Dnr UFV 2017/93

UPPSALA
UNIVERSITET

Rutiner för informationssäkerhet

Säkerhetsarbetet vid Uppsala universitet

Fastställda av Universitetsdirektören 2017-05-22
Senast reviderade 2021-03-29

Innehållsförteckning

1 Inledning

Syftet med nedanstående rutiner är att de ska utgöra en grund för informationssäkerhetsarbetet vid universitetet samt ge en övergripande beskrivning av de säkerhetskrav som ställs på all behandling av information vid universitetet, såväl vid normal verksamhet som i tänkbara krissituationer.

Rutinerna är baserade på *riktlinjer för säkerhetsarbetet vid Uppsala universitet* (UFV 2009/1929) och Myndigheten för samhällsskydd och beredskaps *föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet* (MSBFS 2020:6), *föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter* (MSBFS 2020:7) samt *föreskrifter om rapportering av it-incidenter för statliga myndigheter* (MSBFS 2020:8).

Rutinerna ersätter tidigare *riktlinjer för informationssäkerhet (UFV 2010/424).*

2 Ansvar

Ansvaret för genomförande och tillsyn av informationssäkerheten följer det delegerade verksamhetsansvaret (ordinarie linjeansvar). Det innebär att den som är ansvarig för en verksamhet också är ansvarig för genomförande och tillsyn av dess informationssäkerhet.

Se vidare avsnitt 4.2 *Organisation av informationssäkerhetsarbetet*.

3 Definitioner

Informationssäkerhet. Säkerhet för informationstillgångar avseende förmågan att upprätthålla önskad tillgänglighet, riktighet, konfidentialitet (sekretess) och spårbarhet.

Informationsresurser eller *informationstillgångar* omfattar såväl universitetets information som de resurser som används för att hantera informationen. Begreppet innefattar all elektronisk, pappersbaserad, muntlig eller på annat sätt lagrad eller kommunicerad information samt de informationssystem (hård- och mjukvara) och kommunikationslösningar som hanterar informationen.

IS/IT-system. Informationssystem (IS) – system som håller data och information, till exempel Raindance, Primula, Ladok, Studium, DiVA.
Informationsteknologi (IT) – teknologin som håller systemen, t.ex. datorer, telefoni, servrar, kommunikationsutrustning och annan teknisk utrustning.

Skyddsvärd information. Information som omfattas av sekretess eller annars ska betraktas som konfidentiell, innehåller känsliga personuppgifter, är verksamhetskritisk, licensskyddad eller skyddad av lagar och förordningar. Ofta kallad *känslig* information.

Känsliga personuppgifter. Personuppgifter är all slags information som direkt eller indirekt kan knytas till en fysisk person som är i livet. Med känsliga personuppgifter avses enligt dataskyddsförordningen[1] uppgifter om

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter
- biometriska uppgifter som entydigt identifierar en person

Verksamhetskritisk information kan till exempel vara kritisk för en enskild forskare/forskargrupp, en institution/motsvarande, eller kritisk för hela universitetet – som original till avhandlingar, avtalsoriginal, data/information som samlats in över lång tid och/eller inte går att återskapa, samlad information om värdefull egendom med mera. Känslig information kan vara verksamhetskritisk och vice versa.

4 Omfattning

Avsnitten följer benämningarna i informationssäkerhetsstandarden SS-EN ISO/IEC 27002:2017.

4.1 Informationssäkerhetspolicy

Universitetets rutiner för informationssäkerhet (detta dokument) anger övergripande mål och regler för universitetets informationssäkerhetsarbete.

4.2 Organisation av informationssäkerhetsarbetet

Ansvar för informationssäkerhetsarbetet följer universitetets linjeorganisation.

Universitetsledningen ska informera sig om

- I vilken utsträckning införda säkerhetsåtgärder motsvarar universitetets behov
- Allvarliga risker som inte åtgärdats
- Övriga hinder för att uppnå ledningens målsättning med, och inriktning för, informationssäkerhetsarbetet

Rektor har det övergripande ansvaret för verkställigheten av informationssäkerhets-arbetet, och ett kontrollansvar att utförandet följer det delegerade ansvaret.

Chefer inom universitetet ansvarar för att information om informationssäkerhetsarbetet sprids, att resurser efter behov avsätts för arbetet, att medarbetare ges tillräcklig kunskap, samt att de arbetsmetoder som används bidrar till god informationssäkerhet.

[1] *Europaparlamentets och rådets förordning (EU) 2016/679 (GDPR)*

Dataskyddsombudet ska bland annat informera och ge råd om skyldigheter enligt dataskyddsförordningen, övervaka den interna efterlevnaden av dataskyddsförordningen och övervaka efterlevnaden av universitetets strategi för skydd av personuppgifter.

