är du medarbetare som hanterar data/information i ett projekt (till exempel forskningsprojekt eller upphandlingsprojekt) eller i ett specifikt system ska du göra en informationsklassificering för att säkerställa att du hanterar din data/information på ett säkert sätt. Det innebär att bedöma datats/informationens känslighet för att säkerställa att den data/information som du jobbar med lagras och hanteras i system som är tillräckligt säkra för datats/informationens KRT-värde.

Modell och nivåer för informationsklassificering

Skyddsbehovet för ovan nämnda säkerhetsaspekterna konfidentialitet, riktighet och tillgänglighet ska klassificeras i någon av nivåerna 0–3. Klassificeringsvärdet för en informationstyp uttrycks i en treställig sifferkombination, exempelvis 321, där den inledande siffran avser bedömningen för aspekten konfidentialitet, den andra för aspekten riktighet och den tredje för aspekten tillgänglighet. Detta utgör KRT-värde för en datatyp/informationstyp.



Att identifiera datatyper/informationstyper

Det första steget är att identifiera vilka datatyper/informationstyper som du kommer att hantera i ditt projekt, så som forskningsprojekt, eller system. Om det till exempel rör ett forskningsprojekt, kan det underlätta om du tänker utifrån vilka metoder du använder för att samla in data. Om det exempelvis handlar om intervjuer, kan ”intervjudata” vara en lämplig datatyp i informationsklassificeringen. Ytterligare exempel kan hämtas ur referenstabellen med standardklassificeringar med olika datatyper/informationstyper i slutet av dokumentet.

Att välja rätt klassningsnivå

Nästa steg är att hitta rätt klassningsnivå för var och en av de datatyper/informationstyper som du har identifierat. En bra metod för att hitta rätt klassningsnivå för datatyp/informationstyp är att utgå från vilka konsekvenser som kan uppstå när informationen/data:

- Blir tillgänglig eller avslöjas för obehöriga (avsaknad av konfidentialitet)
- Förvanskas, manipuleras eller ändras av obehöriga (avsaknad av riktighet)
- Inte är åtkomlig när man behöver informationen (tillgänglighet)

Välj rätt klassningsnivå för var och en av aspekterna konfidentialitet, riktighet och tillgänglighet med hjälp av nedanstående exempel på konsekvenser som stöd.

Klass 0

- Inga svårigheter för verksamheten eller tredje part att fullfölja sina uppdrag (till exempel att genomföra ett projekt, exempelvis forskningsprojekt).
- Ingen eller försumbar ekonomisk förlust för Uppsala universitet eller tredje part.

Klass 1

- Inga märkbara större svårigheter för verksamheten att fullfölja sina uppdrag (till exempel att genomföra ett projekt, exempelvis forskningsprojekt).
- Enskilda individer, Uppsala universitet eller tredje part kan notera störningen alternativt uppleva lindriga besvär men utan påvisbar ekonomisk påverkan.

- Ingen påverkan på enskild individs integritet.
- Verksamheten (till exempel forskare, TA-personal eller systemägare) klarar sig utan större negativ påverkan att inte få tillgång till informationen under en arbetsdag.

Klass 2

- Verksamheten kan fullfölja sina uppdrag, men med trolig risk för kännbar påverkan (ekonomiskt eller genom att vidta extraordinära åtgärder)
- Tredje part kan påverkas (ekonomiskt i form av exempelvis sanktionsavgifter eller genom att vidta åtgärder).
- Enskilda individer kan påverkas genom till exempel högre arbetsbelastning, merarbete eller stor ekonomisk påverkan.
- Personuppgifter kan spridas och orsaka skada på den personliga integriteten. Om personuppgifter behandlas blir klassningen alltid minst en 2:a vad gäller konfidentialitet och riktighet.
- Uppsala universitets renommé kan påverkas negativt.

