Stockholms universitet

Rektor

BESLUT
2017-01-26 Dnr SU FV-2.11.2-1923-16

Handläggare:
Benita Falenius
Informationssäkerhetssamordnare
IT-avdelningen

Riktlinjer för informationssäkerhet vid Stockholms universitet

Stockholms universitet

Innehållsförteckning

1. Inledning 4
   1.1. Syfte 4
   1.2. Ansvar 5
   1.3. Centralt stöd 5
   1.4. Utvärdering och uppföljning 5
   1.5. Styrdokument 6
2. Verksamhetsanalys inklusive risk- och sårbarhetsanalys 6
   2.1. Syfte 6
   2.2. Ansvar 7
   2.3. Aktiviteter 7
   2.4. Process för verksamhetsanalys 9
3. Säkerhetskategorier med där tillhörande säkerhetsåtgärder 9
   3.1. Anskaffning, utveckling och underhåll av system 10
   3.2. Åtkomststyrning 10
   3.3. Driftsäkerhet 11
   3.4. Kommunikationssäkerhet 11
   3.5. Leverantörsrelationer 12
4. Incidenthantering 12
   4.1. Syfte 12
   4.2. Ansvar 13
   4.3. Definition 13
   4.4. Identifiering, rapportering och hantering av incidenter 13
   4.5. Eskalering av incidenter för information 13
   4.6. Analys av incidenter 14
5. Kontinuitet vid allvarlig händelse och avbrott 14
   5.1. Syfte 14
   5.2. Ansvar 14
   5.3. Kontinuitetsplan 15

Stockholms universitet

5.4. Krisplan 16
Bilaga 1: Detaljerad process för verksamhetsanalys inkl. risk- och sårbarhetsanalys 17
Bilaga 2: Säkerhetskategorier med där tillhörande säkerhetsåtgärder 19

Stockholms universitet

1. Inledning

Informationssäkerhet – *Ett tillstånd som innebär skydd med avseende på konfidentialitet, tillgänglighet, riktighet och spårbarhet hos information*.

Information och tillhörande informationsteknik är en ytterst viktig strategisk resurs för verksamheten vid Stockholms universitet. Genom att ha en god informationssäkerhet tryggas den information som är viktig för universitetet. Arbetet med informationssäkerhet går ut på att skydda informationstillgångar (tillgångar som är relaterade till information och informationsbehandlingsresurser) mot olika typer av hot.

En förutsättning för ett strukturerat arbete med informationssäkerhet är att det finns en förteckning över informationstillgångarna och dess ägare samt att gällande lagar och regelverk efterlevs. Detta säkras genom en verksamhetsanalys som inkluderar en risk- och sårbarhetsanalys.

Informationssäkerhetsarbetet baseras på etablerade standarder. I dessa finns ett antal säkerhetskategorier som ska fungera som stöd i informationssäkerhetsarbetet. Arbetet med dessa säkerhetskategorier är en del av verksamhetsanalysen. Varje organisation gör en bedömning av vilka säkerhetskategorier som är relevanta för deras verksamhet och som ska ligga till grund för arbetet med informationssäkerhet. I informationssäkerhetsarbetet ingår också incidenthantering och kontinuitetsplanering vid allvarlig händelse och avbrott.

Hur arbetet med verksamhetsanalys, säkerhetskategorier, incidenthantering och kontinuitetsplanering ska genomföras beskrivs nedan.

Vad gäller den fysiska säkerheten, hänvisas till *Riktlinjer för fysisk säkerhet*.

1.1. Syfte

Bristande informationssäkerhet kan få både allvarliga och direkta konsekvenser för såväl medarbetare som studenter som för universitetet i stort. Universitetet hanterar idag en mängd information av stor betydelse. Denna information behöver kunna skyddas mot obehörig åtkomst (*skydd av informationens konfidentialitet*) men behöver även vara tillgänglig för behöriga när den ska användas (*skydd av informationens tillgänglighet*). I vissa fall är behovet av tillgänglighet så högt att några avbrott i praktiken inte är acceptabla. Informationen behöver även skyddas mot obehöriga förändringar (*skydd av informationens riktighet*). För att säkerställa att dessa behov upprätthålls är det av grundläggande betydelse att det i efterhand går att spåra vem som har gjort vad i universitetets system (*skydd av informationens spårbarhet*) - något som även befintlig lagstiftning ställer krav på.

Stockholms universitet

1.2. Ansvar

Rektor har det övergripande ansvaret för informationssäkerheten vid Stockholms universitet.

Förvaltningschefen beslutar i ärenden rörande universitetets säkerhet, inklusive informationssäkerhet. Förvaltningschefen har emellertid delegerat beslutanderätten i frågor rörande universitetets it-säkerhet och ansvar för samordning av och rådgivning kring universitetets arbete med informationssäkerhet till chefen för IT-avdelningen. Dock ska ärenden av principiell karaktär avgöras av förvaltningschefen.

Vid varje institution/motsvarande[1] är prefekten/motsvarande[2] ansvarig för informationssäkerheten. Prefekten ska tillse att anvisningar och rutiner finns inom den egna organisationen och att dessa bl.a. baseras på säkerhetskategorierna och där tillhörande säkerhetsåtgärder. I de fall institutionen använder centrala it-tjänster ansvarar chefen för IT-avdelningen för att anvisningar och rutiner finns.

