Instruktion för genomförande av informationsklassificering

Innehållsförteckning

[1 Instruktion 2](#_Toc473553178)

[1.1 Syfte 2](#_Toc473553179)

[1.2 Användningsområden 2](#_Toc473553180)

[1.3 Genomförande 2](#_Toc473553181)

[1.4 Skyddsvärda och verksamhetskritiska system 3](#_Toc473553182)

[2 Beskrivning av säkerhetsklasserna 4](#_Toc473553183)

[2.1 Konfidentialitet (sekretess) 4](#_Toc473553184)

[2.2 Riktighet 5](#_Toc473553185)

[2.3 Tillgänglighet 6](#_Toc473553186)

[3 Mall för dokumentation av klassificeringen 7](#_Toc473553187)

# 1 Instruktion

## 1.1 Syfte

Syftet med att klassificera informationen med avseende på säkerhetsaspekterna *Konfidentialitet*, *Riktighet* och *Tillgänglighet* är att bedöma och fastställa kraven på hur universitets information och berörda informationssystem ska hanteras med avseende på gällande *Riktlinjer för säkerhetsarbetet vid Uppsala universitet – Informationssäkerhet*.

## 1.2 Användningsområden

Konkreta användningsområden där en informationsklassificering bör ligga till grund för val av lämpliga skyddsåtgärder är:

* Riskhantering av informationssystem eller systemförvaltningsobjekt enligt universitetets *Riktlinjer för riskanalyser av informationssystem*
* Kravställning/kravspecificering inför systemutveckling eller upphandling av system
* Fastställande av säkerhetsdesign av ett informationssystem
* Fastställande av hanteringsregler av information, t.ex. med avseende på krav på kryptering av e-post, regler för och eventuell märkning av intern och extern post, kommunikation via mobiltelefon etc.

## 1.3 Genomförande

Behovet av säkerhet (skyddsbehovet) för information anges i någon av säkerhetsklasserna: *Publik, Basnivå, Hög nivå*eller *Särskilda krav* och klassificeringen görs med utgångspunkt från omfattningen av de konsekvenser som kan uppkomma vid brister i skyddet. Publik information avser information nedladdad från internet, allmänt tillgänglig text eller bild etc. och lämnas därför utan åtgärd vid en informationsklassificering.

Följande steg rekommenderas för genomförande av en informationsklassificering

1. Studera tabellerna i avsnitt **2. Beskrivning av säkerhetsklasserna** nedan för att få en övergripande förståelse för hur säkerhetsklasserna *Basnivå*, *Hög nivå* och *Särskilda krav* är definierade för de fyra säkerhetsaspekterna: *Konfidentialitet*, *Riktighet* och *Tillgänglighet*.
2. Använd strukturen i avsnitt **3. Mall för dokumentation av klassificeringen** nedan och diskutera var och en av de fyra säkerhetsaspekterna med avseende på vilka säkerhetsklasser som är relevanta för den information som hanteras av den informationsresurs (system, förvaltningsobjekt, projekt etc.) som informationsklassificeringen avser.
3. Dokumentera på avsedda platser i mallen och kommentera gärna skälen till bedömningarna på sista sidan.

## 1.4 Skyddsvärda och verksamhetskritiska system

Särskilda skyddsåtgärder för skyddsvärda och verksamhetskritiska system finns angivna i bilaga 2 till Riktlinjer för riskhantering av informationssystem.

Skyddsvärda system - system som hanterar information som klassificeras som **Hög nivå** eller **Särskilda krav** avseende **Konfidentialitet.**

Verksamhetskritiska system - system som hanterar information som klassificeras som **Hög nivå** eller **Särskilda krav** avseende **Tillgänglighet.**

**Skyddsvärda system** är system som omfattas av lagar och förordningar som OSL och PUL och därför behöver ett starkt skydd mot att informationen görs tillgänglig för obehöriga personer, system eller processer för att motverka möjliga konsekvenser som skulle kunna bli mycket allvarliga för enskilda personer, universitetet eller tredje part.

Exempel på skyddsvärda system i universitetets verksamhet är system som hanterar skyddade identiteter och adresser, sekretesskyddad information, starkt integritetskänslig information (t.ex. sjukdomsuppgifter), särskilt känslig forskningsinformation (företagshemligheter), ritningar över lokaler där känslig verksamhet bedrivs eller värdefulla tillgångar förvaras, upphandlingsinformation etc.

**Verksamhetskritiska system** är system eller IT-tjänster som är av mycket stor betydelse för universitetets kärnverksamhet och därför behöver ett skydd som möjliggör att informationen är åtkomlig och användbar på förväntat sätt och inom önskad tid för att motverka möjliga konsekvenser som skulle kunna få mycket allvarliga konsekvenser för enskilda personer, universitetet eller tredje part.

