UMEÅ UNIVERSITET

VÄGLEDNING

INFORMATIONSKLASSNING

Typ av dokument:	*Vägledning*
Datum:	
Dnr:	
Beslutad av:	
Giltighetstid:	*Tills vidare*
Område:	
Ansvarig förvaltningsenhet:	*Universitetsledningens kansli*
Ersätter dokument:	*Rekommendationer informationsklassning, IT-enheten (2015-03-30)*

UMEÅ UNIVERSITET

Innehåll

UMEÅ UNIVERSITET

1. Beskrivning

Dokumentet innehåller klassificeringsmodell med konsekvensnivåer för säkerhetsaspekterna Konfidentialitet, Riktighet, Tillgänglighet som gäller vid Umeå universitet. Bilaga till dokumentet utgörs av det verktyg som myndigheten för samhällsskydd och beredskap (MSB) tillhandahåller för att dokumentera resultatet av genomförd klassning. Universitetet hänvisar till två (2) dokument (Excel) för dokumentation av genomförd klassning; ett för forskningsprojekt och ett för verksamhetssystem (t.ex. centrala it-system) eller it-tjänster. Bilagorna med verktyget återfinns i Aurora under Informationssäkerhet och rubriken Styrande dokument.

2. Bakgrund

Syftet med att klassificera informationen med avseende på säkerhetsaspekterna Konfidentialitet, Riktighet, Tillgänglighet är att bedöma och fastställa kraven på hur universitets information och berörda informationssystem ska hanteras med avseende på säkerhetsåtgärder. Klassning av informationstillgångar innebär att klassa organisationens information och de resurser som hanterar informationen i olika nivåer utifrån den konsekvens otillräckligt skydd ger. Viss information är mer skyddsvärd än annan. Till exempel förekommer sekretessbelagda handlingar/uppgifter vilka har andra krav på hantering än allmänna handlingar. Behovet av skydd skiljer sig därför åt mellan olika information, och varierar dessutom beroende på situation (se användningsområden). Ansvar och roller kopplade till informationssäkerhet och informationsklassning beskrivs i *Regel- Säker informationshantering*.

Ifall informationstillgångarna som ska klassas består både av information och av de resurser som används för att hantera den informationen, så är det själva informationen som är den primära tillgången och därmed det som ska klassas i första hand.

Resurser som används för att hantera informationen, till exempel IT-system, IT-infrastruktur och fysiska tillgångar ska möta kraven som klassningen medför. De resurser som hanterar informationen behöver därför skyddas på lägst den nivå som högst klassad information har.

3. Användningsområden

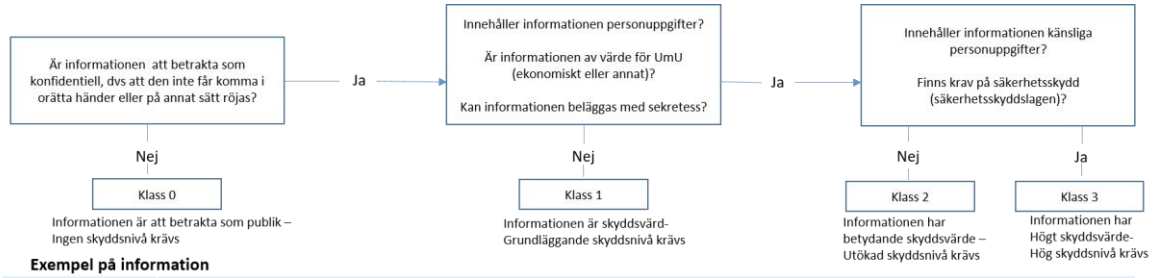
Tillfällen när informationsklassning bör ligga till grund för val av lämpliga skyddsåtgärder är:

- Inför personuppgiftsbehandlingar
- Bedömning hur forskningsmaterial/data ska hanteras och därmed skyddas
- Nulägesbedömning och/eller riskanalys genomförs av ett informationssystem
- Anskaffning, nyutveckling eller förändring av IT-system eller infrastruktur, t.ex. datalagringstjänster
- Fastställande av säkerhetsdesign av ett informationssystem
- Förändringar av rättsliga krav
- Nytillkommen information i verksamheten
- Fastställande av hanteringsregler av information, t.ex. med avseende på krav på kryptering av e-post, regler för kommunikation via mobiltelefon, etc.