Varje medarbetare är skyldig att upprätthålla tillräcklig nivå av informationssäkerhet samt att påpeka brister i informationssäkerheten till överordnad chef.

Alla anställda, studenter, besökare och samarbetspartners ska följa de lagar, regler, föreskrifter och riktlinjer som gäller för universitetet.

1.3. Centralt stöd

För att ge institutioner stöd och vägledning i frågor som berör informationssäkerhet finns vid IT-avdelningen en central informationssäkerhetsfunktion. Funktionens roll är att vara rådgivande mot all verksamhet vid Stockholms universitet och kan t.ex. bidra med rådgivning vid framtagande av anvisningar och rutiner samt delta i arbetet med de verksamhetsanalyser som är en del i informationssäkerhetsarbetet. Informationssäkerhetsfunktionen ska kontinuerligt planera, utbilda, stödja, utvärdera och förbättra informationssäkerhetsarbetet vid universitetet.

1.4. Utvärdering och uppföljning

IT-avdelningen ska varje år göra en universitetsövergripande sammanställning av de tillgångar och risker som rör information och informationsteknik. Utvärdering och uppföljning av arbetet med informationssäkerhet sker utifrån arbetet med säkerhetskategorierna och

[1] Med institution avses fortsättningsvis även centrum och institut som är på samma organisatoriska nivå som institutioner samt avdelningar inom universitetsförvaltningen.
[2] Med prefekt avses fortsättningsvis även föreståndare för centrum och institut som är på samma organisatoriska nivå som institutioner samt avdelningschefer inom universitetsförvaltningen.

Stockholms universitet

säkerhetsåtgärderna. Baserat på detta beräknas sedan key risk indicators (KRI), vilka visar den allmänna risknivån vid institutionen och vid universitetet som helhet. Denna beräkning utförs av IT-avdelningen.

1.5. Styrdokument

Riktlinjer för informationssäkerhet är ett av universitetets styrdokument och kompletteras med underliggande anvisningar och rutiner. Riktlinjerna konkretiserar universitetets säkerhetspolicy och ska skapa förutsättningar för ett systematiskt informationssäkerhetsarbete vid universitetet. De baseras på nedanstående förordningar, föreskrifter och standarder.

- SFS 2015:1052 Förordning om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap
- MSBFS 2016:1 Föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet
- MSBFS 2016:2 Föreskrifter och allmänna råd om statliga myndigheters rapportering av IT-incidenter
- SS-ISO/IEC 27001:2014
- SS-ISO/IEC 27002:2014
- SS/ISO 22301:2012

2. Verksamhetsanalys inklusive risk- och sårbarhetsanalys

2.1. Syfte

Verksamhetsanalysen ska leda till en strukturerad förteckning över informationstillgångarna och dess ägare samt säkra att gällande lagar och regelverk[3] efterlevs. I förteckningen ska de för verksamheten viktigaste informationstillgångarna klassificeras utifrån förmågan att upprätthålla *konfidentialitet, riktighet, tillgänglighet* och *spårbarhet*.

Risk- och sårbarhetsanalysen ska ge god insikt i lokala hot och risker samt bidra till att ge en aggregerad bild av riskerna inom informationssäkerhetsområdet och av behoven av säkerhetsåtgärder på universitetsövergripande nivå. Analysen kan med fördel vara en del av den årliga processen för verksamhetsplanering, då de risker som man vill eliminera kan medföra en kostnad och då även ska kunna beaktas i den årliga budgetprocessen.

[3] Offentlighets- och sekretesslag, Personuppgiftslag, Arkivlag, Arkivförordning, Riksarkivets föreskrifter och allmänna råd om elektroniska handlingar m.fl.

Stockholms universitet

Verksamhetsanalysen definierar tillsammans med risk- och sårbarhetsanalysen det skyddsbehov verksamhetens informationstillgångar har.

2.2. Ansvar

Prefekten ansvarar för genomförandet av en verksamhetsanalys inklusive risk- och sårbarhetsanalys. IT-avdelningen stödjer via informationssäkerhetsfunktionen prefekter vid genomförandet av analysen.

2.3. Aktiviteter

Verksamhetsanalysen är en sammansatt analys bestående av följande aktiviteter:

- *Inventering av de för verksamheten viktigaste informationstillgångarna samt dess ägare*
  Inventering av informationstillgångar syftar till att identifiera för verksamheten viktiga tillgångar och stödjande resurser. Även informationstillgångens ägare ska vara identifierad. Exempel på viktiga tillgångar är forskningsinformation, utbildningsmaterial, underlag inför tentamina och administrativ information såsom olika avtal och budgetar.
- *Informationsklassificering*
  Informationsklassificering syftar till att värdera identifierade informationstillgångar utifrån förmågan att upprätthålla konfidentialitet, riktighet, tillgänglighet och spårbarhet. Mot bakgrund av klassificeringen ska tillgångar ges en lämplig nivå av säkerhetsåtgärder, t.ex. ska upphandlingsunderlag behandlas med konfidentialitet tills ett tilldelningsbeslut är förmedlat.
- *Risk- och sårbarhetsanalys för identifiering av risker mot informationstillgångarna samt riskernas konsekvenser och sannolikheten att de uppträder*

  Risk- och sårbarhetsanalysen syftar till:

