UPPSALA
UNIVERSITET

Dnr UFV 2018/211

Riskhantering

Rutiner för informationssäkerhet

Fastställda av Säkerhetschefen 2018-01-29

Senast reviderade 2018-06-15

Innehållsförteckning

1 Inledning

Nedanstående rutiner beskriver en process för genomförande av riskanalyser för bedömning och behandling av säkerhetsrisker i informationssystem eller annan informationshantering.

Rutinerna utgör en del av universitetets övergripande rutiner för informationssäkerhet (UFV 2017/93), som baseras på Myndigheten för Samhällsskydd och Beredskaps föreskrifter för Statliga myndigheters informationssäkerhet (MSBFS 2016:1).

Dessa rutiner ersätter tidigare regelverk för *riskhantering av informationssystem (2015/322)*.

2 Definitioner

Organisation avser i detta dokument en organisatorisk enhet, t.ex. institution eller motsvarande, eller ett projekt, systemförvaltningsobjekt etc.

Information eller *informationsmängd* innefattar all elektronisk, pappersbaserad, muntlig eller på annat sätt lagrad eller kommunicerad information.

Informationsresurs avser information enligt definitionen ovan samt de informationssystem (hård- och mjukvara) och kommunikationslösningar som hanterar informationen.

Händelse (incident, störning). En oönskad händelse med negativa effekter på universitetet

Hot. En tänkbar/möjlig händelse som skulle kunna inträffa med negativ konsekvens.

Sannolikhet. Sannolikheten för att en händelse ska inträffa (att ett hot ska resultera i en händelse).

Konsekvens. De sammantagna konsekvenserna av en händelse – inkluderande direkta och indirekta kostnader, förtroendeskador, vikande studentantal, minskade forskningsmedel.

Risk. Sammanvägning av konsekvens och sannolikhet för en händelse.

3 Syfte

Dessa riktlinjer avser att ge ett praktiskt och verksamhetsanpassat stöd för kontinuerlig riskhantering av universitetets informationsresurser med avseende på *konfidentialitet*, *riktighet och tillgänglighet.*

4 Mål

Att universitetets informationsresurser är skyddade i enlighet med vid universitetet gällande riktlinjer för informationssäkerhet *(UFV 2017/93)*.

5 Process

Riskhanteringsprocessen i sin helhet genomförs i nedan beskrivna steg, men de enskilda arbetsmomenten kan även utföras separat eller i en kombination. Dock är resultatet från informationsklassificeringen alltid en förutsättning för att kunna göra de efterföljande arbetsmomenten.

1. Avgränsning
2. Konsekvensanalys (med avseende på avbrott)
3. Informationsklassificering
4. Kravanalys
5. Riskanalys
6. Hantering av identifierade säkerhetsbrister

Bilaga 7 beskriver flödet kring de obligatoriska momenten informationsklassificering och kravanalys.

6 Arbetsform

Den arbetsform som rekommenderas är en eller flera workshops med representation från berörd organisation eller arbetsgrupp, gärna med en processledare från universitetets säkerhetsavdelning.

7 Genomförande

7.1 Avgränsning

Innan informationsklassificering och efterföljande arbetsmoment kan påbörjas måste omfattningen definieras. Om den information och de informationsresurser som ska risk-bedömas är relativt homogena kan hela eller delar av processen användas för *grupper av system, ett e-område, ett utvecklings- eller anskaffningsprojekt etc*. Om systemen bedöms som mer heterogena rekommenderas att hantera ett system i taget. Processen kan därtill användas för riskbedömningar som går utanför aktuella systemmiljöer, exempelvis för att analysera den generella informationshanteringen vid en institution.

7.2 Konsekvensanalys

Vid genomförande av en konsekvensanalys görs bedömning av vilka konsekvenser som avbrott av olika tidslängd får för den aktuella verksamheten. Detta moment ingår inte som en obligatorisk del i riskhanteringsprocessen men kan med fördel genomföras riktat mot system med höga krav på tillgänglighet.

Som stöd vid genomförande av konsekvensanalys kan mallen i *Bilaga 1* användas.

7.3 Informationsklassificering

Grunden för en säker hantering av information läggs genom att en informationsklassificering genomförs – en aktivitet där informationens skyddsvärde avgörs 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 förändras eller förstöras, varken obehörigen, av misstag eller på grund av funktionsstörningar.
Tillgänglighet	Informationen ska vara åtkomlig och användbar på förväntat sätt och inom önskad tid.

Informationsklassificeringen genomförs av den organisation som äger informationen. Skyddsbehovet med avseende på säkerhetsaspekterna angivna ovan ska klassificeras i någon av nivåerna 0-3. Klassificeringsvärdet för en informationsmängd uttrycks, baserat på förekommande nivåer, 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.

Som stöd vid informationsklassificeringen kan *Bilaga 2* användas. *Bilaga 6* utgör verktyg för genomförande och rapportering av klassningsresultat. Resultat från genomförda informationsklassificeringar kommer att efterfrågas i samband med institutionernas årliga återrapportering gällande informationssäkerhet – en kopia av genomförd informationsklassificering ska då skickas till säkerhetsavdelningen. Informationsägare vid institutioner och i e-områden ansvarar för att registerförteckningen uppdateras med information om att en informationsklassning genomförts.

7.4 Kravanalys

Kravanalysen är intimt förknippad med momentet informationsklassificering då denna riktas mot ett enskilt eller en gruppering av system. I momentet kravanalys mappas resultatet från genomförd informationsklassificering mot det eller de system som är aktuella i sammanhanget. Klassningsvärden för aktuella informationstyper överförs initialt i detta moment från *Bilaga 6* till *Bilaga 3*.

