Högskolan Kristianstad

RIKTLINJER
2021-03-05
Dnr: 2021-114-142

Fastställd av högskoledirektör 2021-03-15
Versionsnr: 1

Informationssäkerhetsrådet
Högskolan Kristianstad
291 88 Kristianstad
044-250 30 00
www.hkr.se

Riktlinjer för incidenthantering av IT- och informationssäkerhetsincidenter

1. Inledning

Till stöd för arbetet med samhällets informationssäkerhet ska alla myndigheter enligt förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (20 §) skyndsamt rapportera IT-incidenter, som inträffat i myndighetens informationssystem och som allvarligt kan påverka säkerheten i informationshantering, till Myndigheten för samhällsskydd och beredskap (MSB).

Enligt MSB:s föreskrifter om informationssäkerhet för statliga myndigheter (MSBFS 2020:6), 11 §, ska en myndighet ha förmåga att:

- skyndsamt upptäcka och bedöma incidenter och avvikelser,
- återställa manipulerad eller förlorad information, och
- bedöma om inträffad incident ska rapporteras externt.

Om en incident eller avvikelse inträffat ska myndigheten identifiera grundorsaker till incidenten eller avvikelsen och vidta åtgärder för att motverka att liknande incidenter och avvikelser inträffar på nytt.

Hur rapportering av IT-incidenter ska ske framgår av MSB:s föreskrifter om rapportering av it-incidenter för statliga myndigheter (MSBFS 2020:8). Med it-incidenter som omfattas av rapporteringsskyldighet menas en it-incident som;

1. påverkat riktigheten, tillgängligheten eller konfidentialiteten hos den information som bedömts ha behov av utökat skydd, eller

2. inneburit att informationssystem som behandlar information som bedömts ha behov av utökat skydd inte kunnat upprätthålla avsedd funktionalitet, eller

3. påverkat myndighetens förmåga att utföra sitt uppdrag, eller

4. i övrigt allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller i tjänster som myndigheten tillhandahåller åt en annan organisation.

Syftet med detta dokument är att redogöra för samtlig personal hur incidenthantering avseende IT- och informationssäkerhetsincidenter ska gå till på Högskolan Kristianstad

2. IT-incident

En IT-incident avser sådan händelse där högskolans verksamhet som helhet påverkas märkbart negativt till följd av en avsiktlig eller oavsiktlig störning, avbrott eller på annat sätt avsevärt försämrad kvalitet i ett IT-system eller tjänst.

Typexempel på en IT-incident skulle kunna vara:

- Lagringsmedia för server havererar. (*Avbrott i tjänst*)
- Felkonfigurering av brandvägg. (*Avbrott i tjänst och nätverk*)
- Fiberoptisk nätverkskabel grävs av. (*Avbrott i nätverk*)

3. Informationssäkerhetsincident

Definieras av Myndigheten för samhällsskydd och beredskap (MSB) som:
"*En incident där information i systemet eller nätverket, snarare än systemet eller nätverket, i sig, har påverkats.*"

En informationssäkerhetsincident avser således en händelse där information eller en informationstillgång har eller kan ha påverkats negativt genom exempelvis felaktig hantering, obehörig åtkomst, förlorad tillgänglighet och oriktighet.

Begreppet informationssäkerhetsincident delas upp i två underkategorier, där den ena inte behöver utesluta den andra:

- IT-säkerhetsincident
- Personuppgiftsincident

3.1 IT-säkerhetsincident

Med IT-säkerhetsincident avses sådan händelse där känslig information har utsatts för negativ påverkan, t.ex. obehörig åtkomst eller förlorad tillgänglighet, till följd av intern- eller yttre åverkan, eller felaktig hantering av ett IT-system.

