UPPSALA
UNIVERSITET

Dnr UFV 2018/211

Riskhantering

Rutiner för informationssäkerhet

Fastställda av Säkerhetschefen 2018-01-29
Senast reviderade 2021-08-15

Innehållsförteckning

1 Inledning

Nedanstående rutiner beskriver en process för genomförande av moment 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 om informationssäkerhet för Statliga myndigheter (MSBFS 2020:6).

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 *informationstillgångar* 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.

Hot. En möjlig oönskad händelse med negativa konsekvenser för verksamheten.

Sannolikhet. Ett mått på hur troligt det är att ett hot realiseras i en negativ händelse.

Konsekvens. Resultat av att ett hot realiseras i en negativ händelse. Kan vara ekonomisk, dåligt anseende eller t ex legal påverkan.

Risk. Sannolikheten och konsekvensen av att ett hot realiseras i en negativ händelse.

Gapanalys. Identifiering av skillnaden mellan införda säkerhetsåtgärder och identifierat behov av säkerhetsåtgärder.

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 rutiner för informationssäkerhet *(UFV 2017/93)*.

5 Process

Riskhanteringsprocessen i sin helhet genomförs i nedan beskrivna steg. De enskilda arbetsmomenten kan även utföras separat eller i en kombination.
Notera att resultatet från informationsklassificeringen alltid är 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

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 forskningsprojekt, 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 informationstillgång 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 dokumentation av klassningsresultat. En kopia av resultat från genomförda informationsklassificeringar ska skickas till säkerhetsavdelningen.

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 informationstillgångar 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 informationstillgångar som systemet hanterar används för att filtrera fram korrekt uppsättning av krav att rikta mot systemet.

Exempel: Ett system hanterar informationstillgångarna A, B och C som klassificerats enligt följande:

Informationstillgång A: 132
Informationstillgång B: 331
Informationstillgång 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 rutiner för informationssäkerhet *(UFV 2017/93)*. Nedan beskrivs 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.

En kopia av resultat från genomförda kravanalyser ska skickas till säkerhetsavdelningen.

7.5 Riskanalys – en metod för riskbedömning

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 hot bedöms vilka *konsekvenser* det aktuella hotet skulle få för organisationens verksamhet om det realiseras i en negativ

händelse samt *sannolikheten* att hotet realiseras.

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.

Försumbar risk	Acceptera
Låg risk	Bevaka
Medel risk	Planera för att implementera en riskreducerande åtgärd för införande vid lämpligt tillfälle, t.ex. versionsbyte eller motsv.
Hög risk	Omedelbar åtgärd krävs.

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 genom att en gapanalys genomförs. Resultatet från genomförd gapanalys ger underlag för lämpliga riskreducerande åtgärder.

Bilaga 5 beskriver hur identifierade brister ska hanteras och rapporteras.

8 Hantering av incidenter

Alla incidenter ska rapporteras till Servicedesk. Detta gäller för samtliga incidenttyper som beskrivs nedan:

En incident som

- påverkat riktigheten, tillgängligheten eller konfidentialiteten hos den information som bedömts ha behov av utökat skydd, eller
- inneburit att informationssystem som behandlar information som bedömts ha behov av utökat skydd inte kunnat upprätthålla avsedd funktionalitet, eller
- påverkat myndighetens förmåga att utföra sitt uppdrag, eller
- i övrigt allvarligt kan påverka säkerheten i den informations-hantering som myndigheten ansvarar för, eller i tjänster som myndigheten tillhandahåller åt en annan organisation.
- har påverkat sekretessen, integriteten eller tillgängligheten till personuppgifter. En incident har inträffat om personuppgifter har förstörts, oavsiktligt eller olagligt, gått förlorade eller ändrats eller röjts till någon obehörig.

Servicedesk gör bedömningen om vad som ska anmälas vidare till MSB alternativt till IMY (Integritetsskyddsmyndigheten). Rapportering ska ske i enlighet med gällande föreskrifter.

9 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.