Klass 3

- Skapar stora svårigheter för verksamheten, vilket leder till att det blir omöjligt eller nästan omöjligt att fullfölja uppdragen (till exempel att genomföra ett projekt, exempelvis forskningsprojekt).
- Kan resultera i stora ekonomiska förluster för Uppsala universitet eller tredje part, exempelvis i form av stora sanktionsavgifter eller genom att vidta extraordinära åtgärder.
- Individers liv och hälsa/rättigheter äventyras.
- Känsliga personuppgifter kan spridas och orsaka allvarlig skada på den personliga integriteten.
- Kan medföra stor skada på universitetets renommé.

Angående personuppgifters klassificering

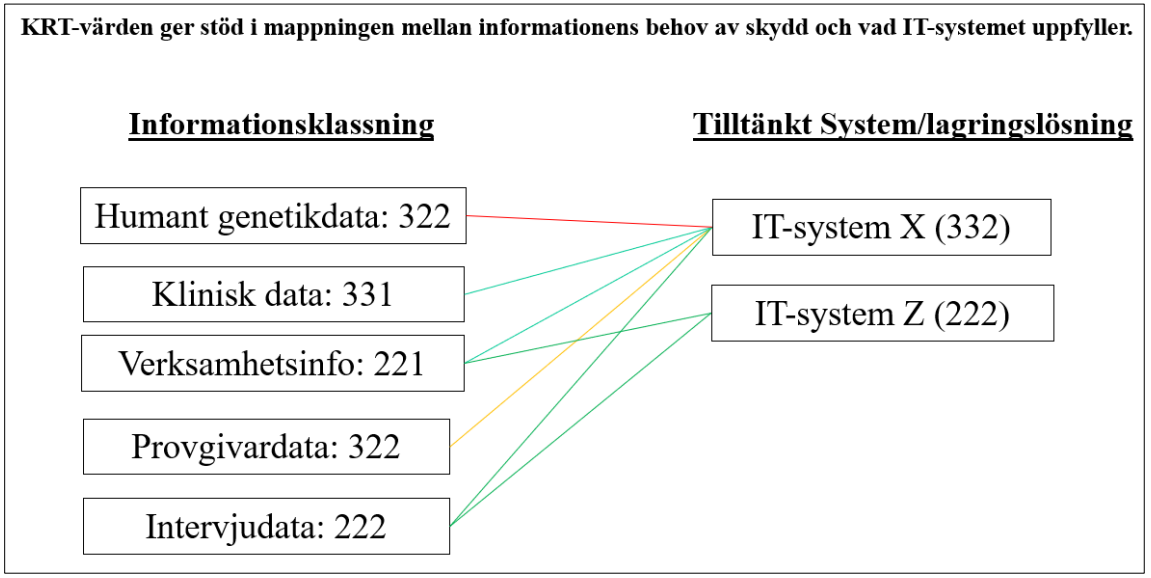
Konfidentialitetsaspekten ska för personuppgifter aldrig klassas lägre än 2, även personuppgifter som är publicerade på webben. I våra system och i vår hantering behöver personuppgifterna ges ett skydd motsvarande klass 2 av följande anledningar:

- En begäran om utlämnande av allmän handling ska alltid föregås av en prövning. En personuppgift kan beläggas med sekretess i samband med denna prövning.
- Om information kommer ut vid sidan av ordinarie utlämningsrutiner, exempelvis genom intrång eller bristande rutiner, kan det skada enskilda individer eller universitetet och resultera i böter.
- Publicering på webben sker i kontrollerad form och är kopplad till tjänsteutövning.

Vad används mina KRT-värden till?

KRT-värden för din data/information behövs för att ta reda på vilka system/lagringslösningar som är tillräckligt säkert för just din data/information. Uppsala universitets centrala system/lagringslösningar är informationsklassificerade med KRT-värden och de ska matcha med KRT-värden för din data/information. Detta gäller även externa och upphandlade system där systemens KRT-värden ska matcha den data/information som ska hanteras i dessa system.