Typexempel på en IT-säkerhetsincident skulle kunna vara:

- Dataintrång – Skadlig programvara (*Virus / Malware*)
- Dataintrång – Kapat epostkonto (*Stulna inloggningsuppgifter*)
- Dataintrång – Utnyttjande av säkerhetsbrist *(hacking)*
- Epostbedrägeri – Nätfiske & Social Engineering (*lura-till sig information*)
- Dataläckage – Otillåten hantering (*information sprids till obehörig*)
- Dataläckage – Borttappat oskyddat USB-minne (*obehörig får åtkomst*)

Konsekvenserna av en IT-säkerhetsincident kan vara allt ifrån försumbara till mycket allvarliga. Således kan IT-säkerhetsincidenter på högskolan komma att klassificeras som följande kategorier enligt nedan exempel:

- IT-säkerhetsincident (*försumbar*)
  - Dator infekteras och oönskade reklamprogram installeras.
  - Användaren blir utsatt för SPAM- eller generella nätfiske-meddelanden via epost.
- IT-säkerhetsincident (*av normalgraden*)
  - Dator infekteras och destruktiv mjukvara installeras.
  - Användaren blir utsatt för riktade nätfiske-meddelanden via epost.
- IT-säkerhetsincident (*allvarlig*)
  - Händelse som påverkar högskolans förmåga att bedriva sin verksamhet ur säkerhetsperspektiv.
  - Händelse som påverkar högskolans möjlighet till säker informationshantering.
  - Händelse som resulterar i att känslig information/data eller personuppgifter exponeras, raderas eller manipuleras på ett otillåtet sätt.

I de fall en IT-säkerhetsincident bedöms som allvarlig ska Högskolans IT-avdelning inom 6 timmar rapportera en övergripande beskrivning (notis), i enlighet med MSBFS 2020:8 (4 §), till Myndigheten för samhällsskydd och beredskap (MSB). Inom 4 veckor från inträffad incident ska Högskolan komplettera incidentrapporteringen till MSB med fullständig rapport, i enlighet med MSBFS 2020:8 (5 §).

3.2 Personuppgiftsincident

En personuppgiftsincident har inträffat vid oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Med personuppgiftsincident avses också en händelse som leder till obehörigt röjande av eller obehörig åtkomst till de behandlade personuppgifterna.

Exempel på personuppgiftsincidenter:

- E-postmeddelande med känsligt eller extra skyddsvärda personuppgifter skickas till fel mottagare.
- En mobiltelefon, dator eller USB-minne med personuppgifter tappas bort eller blir stulen.
- Någon kommer över ett lösenord som gör att en obehörig skulle kunna logga in i system som behandlar personuppgifter.
- Personuppgifter exponeras till följd av en IT-säkerhetsincident/ dataintrång.
- Personuppgifter hamnar i obehöriga händer genom kvarglömda dokument.

När en personuppgiftsincident har inträffat ska först och främst sannolikheten och allvaret, och den därmed följande risken för människors rättigheter och friheter, fastställas. Sådana risker kan till exempel vara att enskilda förlorar kontrollen över sina uppgifter, att enskildas rättigheter inskränks, en identitetsstöld, bedrägeri, ekonomisk förlust, skadat anseende, brott mot sekretess eller andra nackdelar för den berörda fysiska personen.

Om det är sannolikt att personuppgiftsincidenten kommer att medföra en risk för de registrerade måste incidenten anmälas till Integritetsskyddsmyndigheten inom 72 timmar från upptäckt. Är det däremot osannolikt att en personuppgiftsincident medför risker behöver ingen anmälan göras till Integritetsskyddsmyndigheten. Ett beslut att inte anmäla ska motiveras och dokumenteras.

Om en personuppgiftsincident sannolikt leder till en hög risk för fysiska personers rättigheter och friheter måste de registrerade informeras utan onödigt dröjsmål.

4. Incidenthanteringsrutin

Då varje situation och incident som kan uppkomma, oftast är unik med specifika förutsättningar, anses det vara opraktiskt att försöka implementera en detaljerad statisk handlingsplan som redogör för rutinen steg-för-steg.