UMEÅ UNIVERSITET

Nedanstående klassningsmodell är baserad på Umeå universitets informationssäkerhetspolicy, IT-säkerhetsplan, Dataskyddsförordningen (EU 2016/679), MSB:s föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet (MSB FS2016:1) samt det metodstöd för informationssäkerhet som tillhandahålls av MSB.

Konfidentialitet (K)



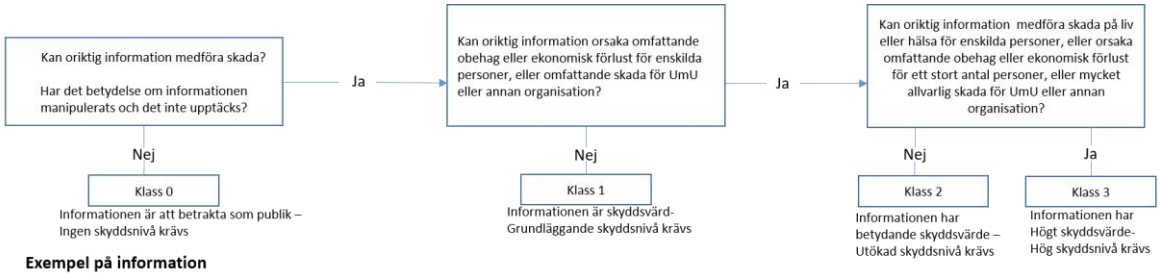
Exempel på information

Klass 0	Information som presenteras publikt på UmUs webb, allmän handling som inte faller under sekretess
Klass 1	Intern information som inte innehåller personuppgifter och inte faller under sekretess
Klass 2	Personuppgifter (allt som kan kopplas till en person), loggar, forskningsmaterial/data/dokumentation
Klass 3	Känsliga personuppgifter eller information kopplad till person med skyddad identitet, lösenord, kryptonycklar, brandväggsregler, eller särskilt känslig forskningsmaterial/data/dokumentation, lagöverträdelser
Kommentar:	Personuppgifter kan klassas i klass 3 om de är så kallade integritetskänsliga personuppgifter. Dit hör t.ex. information som rör någons privata sfär, uppgifter om social förhållanden, värderande uppgifter

Möjliga konsekvenser av brister/röjande

Klass 0	Inga konsekvenser
Klass 1	**Måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Enstaka missnöjda samarbetspartners, uttryck i sociala medier. Lindrig förtroendeskada
Klass 2	**Betydande** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Begränsat missnöje, uttryckt i riks- och lokalmedia. Betydande förtroendeskada.
Klass 3	**Allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Flertalet missnöjda samarbetspartners, drev i riksmedier el sociala grupper. Allvarlig förtroendeskada

Riktighet (R)



Exempel på information

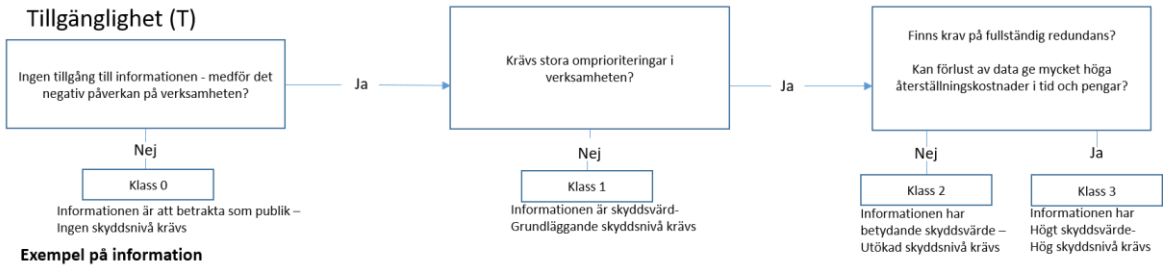
Klass 0	-
Klass 1	Allmän information till externa användare, inter/extern kommunikation via epost
Klass 2	Forskningsmaterial, studentuppgifter grund – och forskarutbildning, personalärenden, loggar
Klass 3	Särskilt känslig forskningsmaterial/data/dokumentation, lösenord, kryptonycklar, brandväggsregler

Möjliga konsekvenser av brister/röjande

Klass 0	Inga konsekvenser
Klass 1	**Måttligt** obehag eller begränsad ekonomisk förlust enskild individ, eller begränsad skada på egen eller annan organisation.
Klass 2	**Betydande** obehag eller ekonomisk förlust för enskilda personer, eller omfattande skada på egen eller annan organisation.
Klass 3	**Allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ, eller orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer. Kan medföra skada på liv eller hälsa för enskilda personer.