Exempel på verksamhetskritiska system universitetets externa webbsidor, Outlook för e-post och kalender, de delar av Studentportalen som studenter behöver för att fullgöra sina studier (tider, lokaler etc.) samt katalog- och inloggningstjänster (DNS, DHCP, CAS, AKKA etc) och andra gemensamma tjänster som är av mycket stor betydelse för utnyttjandet av samtliga IT-tjänster på universitetet.

# 2 Beskrivning av säkerhetsklasserna

## 2.1 Konfidentialitet (sekretess)

Behovet av skydd mot att informationen görs tillgänglig eller avslöjas för obehöriga personer, system eller processer.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Säkerhets- klass** | **Allmän beskrivning** | **Exempel på information** | **Exempel på skydd** | **Möjliga konsekvenser av brister** |
| **Basnivå** | Information som behöver skydd mot oavsiktlig eller obehörig åtkomst. Information som avsiktligt görs tillgänglig för allmänheten. | Merparten information vid universitetet (arbetsmaterial, men även allmänna handlingar) ingår i basnivån. | Informationen ska vara skyddad mot oavsiktlig eller obehörig åtkomst genom inloggning, eller genom inlåsning eller på annat sätt skyddad förvaring.  Offentlig information ska vara tillgänglig på ett kontrollerat sätt. | Brister i skyddet kan medföra obehag eller begränsad ekonomisk förlust för enskilda personer, eller begränsad skada för universitetet eller tredje part. |
| **Hög nivå** | Information som behöver ett starkt skydd mot oavsiktlig eller obehörig åtkomst, inklusive information som omfattas av sekretess. | Sekretesskyddad information, starkt integritetskänslig information (till exempel information om sjukdom) | Informationen ska vara skyddad genom kvalificerad kryptering, inlåsning i väl skyddat skåp eller på annat motsvarande sätt. | Brister i skyddet kan orsaka omfattande obehag eller ekonomisk förlust för enskilda personer, eller omfattande skada för universitetet eller tredje part. |
| **Särskilda krav (kan avse en eller flera aspekter av sekretessskydd)** | Information som behöver ett särskilt starkt skydd mot oavsiktlig eller obehörig åtkomst, inklusive skydd mot kvalificerade angrepp avsedda att komma åt informationen. | Skyddade identiteter eller adresser. Särskilt känslig forskningsinformation (företagshemligheter e.d.).  Information som omfattas av försvarssekretess. | Mycket kvalificerat skydd mot obehörig eller oavsiktlig åtkomst. Skydd mot kvalificerade angrepp avsedda att komma åt informationen ska finnas. | Brister i skyddet kan medföra skada på liv eller hälsa för enskilda personer, eller orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer, eller mycket allvarligt skada för universitetet eller tredje part. |

## 2.2 Riktighet

Behovet av skydd mot att informationen förändras eller förstöras – obehörigen, av misstag eller på grund av funktionsstörningar.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Behov av säkerhet** | **Allmän beskrivning** | **Exempel på information** | **Exempel på skydd** | **Möjliga konsekvenser av brister** |
| **Basnivå** | Information som behöver ett grundläggande skydd mot att förändras eller förstöras. | Merparten information vid universitetet (arbetsmaterial och allmänna handlingar) ingår i basnivån. | Informationen ska vara skyddad – genom säkerhetskopiering, noggrann testning av program, skyddad förvaring, signatur på dokument e.d. – mot oavsiktlig eller obehörig förändring eller förstöring. | Brister i skyddet kan medföra obehag eller begränsad ekonomisk förlust för enskilda personer, eller begränsad skada för universitetet eller tredje part. |
| **Hög nivå** | Information som behöver ett starkt skydd mot att förändras eller förstöras. | Beslut och annan information som har ”rättsverkan” eller som har stor betydelse för universitetet eller enskilda.  Bokföringsmaterial, information i bokförings- och redovisningssystem, listor med tentamensresultat.  Forskningsdata med stor vetenskaplig eller ekonomisk betydelse. | Informationen ska vara väl skyddad  – genom loggning av förändringar, digitala signaturer, manuella signaturer, noggranna hanteringsrutiner e.d. – mot oavsiktlig eller obehörig förändring eller förstöring. | Brister i skyddet kan orsaka omfattande obehag eller ekonomisk förlust för enskilda personer, eller omfattande skada för universitetet eller tredje part. |
| **Särskilda krav (kan avse en eller flera aspekter av skydd av riktighet)** | Information som behöver ett särskilt starkt skydd mot att förändras eller förstöras. | Original till avhandlingar. Ladok- databasens tabeller över personer och deras studieresultat.  Avtalsoriginal. | Mycket kvalificerat skydd mot oavsiktlig och obehörig förändring, till exempel genom användning av certifikatbaserade digitala signaturer och kontrollsummor. Särskilt utformade rutiner för säkerhets-kopiering och loggning av förändringar. | Brister i skyddet kan medföra skada på liv eller hälsa för enskilda personer, eller orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer, eller mycket allvarligt skada för universitetet eller tredje part. |