  - att identifiera och bedöma risker, på en skala från 1 – 4, utifrån vilka konsekvenser de har för verksamheten och hur stor sannolikheten är för att de uppträder
  - att prioritera i vilken ordning risker ska hanteras och åtgärder vidtas
  - att involvera intressenter när beslut om hantering av risker fattas och hålla dem informerade om status för riskhanteringen och dess verkan
  - att regelbundet övervaka och granska risker och riskhanteringsprocessen
  - att utbilda chefer och personal vid institutionen om riskerna och de åtgärder som vidtas för att hantera dem
  - att samla in information för att identifiera universitetsgemensamma och universitetsövergripande risker

Stockholms universitet

- *Inventering av legala krav och verksamhetskrav*
  Inventering av legala krav och verksamhetskrav syftar till att identifiera alla interna och externa krav som rör verksamheten och dess hantering av informationstillgångar. Externa krav är alla relevanta legala krav såsom t.ex. personuppgiftslag (1998:204), offentlighets- och sekretesslag (2009:400) m.fl. Interna krav är universitetets interna regler som finns upptagna i universitetets Regelbok.
- *Beaktande av säkerhetskategorier och dess säkerhetsåtgärder*
  Vad gäller säkerhetskategorierna så finns det ett antal rekommenderade säkerhetsåtgärder som ska vara beaktade (se kapitel 3). Dessa kategorier och åtgärder, som baseras på etablerade standarder, är sådana som universitetet bedömer som relevanta för universitetet som helhet. Informationstillgångarnas ägare behöver ta ställning till huruvida de är relevanta för den egna verksamheten. De säkerhetsåtgärder som bedöms som relevanta graderas utifrån i vilken grad de är genomförda. Målet är att de säkerhetsåtgärder som bedöms relevanta ska vara genomförda till 100 procent och att det därmed är säkerställt att nödvändiga anvisningar och rutiner finns. De åtgärder som är relevanta men inte genomförda ska finnas med i åtgärdsplanen. Bedömningen av i vilken grad en åtgärd är genomförd görs av tillgångens ägare.

  Säkerhetskategorierna är:

  - anskaffning, utveckling och underhåll av system
  - åtkomststyrning
  - driftsäkerhet
  - kommunikationssäkerhet
  - leverantörsrelationer

Verksamhetsanalysen ska resultera i en rapport som visar status samt de åtgärder man avser att vidta. Institutioner ska uppdatera verksamhetsanalysen med lämplig periodicitet dock minst vartannat år. Verksamhetsanalysen genomförs med fördel med stöd av IT-avdelningen.

Risk- och sårbarhetsanalyser ska genomföras vid följande tillfällen:

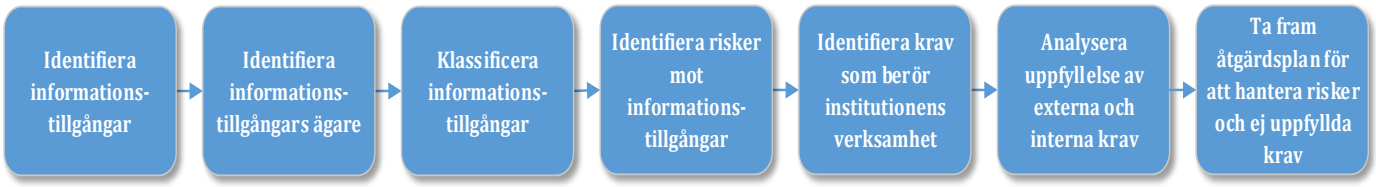
- i samband med större verksamhetsförändringar (t.ex. organisationsförändring eller flytt)
- inför upphandling av molntjänster
- inför tecknandet av personuppgiftsbiträdesavtal med extern leverantör

Genomförandet av en verksamhetsanalys varierar i omfattning och ska anpassas utifrån dess syfte. Normal tidsåtgång är ca 3 timmar. Tidsåtgången för att enbart göra en risk- och sårbarhetsanalys är ca 1 timme.

Stockholms universitet

2.4. Process för verksamhetsanalys

Då det är av största vikt för hela Stockholms universitet att vidmakthålla en god informationssäkerhet är det viktigt att riktlinjerna i detta dokument efterlevs. För att underlätta ett systematiskt informationssäkerhetsarbete är en vägledande process framtagen.



Syftet med denna process är att tillhandahålla en gemensam arbetsgång för att uppnå ett systematiskt informationssäkerhetsarbete. Processen utförs alltid utifrån institutionens perspektiv. För en mer detaljerad beskrivning av processen se bilaga 1.

3. Säkerhetskategorier med där tillhörande säkerhetsåtgärder

Som nämnts ovan är arbetet med säkerhetskategorierna en del av verksamhetsanalysen. I de etablerade standarder som informationssäkerhetsarbetet baseras på finns ett stort antal säkerhetskategorier som fungerar som stöd i informationssäkerhetsarbetet. Säkerhetskategorierna är av olika relevans beroende på verksamhet. Stockholms universitet har identifierat fem säkerhetskategorier som är väsentliga för universitetets verksamhet: *Anskaffning, utveckling och underhåll av system*, *Åtkomststyrning*, *Driftsäkerhet*, *Kommunikationssäkerhet* och *Leverantörsrelationer*.