Vid frågor eller funderingar, kontakta security@uu.se



Följande lagringslösningar med aktuellt KRT-värde finns i dagsläget på Uppsala universitet:

Lagringslösning	KRT-värde utan kryptering	KRT-värde med kryptering
Dataportalen Allvis	223	332
Central datalagring (Argos), nivå 1	211	331
Central datalagring (Argos), nivå 2-4	222	332
Tilläggstjänsten Vesta	332	Ingen kryptering behövs
Tilläggstjänsten Bianca (tillhandahålls av UPPMAX)	321	Ingen kryptering behövs
SUNET Box	222	222

Vid frågor om lagringslösningar, kontakta itsupport@uu.se

Referenstabell – standardvärden för olika datatyper/informationstyper

Nedanstående referenstabell innehåller standardvärden för ett antal datatyper/informationstyper som är vanligt förekommande vid Uppsala universitet.

OBS! Nedanstående standard KRT-värden kan användas som vägledning tillsammans med det klassningsstöd som presenterats ovan. En specifik bedömning av KRT-värden behöver dock göras i varje unikt sammanhang.

Datatyp/informationstyp	**KRT-värde**	**Ev. kommentar**
Personuppgifter	221	All slags information som kan knytas direkt till en person som är i livet såsom personnummer, namn, adress, e-postadress etc. Även uppgifter som mer indirekt kan knytas till en person räknas som personuppgift, exempelvis IP-nummer.
Känsliga personuppgifter	321	Definition enligt dataskyddsförordningen: • Ras eller etniskt ursprung • Politiska åsikter • Religiös eller filosofisk övertygelse • Medlemskap i en fackförening • Hälsa • En persons sexualliv eller sexuella läggning • Genetiska uppgifter och • Biometriska uppgifter som entydigt identifierar en person
Klinisk data/patientuppgifter (ej anonymiserade eller pseudonymiserade)	331	
Anonymiserade personuppgifter (även känsliga personuppgifter t.ex. klinisk data/patientuppgifter)	121	Uppgifterna ska vara anonymiserade på ett sätt som omöjliggör att härleda dessa till en identifierad eller identifierbar fysisk person. Ingen nyckel får finnas någonstans i världen.

		Tänk på att ett anonymiserat material i kombination med olika indirekta identifierare, som uppgift om yrke, kommun och ålder, kan i vissa fall identifiera en person. Det går att minska risken genom att till exempel koda om variabler så att ålder och inkomst anges i större intervall och geografisk plats anges i större områden. Vilka indirekta identifierare som behöver kodas om skiftar mellan olika projekt eftersom risken beror på vilken typ av data som samlats in. Om risken inte går att eliminera helt och hanteringen gäller känsliga personuppgifter ska man utgå ifrån standardklassningen för känsliga personuppgifter.
Pseudonymiserade personuppgifter (även känsliga personuppgifter t.ex. klinisk data/patientuppgifter)	221	Behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en unik person utan att kompletterande uppgifter (vanligtvis kodnycklar) används. Informationen räknas som pseudonymiserad under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person. Tänk på att ett pseudonymiserat material i kombination med olika indirekta identifierare, som uppgift om yrke, kommun och ålder, kan i vissa fall identifiera en person. Det går att minska risken genom att till exempel koda om variabler så att ålder och inkomst anges i större intervall och geografisk plats anges i större områden. Vilka indirekta identifierare som behöver kodas om skiftar mellan olika projekt eftersom risken beror på vilken typ av data som samlats in. Om risken inte går att eliminera helt och hanteringen gäller känsliga personuppgifter, utgå ifrån standardklassningen för känsliga personuppgifter. Tänk också på att en inspelad intervju/dialog oftast inte anses som pseudonymiserad, även om personens/personernas namn inte framgår av inspelningen då en individs röst kan kopplas till en unik individ och därmed är en personuppgift. Detta gäller så länge rösten inte förvrängs eller har ändrats på grund av ålder eller andra orsaker.
Pseudonymiseringsnyckel	331	