## 2.3 Tillgänglighet

Behovet av skydd som möjliggör att informationen är åtkomlig och användbar på förväntat sätt och inom önskad tid.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Behov av säkerhet** | **Allmän beskrivning** | **Exempel på information** | **Exempel på skydd** | **Möjliga konsekvenser** |
| **Basnivå** | Information som normalt ska vara tillgänglig dygnet runt (eller vid särskilt beslutade tider), men där enstaka avbrott upp till en halv arbetsdag endast medför begränsad skada. | Merparten information vid universitetet (arbetsmaterial och allmänna handlingar av i första hand internt intresse) ryms inom basnivån. | Informationen ska helst vara tillgänglig hela dygnet. Avbrott i tillgängligheten under kontorstid ska normalt vara i högst 4 timmar.  Informationens tillgänglighet ska möjliggöras genom stabila och väl testade IT-system, och fungerande stödrutiner. | Brister i tillgängligheten kan medföra obehag eller begränsad ekonomisk förlust för enskilda personer, eller begränsad skada för universitetet eller tredje part. |
| **Hög nivå** | Information som ska vara tillgänglig dygnet runt (eller vid särskilt beslutade tider) utan avbrott. Enstaka kortare avbrott medför endast begränsad skada. | Universitetets externa webbsidor. Information som studenter behöver för att fullgöra studier eller tentamina (t.ex. information om tider och lokaler). Gemensamma mailsystem. Information på filservrar. Allmänna handlingar av stort intresse för allmänheten. | Informationen ska vara tillgänglig under hela dygnet. Avbrott i tillgängligheten ska normal vara i högst 0,5 timmar. Planerade avbrott ska vara aviserade i god tid. | Brister i tillgängligheten kan orsaka omfattande obehag eller ekonomisk förlust för enskilda personer, eller omfattande skada för universitetet eller tredje part. |
| **Särskilda krav (kan avse en eller flera aspekter av tillgänglighet)** | Information som måste vara tillgänglig dygnet runt (eller vid särskilt beslutade tider) utan avbrott, och där även kortare avbrott kan orsaka stor skada. | Katalog- och inloggningstjänster (informationen i dessa). DNS, DHCP och andra tjänster av mycket stor betydelse för utnyttjandet av samtliga IT-tjänster vid universitetet. | Redundanta system och andra åtgärder för att möjliggöra i princip obruten åtkomst trots mycket allvarliga störningar (redundanta system i olika lokaler etc.). | Brister i tillgängligheten kan medföra skada på liv eller hälsa för enskilda personer, eller orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer, eller mycket allvarligt skada för universitetet eller tredje part. |

# 3 Mall för dokumentation av klassificeringen

|  |  |
| --- | --- |
| Informationresurs (*förvaltnings-objekt, informationssystem, projekt etc*.) |  |
| Datum |  |
| Deltagare |  |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |
| --- | --- |
| Vilken information hanteras av aktuell informationsresurs? |  |

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Konfidentialitet (sekretess)**

Skyddsmål: Informationen ska inte göras tillgänglig eller avslöjas för obehöriga personer, system eller processer.

|  |  |  |
| --- | --- | --- |
| **Nivå** | **Finns** | **Exempel på information tillhörig denna nivå** |
| Basnivå |  |  |
| Hög nivå |  |  |
| Särskilda krav |  |  |
| Ange de särskilda kraven: | |  |

**Riktighet (integritet)**

Skyddsmål: Informationen ska inte förändras eller förstöras, varken obehörigen, av misstag eller på grund av funktionsstörningar.

|  |  |  |
| --- | --- | --- |
| **Nivå** | **Finns** | **Exempel på information tillhörig denna nivå** |
| Basnivå |  |  |
| Hög nivå |  |  |
| Särskilda krav |  |  |
| Ange de särskilda kraven: | |  |

**Tillgänglighet**

Skyddsmål: Informationen ska vara åtkomlig och användbar på förväntat sätt och inom önskad tid.

|  |  |  |
| --- | --- | --- |
| **Nivå** | **Finns** | **Exempel på information tillhörig denna nivå** |
| Basnivå |  |  |
| Hög nivå |  |  |
| Särskilda krav |  |  |
| Ange de särskilda kraven: | |  |

**Sammanfattning**

|  |  |  |  |
| --- | --- | --- | --- |
| **Säkerhetsaspekt** | **Basnivå** | **Hög nivå** | **Särskilda krav** |
| Konfidentialitet (sekretess) |  |  |  |
| Riktighet (integritet) |  |  |  |
| Tillgänglighet |  |  |  |

**Kommentarer till bedömningarna**

|  |  |
| --- | --- |
| **#** | **Kommentar** |
|  |  |