Till varje säkerhetskategori finns rekommenderade säkerhetsåtgärder. Beroende på verksamhet kan säkerhetsåtgärderna från några eller alla säkerhetskategorier vara relevanta. Därför ska varje institution identifiera relevanta säkerhetsåtgärder för den egna verksamheten. Arbetet med säkerhetskategorierna innefattar val, införande och förvaltning av säkerhetsåtgärder med hänsyn tagen till de risker som finns avseende universitetets informationssäkerhet. Informationstillgångarnas ägare behöver ta ställning till huruvida säkerhetsåtgärderna är beaktade och säkerställa att det finns anvisningar och rutiner.

Informationssäkerhetskraven och åtgärderna ska i omfattning återspegla det bedömda värdet av informationen och den negativa påverkan på verksamheten som brist på tillräcklig säkerhet kan leda till, dvs. om bedömning görs att bristande säkerhet kan få stora konsekvenser för verksamheten ska informationssäkerhetskraven vara högt ställda och åtgärderna mer omfattande än om bedömningen är att bristande säkerhet inte får så stora konsekvenser. För att identifiera vilka risker som finns samt bedöma riskernas konsekvenser och sannolikheten att de uppstår ska en risk- och sårbarhetsanalys genomföras.

Stockholms universitet

I de fall institutionen använder centrala it-tjänster är det chefen för IT-avdelningen som är ansvarig för identifiering av riskerna och arbetet med säkerhetsåtgärderna.

3.1. Anskaffning, utveckling och underhåll av system

3.1.1 Syfte

Syftet med denna säkerhetskategori är att säkerställa att informationssäkerhet är en integrerad del av informationssystemet[4] över hela dess livscykel, under utveckling, uppbyggnad, test, drift och avveckling.

3.1.2 Ansvar

Prefekten ansvarar för anskaffning, utveckling och underhåll av it- tjänster vid institutionen. Inför ett sådant beslut ska en dialog föras med IT-avdelningen och Ekonomiavdelningen. En risk- och sårbarhetsanalys ska också genomföras, med fördel med stöd av IT-avdelningen.

I de fall institutionen använder universitetets centrala it-tjänster ansvarar chefen för IT-avdelningen för anskaffning, utveckling och underhåll av it-tjänsterna.

3.1.3 Säkerhetsåtgärder

Det finns ett antal säkerhetsåtgärder som rör anskaffning, utveckling och underhåll av system, bl.a. att dokumentera rutiner avseende krav som rör informationssäkerhet för nya informationssystem eller förbättringar av befintliga informationssystem samt att dokumentera rutiner avseende utveckling av program och system. En lista med samtliga åtgärder finns i bilaga 2.

3.2. Åtkomststyrning

3.2.1 Syfte

Åtkomststyrning syftar till att säkerställa att endast behöriga användare har åtkomst till information och informationsbehandlingsresurser. Regler för styrning av åtkomst ska upprättas, dokumenteras och följas upp utifrån verksamhets- och informationssäkerhetskrav. Tillgångens ägare ska fastställa lämpliga regler för styrning av åtkomst, rättigheter och begränsningar för specifika roller. Detaljrikedomen och kraven i säkerhetsåtgärderna ska avspegla de säkerhetsrisker som är förknippade med informationen. Åtkomstkontroller är både logiska och fysiska och dessa ska beaktas tillsammans. Användare och tjänsteleverantörer ska ges tydliga besked om vilka verksamhetsmässiga krav som ska uppfyllas genom åtkomstkontroller.

---

[4] Ett informationssystem eller it-system definieras ofta som ett system som ger it-stöd och används för att samla in, lagra, bearbeta och distribuera information för en domän och därigenom stödjer kommunikation och arbete inom och mellan organisationer.

Stockholms universitet

3.2.2. Ansvar
Prefekten ansvarar för åtkomststyrning till information och it-miljö vid institutionen. IT-avdelningen agerar stöd för att säkra god åtkomststyrning.

I de fall institutionen använder universitetets centrala it-tjänster ansvarar chefen för IT-avdelningen för åtkomststyrningen. Chefen för IT-avdelningen ansvarar för gemensam teknisk it-infrastruktur och dess åtkomststyrning.

3.2.3 Säkerhetsåtgärder
Exempel på säkerhetsåtgärder som rör åtkomststyrning är granskning av användares åtkomsträttigheter, dokumenterade rutiner för aktuella åtkomsträttigheter och system för lösenordshantering. En lista med samtliga åtgärder finns i bilaga 2.

3.3. Driftsäkerhet

3.3.1. Syfte
Syftet med säkerhetskategorin driftsäkerhet är att säkerställa att en relevant nivå av driftsäkerhet upprätthålls när det gäller drift av informationsbehandlings- och kommunikationsresurser (it-resurser som är bärare av information och som används för överföring av data).

3.3.2. Ansvar
Prefekten ansvarar för driftsäkerhet rörande it-miljö vid institutionen. IT-avdelningen agerar stöd för att säkra god driftsäkerhet.

I de fall institutionen använder universitetets centrala it-tjänster ansvarar chefen för IT-avdelningen för driftsäkerheten. Chefen för IT-avdelningen ansvarar för driftsäkerheten i den centrala it-miljön.

3.3.3. Säkerhetsåtgärder
Dokumenterade rutiner ska finnas för t.ex. drift av informationsbehandlings- och kommunikationsresurser, såsom uppstarts- och nedtagningsrutiner, säkerhetskopiering, underhåll av utrustning, hantering av media, datahall samt hantering av e-post och säkerhet. En lista med samtliga åtgärder finns i bilaga 2.