UMEÅ UNIVERSITET

Tillgänglighet (T)



Exempel på information

Klass 0	-
Klass 1	Personalärenden, ekonomidata, lönelistor, loggar
Klass 2	Universitetets diarium
Klass 3	Nationella system, till exempel Ladok

Möjliga konsekvenser av brister/röjande

Klass 0	Inga konsekvenser
Klass 1	**Måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Enstaka missnöjda samarbetspartners. Måttligt produktionsbortfall
Klass 2	**Betydande** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Begränsat missnöje. Stort produktionsbortfall.
Klass 3	**Allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Flertalet missnöjda samarbetspartners. Mycket stort produktionsbortfall.

4. Genomför klassning

Steg 1. Definiera klassningsobjektens information

Det första steget handlar om att inventera klassningsobjektets information, och om att dela upp informationen i meningsfulla mängder. Ibland kan det vara svårt att veta vilken **detaljeringsgrad** man behöver ha när man definierar informationsmängder. Grundregeln är då att det som ska utgöra en informationsmängd är **den minsta sammansatta grupperingen av information som hanteras i klassningsobjektet**

Exempel: Om ett system skapar en pdf-fil med ett visst innehåll, som aldrig delas upp i mindre informationsmängder, så kan pdf-filen betraktas som en informationsmängd.

För att underlätta inventeringen kan man också tänka i termer av var organisationens, verksamhetens eller ett IT-systems information hanteras – tänk – input, bearbetning, lagring och output.

Deltagare från verksamheten bör tillsammans ha kunskap om vilken information som finns i klassningsobjektet. För detta kan man använda tidigare kartläggningar.

Skriv in den inventerade informationen i kolumnerna *Informationsmängd* och *Beskrivning/innehåll* i metodstödets tillhörande Verktyg Använda informationsklassning.

UMEÅ UNIVERSITET

Steg 2. Klassa informationen

Att klassa informationsmängder innebär att man gör en konsekvensbedömning för vad som kan hända om informationens konfidentialitet, riktighet och tillgänglighet inte upprätthålls i den utsträckning verksamheten behöver.

Exempel på frågor man kan ställa sig:

- *Konfidentialitet*: Vad kan konsekvenserna bli ifall informationen läcker ut till obehöriga?
- *Riktighet*: Vad kan konsekvenserna bli ifall informationen är felaktig eller inaktuell?
- *Tillgänglighet*: Vad kan konsekvenserna bli ifall någon (som är behörig) inte får tillgång till informationen?

Använd specifikation av de olika konsekvensnivåerna som finns angivna i klassningsmodellen som stöd vid konsekvensbedömningen. Se utifrån samtliga konsekvenskategorier ni beslutat att använda er av.

Inventera nu externa och interna krav för varje inventerad informationsmängd. Ibland kan man härleda en del av konsekvensbedömningen till specifika interna eller externa krav. Det kan vara exempelvis lagar, föreskrifter, avtal, kundkrav, krav i produktionskedjan och liknande. Kraven kan gälla både för hela klassningsobjektet, och för hela organisationen. Därför är det vanligt att ett och samma krav återkommer för olika informationsmängder.

Skriv in de interna och externa kraven under respektive kolumn för varje informationsmängd. För detta kan man med fördel använda metodstödets tillhörande *verktyg Använda Informationsklassning*.

Klassning av informationsmängder genererar en viss klassningsprofil. En viss informationsmängd kan exempelvis vara mycket kritisk när det gäller tillgänglighet och konfidentialitet, men mindre känslig när det gäller riktighet. En sådan informationsmängd kan då få klassningsprofilen K2-R1-T3.

Klassningen av varje informationsmängd för varje aspekt förs in i respektive kolumn direkt i *verktyget Använda Informationsklassning*.