Personalärenden	221	Exempel: semester, anställningsavtal
Konfidentiella personalärenden	321	Exempel: sjukintyg
Offentlig information i diarium	022	
Sekretessbelagd information	322	
Exportkontrollerad forskning med dubbla användningsområden	221	Länder som bedriver säkerhetshotande verksamhet mot Sverige är intresserade av att olovligen anskaffa forskning som utgör kontrollerad teknik enligt lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd. Sådan forskning behöver därför hanteras med hög säkerhetsmedvetenhet. Viss forskning med dubbla användningsområden omfattas även av sekretess enligt offentlighets- och sekretesslagen (2009:400). Se ”sekretessbelagd information” i denna tabell.
Krigsmateriel	321	Forskning som utgör krigsmateriel eller tekniskt stöd avseende krigsmateriel enligt lagen (1992:1300) om krigsmateriel, omfattas oftast av sekretess enligt offentlighets- och sekretesslagen (2009:400). Sådan forskning kan också utgöra säkerhetsskyddsklassificerad information enligt säkerhetsskyddslagen (2018:585), se rubriken *Information som är av betydelse för Sveriges säkerhet* nedan.
Säkerhetsskyddsklassad information	-	Särskild hantering krävs. Se rubriken *Information som är av betydelse för Sveriges säkerhet* nedan.
Humant/icke humant genetikdata	332	Notera att humant genetikdata inte går att pseudonymisera.
Studentuppgifter	221	
Kursutvärderingar	221	
Undervisningsmaterial	222	
Disciplinärenden	322	
Besöksinformation	211	Information om besökare vid UU.

Ekonomidata	221	
Ritningar (öppna)	021	
Ritningar (skyddade)	321	
IT-systemdokumentation	322	Exempel på IT-systemdokumentation: • Kontinuitetsplan • Kravanalys • Systemkarta • Teknisk dokumentation såsom uppsättning, underhåll, driftrutiner, beroenden, IP-adresser, fysisk placering, behörigheter till systemet, övervakning/larm mm.
Backup		Beroende på klassningen på den information backupen innehåller.
Loggar		Beroende på klassningen på den information som hanteras.

Mall för dokumentation och hur den används

För att underlätta dokumentationen av informationsklassificeringen finns det en färdig mall som du kan använda dig av. Mallen heter UFV 2018-211 Mall Informationsklassificering och du hittar den i regelsamlingen under avsnittet 9 Bilagor Rutiner för riskhantering - informationssäkerhet - Uppsala universitet

Exempel på ett forskningsprojekt:

Vi planerar en kvalitativ studie om upplevelsen av provtagning för canceranalys som uppföljning efter behandling av cellförändringar. Enskilda intervjuer kommer att hållas via Zoom, spelas in på ljudfil och transkriberas till text för innehållsanalys.

Läs mer om kryptering i vägledningen för Lagringslösningar, delning av data och kryptering.

För mer information och få tillgång till de olika centrala lagrings-lösningarna och ange KRT-värde, kontakta itsupport@uu.se

Glöm inte att göra en anmälan om personuppgiftsbehandling om ditt forskningsprojekt ska hantera personuppgifter. Anmälan om personuppgiftsbehandling

ID	Datatyp/ informationstyp	Förklaring	Lagringslösning/IT-tjänst	Roller	KRT värde	Motivering
1	Ljudfiler från genomförda intervjuer	Innehåller känsliga personuppgifter	UU:s centralt erbjudna lagringslösningar (Vesta, Bianca alt. krypterat i Allvis eller Argos). Delas säkert via Cryptshare	Forskare, handledare	321	
2	Transkriberad intervjudata (rådata)	Innehåller känsliga personuppgifter	UU:s centralt erbjudna lagringslösningar (Vesta, Bianca alt. krypterat i Allvis eller Argos). AI-transkriberingsverktyg Whisper. Delas säkert via Cryptshare	Forskare, handledare	321	
3	Transkriberad intervjudata - pseudonymiserad		UU:s centralt erbjudna lagringslösningar Allvis eller Argos	Forskare, handledare	221	Bakvägsidentifiering bedöms vara osannolik.
4	Pseudonymiserings-nyckel/Kodnycklar	Översätter personnummer till kodnummer	Enligt säkerhetsavdelningens rekommendationer	Forskare, handledare	331	
5	Bearbetat forskningsdata	Analys och slutsatser	UU:s centralt erbjudna lagringslösningar Allvis eller Argos	Forskare, handledare	221	Forskningsdata som bearbetas är pseudonymiserad
6	Utkast till artikel före publicering		UU:s centralt erbjudna lagringslösningar Allvis eller Argos	Forskare, handledare	221	
7	Förteckning över deltagare	Grundläggande personuppgifter, som till exempel personnummer, namn, e-post, m.m.	UU:s centralt erbjudna lagringslösningar (Vesta alt. krypterat i Allvis eller Argos)	Forskare, handledare	321	K=3 motiveras utifrån deltagande i känsligt sammanhang
8	Samtyckesblankett	Namn, namnteckning	I pappersform – inlåst. I digital form – se ovan	Forskare, handledare	321	K=3 motiveras utifrån deltagande i känsligt sammanhang