3.4. Kommunikationssäkerhet

3.4.1. Syfte
Säkerhetsåtgärder för kommunikationssäkerhet syftar till att säkerställa skyddet av information i nätverk och skydda anslutna tjänster.

3.4.2. Ansvar
Prefekten ansvarar för styrning av kommunikationssäkerhet vid institutionen. IT-avdelningen agerar stöd för att säkra god kommunikationssäkerhet.

Stockholms universitet

I de fall institutionen använder universitetets centrala it-tjänster ansvarar chefen för IT-avdelningen för kommunikationssäkerheten i dessa.

3.4.3. Säkerhetsåtgärder
Det finns ett antal säkerhetsåtgärder som rör kommunikationssäkerhet. Exempelvis ska det finnas dokumenterade rutiner för hantering och styrning av nätverk och dokumenterade rutiner för vilka krav som ska ingå i avtal. En lista med samtliga åtgärder finns i bilaga 2.

3.5. Leverantörsrelationer

3.5.1. Syfte
Syftet med säkerhetskategorin leverantörsrelationer är att säkerställa skydd av de informationstillgångar som leverantörer har åtkomst till.

3.5.2. Ansvar
Prefekten ansvarar för de leverantörsrelationer som är unika och aktuella vid institutionen.

Chefen för IT-avdelningen ansvarar för leverantörsrelationer som är universitetsövergripande.

3.5.3. Säkerhetsåtgärder
Informationssäkerhetsåtgärder ska identifieras och fastställas i ett regelverk för att specifikt hantera leverantörers åtkomst till verksamhetens information. Dessa säkerhetsåtgärder ska adressera både processer och rutiner inom den egna verksamheten, men också leverantörens processer och rutiner.

Exempel på en säkerhetsåtgärd, som rör leverantörsrelationer, avser verifiering av leverantörens tjänsteleverans, vilket innebär att det ska finnas dokumenterade rutiner för att säkra detta. En lista med samtliga åtgärder finns i bilaga 2.

4. Incidenthantering

4.1. Syfte

Syftet med incidenthanteringen är att:

- synliggöra risker och vidta åtgärder mot bakgrund av inträffade negativa händelser och tillbud i verksamheten
- minska negativ påverkan på verksamheten och stärka motståndsförmågan samt förebygga att incidenter inträffar
- ge stöd vid prioritering
- ge underlag för ökat medvetande om vikten av incidenthantering
- ge underlag för beslut om verksamhetsförändring och tillhörande styrande dokument

Stockholms universitet

4.2. Ansvar

Prefekten ansvarar för incidenthanteringen vid institutionen. IT-avdelningen agerar stöd för att säkra bra rutiner för incidenthantering.

Chefen för IT-avdelningen ansvarar för samordning av inrapporterade informationssäkerhetsincidenter.

Alla anställda, studenter samt personer som arbetar på uppdrag av Stockholms universitet ska rapportera incidenter som rör informationssäkerhet. Rutinerna ska därför vara beskrivna och förmedlade på ett lämpligt sätt.

4.3. Definition

En incident är en händelse (eller ett tillbud) som kan få negativ påverkan på Stockholms universitets verksamhet. En incident kan vara resultatet av en avsiktlig handling eller något som skett utan uppsåt. Den gemensamma nämnaren är att verksamheten hotas t.ex. genom otillåten hantering av information, driftavbrott, brand, stöld etc.

4.4. Identifiering, rapportering och hantering av incidenter

Det är viktigt att det inom verksamheten finns god kännedom om vilka åtgärder som ska vidtas och hur incidenter och tillbud ska rapporteras vid universitetet. För att säkerställa att eventuella incidenter får minimal påverkan på universitetets verksamhet ska det finnas en formaliserad process för rapportering och hantering av incidenter. Det ska genom denna process säkerställas att incidenter och tillbud blir rapporterade på ett sådant sätt att lämpliga åtgärder kan vidtas både på kort och på lång sikt.

Alla anställda, uppdragstagare och tredjepartsanvändare ska notera och rapportera observerade eller misstänkta incidenter. Är incidenten av mer känslig karaktär kan rapportering ske direkt till IT-avdelningen per telefon. IT-incidenter som rör de centrala it-tjänsterna rapporteras via Serviceportalen. Om lokal incidenthantering föreligger ska det finnas processer och rutiner för detta och IT-avdelningen ska ha kännedom om hur dessa incidenter hanteras för att kunna få en samlad bild av universitetets totala mängd incidenter.

Incidenter ska hanteras med nödvändig skyndsamhet så att universitetets informationstillgångar inte skadas.

4.5. Eskalering av incidenter för information

Vid incidenter som bedöms kunna få stor påverkan på universitetets verksamhet (vid osäkerhet – kontakta IT-avdelningen) ska även IT-avdelningen omgående erhålla information om detta genom att e-post skickas till infosakfunktionen@su.se. E-post som skickas till denna adress hanteras med stor konfidentialitet och endast ett begränsat antal personer vid universitetet har tillgång till informationen. Det går även bra att kontakta IT-avdelningen per

telefon. Chefen för IT-avdelningen ansvarar för att berörda informeras om incidenten, dess påverkan och konsekvens samt om vilka åtgärder som vidtagits. Chefen för IT-avdelningen ansvarar också för att universitetsledningen erhåller nödvändig information.

