HÖGSKOLAN
I HALMSTAD

Riktlinjer för hantering av information

Fastställd av högskoledirektör 2018-10-18, dnr I 2018/65

Innehåll

Bakgrund

Beroende på typ av information, och de faktiska uppgifternas innehåll ställs olika krav på hantering av uppgifter. För information i Högskolans centrala och administrativa IT-system utgör resultatet av informationsklassningen grund för hur informationen får hanteras.

Även annan information inom Högskolan, till exempel dokument och epostmeddelanden, ska, om möjligt, hanteras enligt denna instruktion.

För mycket av Högskolans information är konsekvensen av bristande konfidentialitet måttlig, och där bristande riktighet och bristande tillgänglighet kan få betydande konsekvenser. Denna information ska hanteras enligt grundnivån för informationssäkerhet, som beskrivs nedan.

För information där bristande konfidentialitet kan få betydande konsekvenser gäller ytterligare krav; även dessa beskrivs nedan. Dessa högre krav gäller även för skyddsvärd och särskilt skyddsvärd information.

För information där bristande konfidentialitet, riktighet eller tillgänglighet kan leda till allvarliga konsekvenser ska separat diskussion om hanteringen föras med informationssäkerhetsansvarig, eller någon som denne utsett.

Grundnivå

Personal

Personal ska ha genomgått informationssäkerhetsutbildning, och förstå sitt informationssäkerhetsansvar.

Hantering av information

Information ska hanteras så att myndigheten kan få åtkomst till den.

Information (lagringsenheter och dokumentation) ska hanteras korrekt och med försiktighet, oavsett var hanteringen sker.

Lokala diskar och t.ex. USB-diskar bör endast användas för tillfällig lagring. Undantag görs för forskningsdata som lagras på extern hårddisk. Säkerhetskopiering ska, om möjligt, göras inom Högskolan eller inom av Högskolan rekommenderad tjänst.

I enlighet med persondataförordningen får personuppgifter bara hanteras (inklusive lagras) inom Högskolan, och inom Högskolan godkända IT-tjänster.

Styrning av åtkomst

Endast behörig personal ska kunna läsa, ändra eller radera information, oavsett medium. Förändring av behörighet ska ske löpande, vid behov, och beställs av verksamhetsansvarig till systemförvaltare eller motsvarande.

Användarkonton och åtkomsträttigheter bör granskas regelbundet. Rättigheter ska återkallas när åtkomst inte längre behövs.

Användaridentiteter ska vara unika, individuella, och kunna spåras till en fysisk person.

Autentisering ska ske med minst lösenord. I de fall ett lösenord måste skrivas ned ska det förvaras inlåst.

Lösenord som är tillgängliga för flera personer ska undvikas, men om de används ska de hållas i säkert förvar enligt särskilda rutiner. Lösenord bör ej överföras eller lagras i klartext.

Hög behörighet ska kunna kontrolleras, och inte vara möjlig att tilldela sig själv.

Skilda roller för loggadministration, daglig drift och tilldelning av åtkomsträttigheter bör finnas.

Dator eller liknande, som innehåller skyddsvärd information, och som lämnas obevakad ska skyddas, t.ex. med lösenordsskyddad skärmsläckare, utloggning eller avstängning.

Fysisk och miljörelaterad säkerhet

Det ska finnas fysiska avgränsningar och passerkontroll som förhindrar intrång, otillåten användning, stöld, brand och annan skada.

Obevakad utrustning och information ska ha anpassat skydd, t.ex. skyddad förvaring, låst skåp eller låst rum.

Elavbrott ska motverkas. Kablar för elförsörjning och kommunikation ska ha anpassat skydd mot störning och skada.

Driftsäkerhet

Säkerhetskopiering ska utföras regelbundet, minst var 24e timme. Test och kontroll av kopior bör göras.

Digitalt lagrad information bör lagras på minst två fysiska platser.

Säkerhetskopian ska skyddas enligt den klassning som informationen innehåller.

Generella återstarts- och återställningsrutiner ska finnas.

Säkerhetsrelevanta händelser i IT-system bör registreras tillsammans med datum, tid, identitet. Loggen ska skyddas, sparas, och analyseras regelbundet eller vid behov. Automatiska analyser av loggen ska vara möjlig. Vid fel på loggfunktionen ska behörig administratör få meddelande om detta.

Endast behörig person ska kunna förändra information, program och/eller konfiguration.

Sammankoppling med andra nätverk får endast ske efter att nödvändiga säkerhetsåtgärder vidtagits.

Intrångsskydd ska förhindra obehörig åtkomst till IT-system, och det ska kontrollera både inkommande och utgående informationsflöde.

Upptäckande, förebyggande och återställande skydd mot skadlig kod ska vara installerat, aktivt och uppdaterat.

Säkerhets- och programvaruuppdateringar ska vid behov införas.

IT-system

Informationssäkerhet ska vara en integrerad del över IT-systems hela livscykel, även vid återanvändning och återvinning. Informationsklassning och riskbedömning är grunden för val av säkerhetsskydd.

IT-system inkl. säkerhetsfunktioner ska vara stabilt och väl testat och det ska finnas aktuell systemdokumentation.

Utvecklings- och testsystem ska vara separerade från driftsatt system för att minska risken för driftstörning eller informationssäkerhetsincident.

Leverantörsrelationer

Relevanta informationssäkerhetskrav ska avtalas med leverantör och dessa ska revideras och kontrolleras efter behov.

Det ska tecknas avtal gällande leverantörens tillgång till och användning av Högskolans information. Även ansvar och roller, eventuella revisionsrättigheter och hantering av eventuella personuppgifter ska regleras.

Högre krav – konfidentialitet

Hantering av tillgångar

Särskilda, separerade skrivare ska användas för utskrift.

Kopiering av information är endast tillåten efter godkännande av systemägare.

Vid förstöring av papper ska papperstugg eller kontrollerad bränning användas. Vid förstöring av digitalt lagringsmedium ska överskrivning eller mekanisk förstöring användas.

Sekretessbelagd information ska hanteras i särskild ordning.

Styrning av åtkomst

Förinställda eller onödiga användarkonton ska blockeras eller förses med nytt lösenord.

Stark autentisering, t.ex. tvåfaktorsautentisering, bör användas.

Nedkoppling vid inaktivitet, begränsad uppkopplingstid och speciell lösning för fjärråtkomst bör användas.

Om obehörig tagit del av information ska detta anmälas till IT-avdelningen.

Kryptering

Särskild krypteringsutredning ska göras för att avgöra om information ska sändas och lagras krypterad.

När kryptering används ska den vara avsedd för specifik informationssäkerhetsklass.

Kryptonyckelhantering och skydd av kryptonyckel måste ske så att inte information röjs eller riktighet påverkas

När kryptering används ska det säkerställas att information går att återställa av fler än en person, alternativt att informationen även finns tillgänglig för myndigheten i okrypterad form.

Driftsäkerhet

Onödiga tjänster, protokoll och programvaror ska tas bort eller inaktiveras

Övervakning av IT-system ska ske, t.ex avseende drifttillståndsförändringar, strömbortfall, varningar, larm och andra specificerade händelser.

Systemförändringar ska ske i kontrollerad ordning.