Under den aktiva fasen när känsliga ljudfiler används för transkribering ska Vesta eller Bianca användas. När ljudfiler inte längre används kan de krypteras och lagras i Allvis eller Argos.

Cryptshare ska användas för delning av data/information som har en 3:a på konfidentialitet eller riktighet och Myfiles kan användas för icke-känslig information.

Kodnycklar/pseudonymiseringsnycklar/krypteringsnycklar och kodlistor ska:

- Förvaras separat från den information som den är kopplad till
- Förvaras i så få kopior som möjligt, dock ska minst en säkerhetskopia finnas
- Förvaras i någon form av lösning som uppfyller de krav som faller ut för klassificeringsnivån 332 enligt universitetets metoder för informations-klassificering och kravanalys
- Ska i den lösning som väljs för lagring skyddas med ett starkt lösenord (ska bestå av minst 10 tecken – varav minst en versal, minst en gemen, och antingen minst ett specialtecken eller en siffra.)
- Kommuniceras på ett säkert sätt, endast till behöriga personer

3.4 Regler för säker informationshantering

För information om aspekterna konfidentialitet, riktighet och tillgänglighet samt förekommande klasser se *rutinerna för riskhantering* (UFV 2018/211), se särskilt *Stöd vid informationsklassificering*.

3.4.1 Konfidentialitet

Regler klass 0 och 1

- Informationen får lagras på tjänstedatorn, informationssystem eller flyttbar lagringsmedia utan restriktioner.
  För bedömning om det dessutom är lämpligt att lagra informationen i en molntjänst - se punkten 3.2 *Användning av molntjänster och andra externa informationssystem*, eller kontakta säkerhetsavdelningen för vägledning.
- Informationen får överföras elektroniskt, exempelvis via e-post eller på nätet, utan kryptering.
- Informationen får göras tillgänglig för extern åtkomst.
- Informationen får sändas via post och fax, såväl internt som externt.

Följande regler gäller även för klass 1

- Informationen får lagras i informationssystem som uppfyller kravanalysens klassningsnivå 1 för konfidentialitet.
- Informationen får göras tillgänglig för extern åtkomst genom identifiering av användare.

Regler klass 2

- Informationen får lagras på tjänstedatorn, informationssystem eller flyttbar lagringsmedia under förutsättning att enheten hanteras i enlighet med anvisningar i avsnittet 3.1.1, *Eget ansvar/personligt förhållningssätt.* Därtill får informationen, under vissa förutsättningar, lagras i molntjänst.
  För bedömning om det är lämpligt att lagra informationen i en molntjänst - se punkten 3.2, *Användning av molntjänster och andra externa informationssystem*, eller kontakta säkerhetsavdelningen.
- Informationen får lagras i en lagringslösning som uppfyller kravanalysens klassningsnivå 2 för konfidentialitet.
- Informationen får överföras elektroniskt, exempelvis via e-post eller hemsida, utan kryptering.
- Informationen får sändas via post och fax, såväl internt som externt.

- Vid byte av tjänstedator och flyttbar lagringsmedia ska all information på den avvecklade hårddisken skrivas över på sådant sätt att den inte kan återskapas.