Säkerhetschefen ansvarar för

- Samordning, utveckling och uppföljning av informationssäkerhetsarbetet
- Att utforma och förvalta regelverk för informationssäkerhet
- Att stödja verksamheten i informationssäkerhetsfrågor
- Att säkerställa att krav på informationssäkerhet beaktas i samband med anskaffning, utveckling och drift av IS/IT-system
- Hantering av säkerhetsrelaterad informationsspridning och utbildning
- Hantering av allvarliga säkerhetsincidenter

Alla medarbetare ska följa universitetets mål och strategier, föreskrifter, riktlinjer och övriga beslut. Avvikelser, brister, risker och incidenter rapporteras till närmaste chef. Se även avsnitt 4.12 *Hantering av informationssäkerhetsincidenter*.

4.3 Personalsäkerhet

Om en bakgrundskontroll vid anställning önskas ska den utföras i enlighet med relevanta författningar och etiska krav, samt stå i proportion till verksamhetskrav, klassificering av den information personen kommer att ges behörighet till, samt de upplevda riskerna.

Prefekt/motsvarande ansvarar för att medarbetare är tillräckligt informerade om sina roller och ansvar ifråga om informationssäkerhet innan de ges åtkomst till universitetets informationssystem. Medarbetarna ska även erhålla relevant information om riktlinjer och övriga regelverk, samt möjligheterna till utbildning.

Alla medarbetare ska erbjudas lämplig utbildning och fortbildning för ökad medvetenhet i den omfattning som är relevant för deras befattning. Grundläggande utbildningar ska erbjudas både via lärarledda tillfällen och via internetbaserade kurser. Utöver det ska målgruppsanpassade kurser och informationsträffar erbjudas utifrån verksamhetens behov och önskemål.

Säkerhetschefen ansvarar för att aktuell och lättillgänglig information om riktlinjer, utbildningsmöjligheter med mera finns på universitetets interna webb.

4.4 Hantering av tillgångar

Informationssäkerhetsarbetet på universitetet ska bedrivas systematiskt och riskbaserat med stöd av standarderna inom SS-EN ISO/IEC27000.

Universitetets informationstillgångar ska vara skyddade på ett säkert sätt med avseende på tillgänglighet, riktighet och konfidentialitet. Arbetet med informationssäkerhet ska sträva efter att balansera risker – trolig frekvens och konsekvenser – mot kostnader för skyddsåtgärder. Arbetet ska för varje område planeras, styras och utföras strukturerat.

Immateriella rättigheter ska skyddas genom att inköp av programvaror eller licenser sker via universitetets licensregister och att gällande bestämmelser rörande upphovsrätt följs.

Hantering av inventarier ska följa universitetets regelverk för anläggningsregister.

Löpande förbättringsåtgärder ska införas som ett resultat av kontinuerlig uppföljning. Därutöver ska säkerhetsförbättringar införas vid behov, t.ex. vid allvarliga incidenter.

Grundläggande krav för hantering av universitetets informationsresurser är att

- Resurserna ska vara identifierade och dokumenterade.
- Skyddsåtgärder med avseende på riktighet, tillgänglighet och konfidentialitet ska baseras på informationsklassificering – se *rutiner för riskhantering* (UFV 2018/211), bilaga 2, *Stöd för informationsklassificering*.
- Informationssystem som innehåller skyddsvärd information ska ha ansvarsförbindelser för systemets administratörer och andra användare med högre behörigheter.
- Allmänna handlingar hanteras enligt *Hantering av allmänna handlingar vid universitetet (UFV 2020/1013)*.
- Externa parters tillgång till och hantering av universitetets informationsresurser (utnyttjande, förvaltning, underhåll etc.) ska regleras i avtal.

4.5 Styrning av åtkomst

Inom universitetet baseras åtkomsträtten till informationen bland annat på tryckfrihetsförordningen, offentlighets- och sekretesslagen och dataskyddsförordningen.

Alla informationssystem ska ha rutiner och system för behörighetskontroll i syfte att förhindra otillåten åtkomst, förändring eller förstöring av information. Avsnittet *Styrning av åtkomst* i *rutiner för anskaffning och drift av IT-system* (UFV 2020/2599) anger detaljerade säkerhetskrav.

4.6 Kryptering

Okrypterad information är läsbar för alla. *Kryptering* innebär att informationen kodas så att den inte går att läsa utan en nyckel för dekryptering. Skyddsvärd information i informationssystem och IT-tjänster ska skyddas genom kryptering, antingen av informationen i sig, lagringsmedia eller kommunikationsvägarna.

Se universitetets *rutiner för säker informationshantering* (UFV 2018/668) och *rutiner för säkerhetsåtgärder i informationssystem* (UFV 2021/276).

4.7 Fysisk och miljörelaterad säkerhet

Lokaler och utrustning där universitetets informationstillgångar förvaras och hanteras ska vara utrustade med väl avvägda skydd gällande brand, intrång, stöld, elförsörjning, klimat, otillåten användning och andra skador eller störningar.