Det högsta klassningsvärdet för respektive aspekt (konfidentialitet, riktighet och tillgänglighet) som påträffas bland de informationsmängder som systemet hanterar används för att filtrera fram korrekt uppsättning av krav att rikta mot systemet.

Exempel: Ett system hanterar informationsmängderna A, B och C som klassificerats enligt följande:
Informationsmängd A: 132
Informationsmängd B: 331
Informationsmängd C: 222
Det aktuella systemet som analyseras behöver i detta exempel leva upp till krav motsvarande 332.

Momentet med att filtrera fram krav ur den totala kravlistan genomförs med stöd av nedan angiven bilaga.

I kravanalysen granskas efterlevnadnivån av universitetets riktlinjer för informationssäkerhet *(UFV 2017/93)*. I tabellen nedan framgår de säkerhetsområden som omfattas av riktlinjerna och målen för säkerhetsarbetet (skyddsmålen) inom dessa områden.

Riktlinjer	Universitetets riktlinjer för informationssäkerhet är kända inom organisationen.
Organisation och ansvar	Ansvar och ansvarsområden för informationssäkerhetsarbetet är uttalat inom organisationen.
Personalsäkerhet	Anställda och övriga berörda parter är medvetna om det egna ansvaret för informationssäkerhet.
Hantering av tillgångar	Informationsresursen/erna skyddas på ett lämpligt sätt.
Styrning av åtkomst	Endast behöriga användare har åtkomst till informationsresursen/erna.
Kryptering	Känslig information skyddas genom kryptering.
Fysisk och miljörelaterad säkerhet	Berörda lokaler och utrustning är skyddade mot obehörigt tillträde, skador och störningar.
Driftsäkerhet	Driften av den aktuella informationsresursen/erna sker på ett korrekt och säkert sätt.

Kommunikationssäkerhet	Dataöverföring till/från informationsresursen/erna skyddas på ett lämpligt sätt.
Anskaffning, utveckling och underhåll av system	Informationssäkerhet hanteras som en integrerad del av informationsresursen/erna över hela livscykeln.
Leverantörsrelationer	Informationssäkerhetskrav enligt universitetets riktlinjer är reglerade i avtal med externa leverantörer.
Incidenthantering	Rutiner för hantering av informationssäkerhetsincidenter är kända inom organisationen.
Kontinuitetshantering	Organisationen har en dokumenterad och verifierad plan för tillgång till informationen i en kris eller katastrofsituation.
Efterlevnad	Organisationen följer författningsenliga och avtalsmässiga informationssäkerhetskrav och skyldigheter.

Kravanalysen genomförs av den organisation som äger de aktuella systemresurserna med stöd av representanter för stöd- och servicefunktioner som t.ex. drift- och förvaltningsorganisationen. Systemägare/e-områdesansvarig ansvarar för att universitetets systemkarta uppdateras med referens till registerförteckningen (Dnr) samt status på arbetet med åtgärder kopplade till kravanalysen. En kopia från genomförd kravanalys ska skickas till säkerhetsavdelningen som ansvarar för samordning av universitetets informationssäkerhetsarbete.

7.5 Riskanalys

I riskanalysen bedöms de *hot* som organisationen exponeras för på grund av sedan tidigare kända eller misstänkta säkerhetsbrister eller de brister som detekterats vid genomförande av kravanalysen. För varje identifierat riskscenario bedöms vilka *konsekvenser* det aktuella hotet skulle få om det realiseras i en incident eller störning i organisationens verksamhet samt *sannolikheten* för att de skulle inträffa.

Riskanalysen utgör inte en obligatorisk del i riskhanteringsprocessen, men kan med fördel användas som komplement till momentet kravanalys.

För varje identifierat hot beräknas en *riskfaktor* fram som en sammanvägning av konsekvens och sannolikhet. Riskfaktorn kategoriserar risken i någon av grupperna nedan som indikerar hur risken ska hanteras av organisationen.

Låg risk	Bevakas.
Medel risk	Planera för att implementera en riskreducerande åtgärd för införande vid lämpligt tillfälle, t.ex. versionsbyte eller motsvarande.
Hög risk	Omedelbar åtgärd krävs.

Riskanalysen genomförs av den organisation som äger de aktuella informationsresurserna med stöd av representanter från stöd- och servicefunktioner som t.ex. drift- och

förvaltningsorganisationen.

Som stöd för riskanalysen kan *Bilaga 4* användas.

7.6 Hantering av identifierade säkerhetsbrister

I ett läge då säkerhetsbrister identifierats i samband med att en kravanalys genomförts finns en tydlig indikation på att det analyserade systemet inte lever upp till en nödvändig nivå av säkerhet. Varje identifierad brist behöver därför analyseras och bedömas samt bli föremål för någon form av riskreducerande åtgärd.

Bilaga 5 beskriver hur identifierade brister ska hanteras och rapporteras.

8 Bilagor

Bilaga 1 – Arbetsdokument för genomförande av konsekvensanalys.

Bilaga 2 – Instruktion för genomförande av informationsklassificering.

Bilaga 3 – Arbetsdokument för genomförande av kravanalys.

Bilaga 4 – Arbetsdokument för genomförande av riskanalys.

Bilaga 5 – Hantering av identifierade säkerhetsbrister.

Bilaga 6 – Arbetsdokument för genomförande av informationsklassificering.

Bilaga 7 – Genomförande/rapportering av momenten informationsklassificering och kravanalys.