Istället implementeras en incidenthanteringsrutin med viktiga moment i en rekommenderad ordning, som ska utföras under incidenthanteringsprocessen. Ordningsföljden är dock endast en rekommendation med det enda kravet att samtliga moment genomförs. Detta för att dynamiskt kunna anpassa arbetssättet och prioritera ingrepp och lösningar efter situationens förutsättningar.

Incidenthanteringen ska omfatta följande moment (*rekommenderad ordning*):

- Fastställ vad för typ av incident som har inträffat (*IT, InfoSäk, osv*)
- Identifiera påverkade system och resurser.
- Begränsa incidenten och förhindra vidare spridning.
- Utvärdera lösningsalternativ (kortsiktig) och implementera.
- Samla in loggdata, rapporter och annan relevant händelsedokumentation.
- Dokumentera information om incidenten. (*händelse, tid, omfattning, osv*)
- Dokumentera lösningsimplementation. (*hur åtgärdades problemet?*)
- Informera IT-chef om incidenten, påverkan och lösning.
- Informera Dataskyddsombud vid personuppgiftsincident.
- Rapportera till MSB och/eller Integritetsskyddsmyndigheten enligt direktiv.
- Utvärdera långsiktiga lösningsalternativ (*om relevant*) och implementera.
- Upprätta arbetsrutiner och/eller systemimplementationer som förebygger framtida liknande incidenter.
- Om det anses nödvändigt, komplettera rapportering till MSB och Integritetsskyddsmyndigheten.

Incidenter ska hanteras och prioriteras baserat på vilken omfattning/påverkan de har på verksamheten som helhet.

Återkoppling ska ske i efterhand till högskolans informationssäkerhetsråd beträffande inträffade incidenter.

4.1 Incidentrapportering till Högskolan Kristianstad

Samtliga IT- och informationssäkerhetsincidenter ska i första hand rapporteras till Högskolan Kristianstads servicedesk (3030). Det är viktigt att rapportera så snart som möjligt efter upptäckt. I de fall ärendet inte går att lösa direkt, delegeras ärendet vidare till berörd part/avdelning.

Epost: 3030@hkr.se
Telefon: 044 250 30 30

4.2 Incidentrapportering till MSB

För IT-incidenter och informationssäkerhetsincidenter (*ej personuppgiftsincident*), ansvarar IT-chef för att rapportering till MSB sker enligt gällande direktiv.

Det är således IT-chef som beslutar/avgör huruvida en incident är att betrakta som anmälningspliktig eller ej.

IT-chef kan delegera incidentrapporteringen till annan utsedd om så görs från fall till fall (*ej tillsvidare*).

Incidenter som omfattar anmälningspliktiga IT- eller informationssäkerhets-incidenter ska rapporteras övergripande (notis) till MSBinom 6 timmar efter upptäckt.

Senast 4 veckor efter upptäckt ska kompletterande rapport vara MSB tillhanda, via MSB:s rapporteringsformulär.

För information och stöd gällande ifyllnad av rapporteringsformuläret, se MSB:s stöddokument.

4.3 Incidentrapportering till Integritetsskyddsmyndigheten

Vid personuppgiftsincidenter ansvarar högskolans dataskyddsombud för rapporteringen till Integritetsskyddsmyndigheten. Det är dataskyddsombudet som avgör om personuppgiftsincidenten är anmälningspliktig eller inte och som därefter ansvarar för att anmälan sker via Integritetsskyddsmyndigheten:s rapporteringsformulär. I de fall det beslutats att inte anmäla (ej anmälningspliktig), motiveras och dokumenteras detta.

Anmälan till Integritetsskyddsmyndigheten ska enligt Dataskyddsförordningen göras inom 72 timmar från det att incidenten har upptäckts.

Om det inte är möjligt att lämna all information inom 72 timmar kan anmälan delas upp och information lämnas allt eftersom det blir möjligt. Om anmälan till Integritetsskyddsmyndigheten görs efter 72 timmar ska skälen för förseningen anges.

5. Uppföljning

Uppföljning av riktlinjerna ska ske av informationssäkerhetsrådet löpande.

6. Giltighet

Detta dokument gäller fr o m den 15 mars 2021.