Enligt regeringsbeslut ska, fr.o.m. april 2016, statliga myndigheter under regeringen rapportera it-incidenter som allvarligt påverkar säkerheten till Myndigheten för samhällsskydd och beredskap. Detta för att ge en bättre överblick över de hot som förekommer på nationell nivå. IT-avdelningen rapporterar in it-säkerhetsincidenterna och är universitetets kontakt gentemot Myndigheten för samhällsskydd och beredskap. Detta innebär att IT-avdelningen omgående ska kontaktas, via infosakfunktionen@su.se eller via telefon, när en it-säkerhetsincident har inträffat. IT-avdelningen är ett stöd vid bedömning huruvida rapportering ska ske eller ej.

Om institutionen överlåter en del av sin informationshantering till en icke statlig aktör ska institutionen i överlåtelseavtalet se till att motparten åtar sig att rapportera it-incidenter till institutionen. Institutionen ska utan dröjsmål vidarebefordra informationen till IT-avdelningen.

4.6. Analys av incidenter

Alla ärenden som klassificeras som incidenter ska efter hantering analyseras med avseende på orsak och verkan. Detta då det kan finnas ett samband mellan olika incidenter som inte är direkt synligt. Ett antal mindre incidenter kan tillsammans visa på omfattande säkerhetsbrister som är svåra att identifiera utan en genomgående analys.

5. Kontinuitet vid allvarlig händelse och avbrott

5.1. Syfte

Kontinuitetsplanering handlar om att minska universitetets sårbarhet och öka motståndskraften mot olika händelser som kan påverka den verksamhet som bedöms som kritisk. Universitetet är enligt MSBFS 2016:1 Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet skyldigt att kontinuitetsplanera, varför risk- och sårbarhetsanalysen är väsentlig.

5.2. Ansvar

Kontinuitet kan delas in i tre delar:

- verksamhetsrelaterad kontinuitetsplan (BCM, Business continuity management)
- it-inriktad kontinuitetsplan (ITSCM, IT service continuity management)
- krisplan

Förvaltningschefen ansvarar för universitetets kontinuitetsplanering (BCM) inklusive all krisplanering.

Prefekten ansvarar för it-inriktad kontinuitetsplanering (ITSCM) vid institutioner med egen it-miljö.

Chefen för IT-avdelningen ansvarar för it-inriktad kontinuitetsplanering (ITSCM) i den centrala it-miljön, liksom för att den it-inriktade processen för kontinuitetsplaneringen är kommunicerad till berörda, att den är ändamålsenlig och att anvisningar/rutiner är tillgängliga.

Chefen för Tekniska avdelningen samordnar universitetets krisplan och krisorganisation. From den 1 januari 2017 ansvarar chefen för Fastighetsavdelningen att samordningen sker.

5.3. Kontinuitetsplan

En klassificering ska göras av vilka verksamheter och tjänster som är mest verksamhetskritiska. Detta kan ske med stöd av IT-avdelningen. Kontinuitetshanteringen ska identifiera och hantera risker som kan leda till allvarliga störningar eller avbrott i leveransen av dessa verksamheter och tjänster. Verksamheterna och tjänsterna ska kunna återställas snarast möjligt så att verksamheten påverkas minimalt. Kontinuitetshanteringen ska även hantera ett snabbt förändrat behov av resurser och kapacitet i befintliga verksamheter och tjänster på grund av följdverkningar av avbrott och störningar.

Kontinuitetshanteringen är en kontinuerlig process som inbegriper att:

Planera

- analysera vilka verksamheter och tjänster som är kritiska för verksamheten
- identifiera och analysera risker som kan hota eller störa verksamheter och tjänster
- ta fram lösningar för att undvika störningar eller minimera konsekvenserna

Genomföra

- införa lösningar för att undvika risker och där tillhörande konsekvenser
- fördela ansvar
- ta fram kontinuitetsplan med rutiner för att hantera störningar
- informera och utbilda
- testa och införa kontinuitetsplanen

Följa upp

- följa upp hur planen fungerar

- analysera inträffade störningar och incidenter

Förbättra

- förnya sårbarhetsanalysen
- ändra tekniska, administrativa och organisatoriska lösningar och rutiner
- förbättra planen

5.4. Krisplan

Syftet med en krisplan vid universitetet är att skapa handlingsberedskap för en sammanhållen och tydlig central krisledning och att utveckla rutiner för insatser vid allvarliga händelser.

Prefekten måste veta hur krisplanen för universitet fungerar i stort och vad som förväntas av denne i en krissituation. Detta innebär att varje institution måste upprätta en åtgärdsplan för hantering av olika krissituationer som kan uppstå.

Det är av stor vikt att samtlig personal känner till åtgärdsplanen och vem som ska kontaktas i händelse av kris.

Krisplanen aktiveras av förvaltningschefen när en allvarlig händelse drabbar universitetet.