Se avsnittet *Fysisk och miljörelaterad säkerhet* i *rutiner för anskaffning och drift av IT-system* (UFV 2020/2599).

4.8 Driftsäkerhet

Driftrutiner och ansvar ska syfta till att säkerställa korrekt och säker drift av informationsbehandlingsresurser.

Vid driftsättning och daglig drift av universitetets informationssystem ska universitetets *riktlinjer inom IT-området* (UFV 2016/896) följas. Förutom de övergripande riktlinjerna finns även *rutiner för produktionssättning av IT-system för central användning vid Uppsala universitet* (UFV 2014/1171), liksom *rutiner för anskaffning och drift av IT-system* (UFV 2020/2599) och *rutiner för säkerhetsåtgärder i informationssystem* (UFV 2021/276).

4.9 Kommunikationssäkerhet

Rutiner för hantering av nätverk och nätverkstjänster ska säkerställa korrekt skydd av information i nätverk och dess stödjande informationsbehandlingsresurser.

Vid dataöverföring i interna och externa nätverk ska *rutiner för anskaffning och drift av IT-system* (UFV 2020/2599) och *rutiner för säkerhetsåtgärder i informationssystem* (UFV 2021/276) följas.

4.10 Anskaffning, utveckling och underhåll av system

Rutiner vid anskaffning, utveckling och underhåll av system ska säkerställa att system och tjänster svarar mot universitetets krav på god informationssäkerhet och bidra till att upprätthålla en hög nivå av säkerhet i driftmiljöer och i universitetets datornät.

Informationssäkerhet ska hanteras som en integrerad del av informationssystem över hela livscykeln. Universitetets *rutiner för anskaffning och drift av IT-system* (UFV 2020/2599) ska följas vid såväl anskaffning som utveckling och underhåll av system.

Universitetets *rutiner för säker systemutveckling* (2014/1307) ska följas vid egenutveckling av system.

Avveckling av system ska följa universitetets *rutiner för utrangerad utrustning* (UFV 2014/1279)

Se även universitetets *riktlinjer inom IT-området* (UFV 2016/896).

4.11 Leverantörsrelationer

Informationssäkerhetskrav enligt universitetets riktlinjer ska vara reglerade i avtal med externa leverantörer. *Rutiner för anskaffning och drift av IT-system* (UFV 2020/2599) innehåller stöd för kravställning i samband med anskaffning och drift.

4.12 Hantering av informationssäkerhetsincidenter

Universitetets verksamma ska alltid rapportera alla typer av informationssäkerhets-incidenter till universitetets servicedesk.

Löpande bevakning, uppföljning och rapportering av informationssäkerhetsincidenter ska göras av universitetets säkerhetsavdelning.

Incidenter med koppling till informationssäkerhet ska rapporteras enligt Myndigheten för samhällsskydd och beredskaps *föreskrifter om rapportering av it-incidenter för statliga myndigheter* (MSBFS 2020:8). Servicedesk ansvarar för sammanställning av relevant information och rapportering till MSB.

4.13 Informationssäkerhetsaspekter avseende hanteringen av verksamhetens kontinuitet

Avbrottsplanering ska genomföras för alla informationssystem där längre avbrott eller andra störningar kan orsaka stor skada för universitet, verksamma vid universitetet eller andra berörda. Baserad på prioriteringar i verksamheternas avbrottsplaner ska en återstartsplan finnas för återgång till drift av ordinarie system. Såväl avbrotts- som återstartsplaner ska vara dokumenterade och testas regelbundet.

Se *rutiner för säkerhetsåtgärder i informationssystem* (UFV 2021/276), avsnittet om redundans och återställning.

4.14 Efterlevnad

Informationssäkerhetsarbetet ska årligen följas upp för att säkerställa att det bedrivs i enlighet med universitetets regler och riktlinjer, samt författningsenliga och avtalsmässiga informationssäkerhetskrav. Det innebär att

- E-områdesansvariga/systemägare ska se till att informationssäkerhetsarbetet ingår i den årliga verksamhetsplaneringen för e-områden och informations-system.
- Projektägare ska se till att en bedömning av informationssäkerhetsrisker genomföras i ett tidigt skede av projekt för att identifiera nödvändiga säkerhetsåtgärder.
- Säkerhetsavdelningen ska
    - granska teknisk efterlevnad för att säkerställa att skyddsåtgärder införts korrekt
    - genomföra olika säkerhets- och sårbarhetsgranskningar
    - bedriva omvärldsbevakning för att underlätta identifiering och hantering av hot mot och sårbarheter i universitetets informationssystem
    - stödja och följa upp övrig verksamhets arbete med informationssäkerhet
    - sammanställa rapporter till ledningen