Varje delmängd ska klassas. Konceptet här är ”högst vinner”, det vill säga för en informationsmängd som består av flera delmängder där varje delmängd blir olika klassad så ska det värde som är högst vara det som är beslutande. Exempel med delmängderna personuppgifter, mätdata och löneuppgifter skulle kunna vara

Informationstyp	**K**	**R**	**T**
Personuppgifter	**2**	1	1
Mätdata	1	1	**3**
Löneuppgifter	1	1	1
Totalt	2	1	3

Det betyder att de resurser (IT-system eller IT-tjänster) som hanterar informationen behöver skyddas på lägst den nivå som högst klassad information har.

Steg 3. Ta fram en bruttolista på säkerhetsåtgärder

Resultatet ska bli en bruttolista på säkerhetsåtgärder som ska vara införda för att den klassade informationstillgången ska ha rätt skydd utifrån vald konsekvensnivå.

Detta steg kan vara olika besvärligt för olika roller på universitetet som helhet och rekommendationen är att **diskutera detta steg med IT-säkerhetskunniga på ITS**. Ett grundtips är att medarbetare i till exempel forskningsprojekt eller i annan för universitetet fortlöpande verksamhet mest troligt endast behöver känna till hur information får hanteras som är kopplad till *konfidentialitet*.

Vissa säkerhetsåtgärder åligger verksamhetsansvariga, informationsägare och systemägare, till exempel behörighetsstyrning och rutin för kontinuitetsplanering (*Tillgänglighet*).

Steg 4. Utför kompletterande riskanalys

I det fall aktuellt klassningsobjekt sedan tidigare har fastställda säkerhetsåtgärder men ska användas i ett nytt sammanhang kan man behöva göra precisering för att avgöra lämpligheten av säkerhetsåtgärderna som har identifierats i steg 3.

Det kan vara så att specifik lagstiftning kan ställa höga krav eller skyddet av informationstillgången behöver höjas, eller att nya förhållanden kan göra att utvalda säkerhetsåtgärder är otillräckliga, överskyddande, eller på annat sätt olämpliga. Ibland kan man upptäcka att föreslagna säkerhetsåtgärder är onödiga eller medför omotiverade kostnader. För att avgöra det behövs en kompletterande riskanalys för att hitta den lösning som passar.

Steg 5. Fastställ nettolista på säkerhetsåtgärder

Den justering som gjorts av skyddsnivån, utifrån hänsyn till de lokala risker som informationstillgången utsätts för och andra interna och externa krav, så skapas en nettolista som beskriver skyddsnivån för den specifika informationstillgången.

Nettolistan är ett underlag för hur organisationen ska hantera informationstillgången sett till förmåga och effekt i säkerhetsåtgärderna och andra specifika hanteringsregler.

De säkerhetsåtgärder som inte finns på plats, eller som inte motsvarar den nivå som krävs ska skrivas in i en handlingsplan för att åtgärdas**.**

5. Referenstabell för skyddsvärd information

Nedanstående referenstabell innehåller standardvärden för ett antal informationstyper som är vanligt förekommande vid universitetet. Angivna skyddsvärden ska ses som riktvärden. En specifik informationsklassificering (bedömning av skyddsvärde) behöver göras i varje unikt sammanhang – nedanstående bedömningar kan användas som vägledning tillsammans med det klassningsstöd som presenterats ovan

UMEÅ UNIVERSITET

Beteckning	**Skydds-värde**	**kommentar**
Personuppgifter	Betydande	All slags information som kan knytas direkt till en person som är i livet såsom personnummer, namn, adress etc. Även uppgifter som mer indirekt kan knytas till en person räknas som personuppgift, exempelvis IP-nummer
Känsliga personuppgifter	Högt	• ras eller etniskt ursprung • politiska åsikter • religiös eller filosofisk övertygelse • medlemskap i en fackförening • hälsouppgifter • en persons sexualliv eller sexuella läggning • genetiska uppgifter och • biometriska uppgifter som entydigt identifierar en person
Lagöverträdelser	Högt	
Patientuppgifter (ex studenthälsan)	Högt	
Anonymiserade personuppgifter (patientuppgifter)	Skyddsvärt	Uppgifterna ska vara anonymiserade på ett sätt som omöjliggör att härleda dessa till en unik person. Ingen nyckel får finnas någonstans i världen.
Pseudonymiserade personuppgifter (klinisk data/patientuppgifter)	Skyddsvärt	Säker nyckelhantering utgör ett absolut krav
Pseudonymiseringsnyckel	Högt	
Personalärenden	Betydande	Exempel: Sjukskrivningar
Integritetskänsliga personuppgifter	Högt	