Stockholms universitet

Bilaga 1: Detaljerad process för verksamhetsanalys inkl. risk- och sårbarhetsanalys

1. Identifiera informationstillgångar
    - Indata: Organisationsinformation och potentiella informationstillgångar
    - Identifiera de viktigaste informationstillgångarna
    - Resultat: Tillgångskarta (T.ex. forskningsinformation, system, utbildningsmaterial, personuppgifter)

2. Identifiera informationstillgångars ägare
    - Indata: Tillgångskarta
    - Identifiera ägare och ansvar utifrån tillgångskarta
    - Resultat: Kartlagt ägarskap och ansvar (Exempel på ägare är prefekt, administrativ chef, objektägare)

3. Klassificera informationstillgångar
    - Indata: Tillgångskarta, ägarskap
    - Klassificera tillgångar utifrån egenskaperna *konfidentialitet*, *tillgänglighet*, *riktighet* och *spårbarhet*
    - Resultat: Klassificerade informationstillgångar

4. Identifiera risker mot informationstillgångar
    - Indata: Tillgångskarta, ägarskap och klassificering
    - Identifiera och klassificera risker utifrån sannolikhet och konsekvens. Eskalera vid behov risker med hög sannolikhet och konsekvens till högre ledning
    - Resultat: Riskkarta (Exempel på risk är obehörigt intrång och förstörande av forskningsdata)

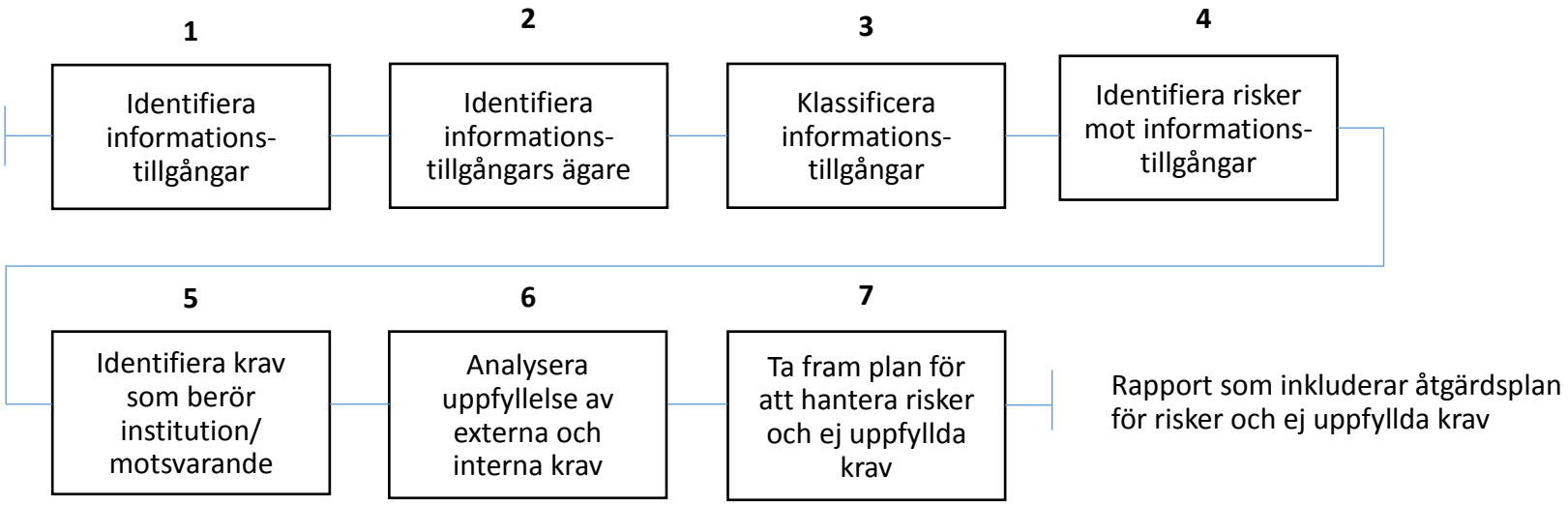
5. Identifiera krav som berör institutionens verksamhet
    - Indata: Externa och interna krav
    - Identifiera legala krav
    - Resultat: Applicerbara externa och interna krav (Exempel på krav är PUL)

6. Analysera uppfyllelse av externa och interna krav
    - Indata: Applicerbara interna och externa krav. Tillgångskarta
    - Analysera utifrån åtgärder för respektive säkerhetskategori i nr 3.1 – 3.5 enligt Riktlinjer för informationssäkerhet
    - Analysera utifrån externa krav
    - Säkerställ att IT-avdelningens informationssäkerhetsfunktion informeras om resultatet
    - Resultat: Analys av uppfyllelse av interna och externa krav

7. Ta fram åtgärdsplan för att hantera risker och ej uppfyllda krav
    - Indata: Riskkarta. Analys av uppfyllelse av interna och externa krav
    - Ta fram åtgärdsplan för identifierade risker i riskkarta
    - Prioritera åtgärder och ta fram tidplan
    - Identifiera ansvarsroll samt ansvarig person för respektive aktivitet
    - Resultat: Rapport som inkluderar åtgärdsplan för risker och ej uppfyllda krav