Regler klass 3

- Vid lagring på tjänstedator och extern lagringsmedia, som till exempel USB-minne eller extern hårddisk, ska informationen lagras i krypterad form.
- Informationen ska lagras i informationssystem som uppfyller kravanalysens klassningsnivå 3 för konfidentialitet.
- Informationen ska vid elektronisk överföring, exempelvis via e-post eller hemsida, krypteras innan den överförs internt eller externt.
- Information som ska skickas externt med post ska skickas rekommenderat.
- Utbytt tjänstedator och flyttbar lagringsmedia ska hanteras enligt *rutiner för utrangerad utrustning* (UFV 2014/1279).

3.4.2 Riktighet

Se regler i avsnittet 3.4.1, *Konfidentialitet.* För aspekten riktighet gäller motsvarande regler som för konfidentialitetsaspekten, dock med undantag för destruktionskravet vid utbyte av hårddisk.

3.4.3 Tillgänglighet

Tillgänglighetsaspekten för information som hanteras utanför centrala och lokala system handlar till stor del om säkerhetskopiering. Det innebär att försäkra sig mot informationsförlust då informationen lagras på en tjänstedator alternativt på flyttbar lagringsmedia. I dessa fall ansvarar innehavaren av den aktuella utrustningen att se till att säkerhetskopiering sker med relevant periodicitet och på ett säkert sätt. Detta gäller oavsett hur informationen klassificerats med avseende på tillgänglighet, d.v.s. kravet på säkerhetskopiering gäller lika för klassningsnivåerna 0 till 3.

Särskilda noteringar (lagrum mm)

Information som är av betydelse för Sveriges säkerhet

Säkerhetsskydd handlar om att skydda Sveriges säkerhet mot spioneri, sabotage, terrorism och vissa andra hot. Uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), men som även har betydelse för Sveriges säkerhet, behöver hanteras i enlighet med säkerhetsskyddslagen (2018:585). Uppgifterna kan bland annat handla om nationell samhällsviktig verksamhet, exempelvis infrastruktur för energiförsörjning och kommunikation, eller försvarsverksamhet och totalförsvarsplanering.

Verksamheter som hanterar säkerhetsskyddsklassificerade handlingar ska alltid ha en särskild säkerhetsskyddsplan.
Kontakta Uppsala universitets säkerhetsskyddschef, Fredrik Blomqvist, vid frågor som rör säkerhetsskyddslagen.

Offentlighets- och sekretesslagen (2009:400)

Eftersom Uppsala universitet är en myndighet så är nästan alla informationstillgångar vid Uppsala universitet allmänna handlingar. Visa uppgifter i allmänna handlingar omfattas dock av sekretess enligt offentlighets- och sekretesslagen (2009:400).

Informationen kan hemlighållas enligt offentlighets- och sekretesslagen om den omfattar:

- Rikets säkerhet eller dess förhållande till annan stat eller mellanfolklig organisation
- Rikets centrala finanspolitik, penningpolitik eller valutapolitik
- Myndigheternas verksamhet för inspektion, kontroll eller annan tillsyn
- Intresset att förebygga eller beivra brott
- Det allmännas ekonomiska intresse
- Skyddet för enskilda medborgares personliga eller ekonomiska förhållanden
- Intresset att bevara djur- och växtarter
- Handlingar i ärenden där beslut ännu inte fattats är oftast inte offentliga.

Konfidentialitetsaspekten för information som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400) ska aldrig klassas lägre än 3.

Hantering av strategiska produkter

Strategiska produkter inbegriper krigsmateriel och så kallade produkter med dubbla användningsområden. Produkter med dubbla användningsområden (PDA) är ”produkter, inbegripen programvara och teknik, som kan användas för både civila och militära ändamål, och inbegriper produkter som kan användas för utformning, utveckling, produktion eller användning av kärnvapen, kemiska vapen eller biologiska vapen eller bärare av dessa, inbegripet alla varor som kan användas både för icke-explosiva ändamål och för att på något sätt bidra vid tillverkning av kärnvapen eller andra kärnladdningar”[1]. Vid Uppsala universitet är det främst exportkontroll av PDA som berör verksamheten och då handlar det ofta om att säkerställa att viss kunskap eller information inte sprids till obehöriga.