Stockholms universitet

Process vid behov av att säkra strategiskt viktiga informationstillgångar



Stockholms universitet

Bilaga 2: Säkerhetskategorier med där tillhörande säkerhetsåtgärder

Anskaffning, utveckling och underhåll av system

Åtgärd	**Ansvarig för uppfyllelse**
Analys och specifikation av informationssäkerhetskrav: Dokumenterade rutiner avseende krav som rör informationssäkerhet för nya informationssystem eller förbättringar av befintligt informationssystem ska finnas	Prefekt/motsvarande
Säkerställande av programtjänster på publika nätverk: Dokumenterade rutiner avseende användning av publika programtjänster ska finnas.	Tillgångens ägare
Skydd av programtjänster i transaktioner: Dokumenterade rutiner avseende programtjänsters transaktioner ska finnas.	Tillgångens ägare
Regler för säker utveckling: Dokumenterade rutiner avseende utveckling av program och system ska finnas.	Prefekt/motsvarande
Rutiner för hantering av systemändringar: Dokumenterade rutiner avseende systemförändringar inom utvecklingscykeln ska finnas.	Prefekt/motsvarande
Teknisk granskning av tillämpningar efter ändringar i driftmiljö: Dokumenterade rutiner avseende ändring i driftmiljö ska finnas.	Tillgångens ägare
Restriktioner för ändringar i programpaket: Dokumenterade rutiner avseende ändringar av programpaket ska finnas.	Tillgångens ägare
Säker utvecklingsmiljö: Dokumenterade rutiner avseende behov av skydd för utvecklingsmiljö ska finnas.	Prefekt/motsvarande

Stockholms universitet

Outsourcad utveckling: Dokumenterade rutiner avseende hur övervakning och styrning av outsourcad systemutveckling ska finnas.	Prefekt/motsvarande
Testdata: Dokumenterade rutiner avseende hantering av testdata ska finnas.	Tillgångens ägare

Stockholms universitet

Åtkomststyrning

Åtgärd	**Ansvarig för uppfyllelse**
Regler för styrning av åtkomst: Dokumenterade rutiner avseende åtkomst till nätverk och nätverkstjänster som användare specifikt beviljats tillstånd för ska finnas. (föreskrift för användning av universitetets information och informationshanterande resurser som finns i Regelboken).	Prefekt/motsvarande
Granskning av användares åtkomsträttigheter: Dokumenterade rutiner avseende aktuella åtkomsträttigheter ska finnas.	Tillgångens ägare
System för lösenordshantering: Dokumenterade rutiner avseende hur tilldelning av lösenord ska finnas.	Tillgångens ägare
Användning av privilegierade verktygsprogram: Dokumenterade rutiner avseende verktygsprogram som kan ha förmåga att kringgå säkerhetsåtgärder ska finnas.	Tillgångens ägare
Åtkomstkontroll till källkod för program: Dokumenterade rutiner avseende tillgång till källkod ska finnas.	Tillgångens ägare

Stockholms universitet

Driftsäkerhet

Åtgärd	**Ansvarig för uppfyllelse**
Driftrutiner: Dokumenterade driftrutiner avseende informationsbehandlings- och kommunikationsresurser ska finnas.	Tillgångens ägare
Ändringshantering: Dokumenterade rutiner avseende förändringar i informationsbehandlingsresurser och system ska finnas.	Tillgångens ägare
Kapacitetskrav: Dokumenterade rutiner avseende nuvarande och framtida kapacitetskrav ska finnas.	Tillgångens ägare
Separation av utvecklings- test- och driftmiljöer: Dokumenterade rutiner avseende val av separation mellan miljöerna ska finnas.	Tillgångens ägare
Skydd mot skadlig kod: Dokumenterade rutiner avseende upptäckande, förebyggande och återställande ska finnas.	Tillgångens ägare
Säkerhetskopiering: Dokumenterade rutiner avseende säkerhetskopiering av information, program och speglingar av system ska finnas.	Tillgångens ägare
Loggning och övervakning: Dokumenterade rutiner avseende händelseloggar ska finnas.	Prefekt/motsvarande
Styrning av driftsystem: Dokumenterade rutiner avseende installation av program på driftsystem ska finnas.	Tillgångens ägare
Hantering av tekniska sårbarheter: Dokumenterade rutiner avseende hantering av tekniska sårbarheter i de informationssystem som används ska finnas.	Tillgångens ägare

Stockholms universitet

Restriktioner för installation av program: Dokumenterade rutiner avseende programinstallationer ska finnas.	Tillgångens ägare

Stockholms universitet

Kommunikationssäkerhet

Åtgärd	**Ansvarig för uppfyllelse**
Säkerhetsåtgärder för nätverk: Dokumenterade rutiner avseende hantering och styrning av nätverk ska finnas	Prefekt/motsvarande
Säkerhet hos nätverkstjänster: Dokumenterade rutiner avseende vilka krav som bör ingå i avtal ska finnas.	Tillgångens ägare
Separation av nätverk: Dokumenterade rutiner avseende hantering av nätverk ska finnas	Prefekt/motsvarande
Informationsöverföring: Dokumenterade rutiner avseende överföring av information genom användning av kommunikationsmedel ska finnas.	Prefekt/motsvarande

Stockholms universitet

Leverantörsrelationer

Åtgärd	**Ansvarig för uppfyllelse**
Informationssäkerhetsregler för leverantörsrelationer: Dokumenterade rutiner avseende leverantörens åtkomst till organisationens information ska finnas.	Prefekt/motsvarande
Hantering av säkerhet inom leverantörsavtal: Dokumenterade rutiner avseende vilka informationssäkerhetskrav som bör ingå ska finnas.	Prefekt/motsvarande
Hantering av leverantörens tjänsteleverans: Dokumenterade rutiner avseende verifiering av överenskommen nivå ska finnas.	Prefekt/motsvarande