Här kommer några exempel på forskning som kan utgöra PDA eller krigsmateriel: Artificiell intelligens, robotteknik, halvledare, cybersäkerhet, rymden, försvar, energilagring, kvant- och kärnteknik samt nanoteknik och bioteknik. För mer information se Medarbetaringången, Exportkontroll - Uppsala universitet

Skyldigheter som följer av avtal

Vid informationsklassificering, var särskilt uppmärksam på skyldigheter som följer av ingångna avtal.
Har verksamheten åtagit sig att skydda konfidentiell information som mottagits från en tredje part?
Har verksamheten åtagit sig att hantera informationstillgångar i enlighet med ett annat lands lagstiftning och/eller sanktionsbestämmelser?
Tänk på att ett avtalsbrott kan medföra exempelvis ekonomiska konsekvenser och konsekvenser som kan påverka universitetets renommé negativt. Detta behöver beaktas vid bedömning av klassningsnivåer.

[1] Rådets förordning (EU) 2021/821

Larmkedjan vid Uppsala universitet

Larma vid behov

Uppsala universitets larmnummer är 018-471 2500 och universitetets campusväktare är tillgängliga dygnet runt. Larmkedjan vid universitetet är organiserad enligt nedan.

Fara för liv eller egendom
Händelsen innebär, eller kan innebära, fara för människors liv eller universitetets egendom.

1. Larma 112.
2. Ring därefter larmnumret 018-471 2500, som bemannas av Securitas. Tala om på vilket campusområde/motsvarande du befinner dig, vad som har hänt och begär campusväktare till platsen. Begär även framkoppling till TiB (tjänsteperson i beredskap).
3. Underrätta närmaste chef.

Behov av väktarstöd

1. Ring 018-471 2500.
2. Tala om på vilket campusområde/motsvarande du befinner dig, vad som har hänt och begär campusväktare till platsen.
3. Underrätta närmaste chef.

Incidentrapportering

I händelse av en arbetsmiljörelaterad incident anmäls denna via universitetets incidentrapporteringssystem (IA-systemet) enligt anvisningar på Medarbetaringången.

Säkerhetsincident är ett samlingsnamn för IT-säkerhets-, cybersäkerhets-, informationssäkerhets- och personuppgiftsincidenter.
Exempel på säkerhetsincidenter är:

- Nätfiske (phising), bedrägeriförsök och annan misstänkt e-post
- Intrångsförsök på din dator
- Lösenord som kommit på avvägar
- Personuppgifter som kan ha hanterats fel, spridits mm
- Virus eller annan skadlig kod (malware, ransomware)
- Falska webbsidor
- Överbelastningsattacker

Om du upptäcker en säkerhetsincident meddelar du snarast din närmaste chef samt mailar till security@uu.se om att det har skett en incident och kortfattat redogör vad som har hänt. Säkerhetsavdelningen tar emot meddelandet, gör en första bedömning och meddelar incidentmanager på avdelningen för universitetsgemensam IT (UIT).

Säkerhetsavdelningens råd och stöd

Ansvarig chef har huvudansvaret för arbetsmiljön vid institutionen/motsv. Därför är det i första hand ansvarig chef som bör kontakta Säkerhetsavdelningen om det finns ett behov av råd gällande säkerhetsaspekter. I ett senare skede, eller efter det att ärendet är avslutat, kan det vara aktuellt att titta på händelsen mer övergripande. Samverkan är viktigt för att ge kraft åt varandra under hanteringen av en händelse. Vidare, genom att fundera kring erfarenheter och lärdomar så bygger vi kunskap som kan underlätta hanteringen av framtida incidenter.

Kontakt med Säkerhetsavdelningen sker företrädelsevis genom att maila security@uu.se.

Webbutbildningar och vägledningar

För ytterligare råd och stöd hänvisas Uppsala universitets medarbetare till Medarbetaringången där webbutbildningar och vägledningar från Säkerhetsavdelningen publiceras.

Författare

Namn Jenny Jonasson och Samantha Tinet

Enheten för informationssäkerhet

Dokumenthistorik

2024-10-28	Skapad	JJ, ST
2024-11-14	Granskad	VB
2024-11-14	Uppdaterad	JJ, ST
2024-12-1	Fastställd	VB