HÖGSKOLAN I BORÅS

Handlingstyp:		Diarienr:	Bilagor:	Sida:
Riktlinjer		219-21	-	1 av 7
Ansvarig handläggare:	**Fastställd av:**	**Beslutsdatum:**		**Ersätter:**
Informationssäkerhetssamordnare	Förvaltningschef	2021-03-17		581-18

Riktlinjer för hantering av IT- och informationssäkerhetsincidenter

Innehåll

1 Inledning

Riktlinjer för hantering av IT- och informationssäkerhetsincidenter vänder sig till alla verksamma vid Högskolan i Borås och särskilt till ansvariga för IT-incidenter, informationssäkerhet, CSIRT-gruppen[1] samt Dataskyddsgruppen.

I MSBFS 2020:6, angående statliga myndigheters informationssäkerhet, anges följande:

> *11 § Myndigheten ska ha förmåga att*
> *1.skyndsamt upptäcka och bedöma incidenter och avvikelser,*
> *2.återställa manipulerad eller förlorad information, och*
> *3.bedöma om inträffad incident ska rapporteras externt.*

Det huvudsakliga syftet med denna riktlinje är att beskriva hur incidenter ska hanteras och hur rapportering av incidenter ska ske vid Högskolan i Borås.

1.1 Rapportera incidenter

Den som upptäcker en IT- och/eller informationssäkerhetsincident vid Högskolan i Borås, ska omgående rapportera detta till:

E-post: it@hb.se
Telefon: 033-435 46 90

Vid kritiska incidenter kontaktas IT-avdelningen alltid via ovanstående telefonnummer. Utanför kontorstid rapporteras kritiska incidenter till IT-chef.

1.2 Definition incidenter

1.2.1 IT-incident

En IT-incident är en oönskad och oplanerad störning eller en försämring av kvaliteten i en tjänst som kan få eller har fått negativa konsekvenser för verksamheten, enskild individ eller tredje man. En IT-incident kan antingen bero på ett avsiktligt eller oavsiktligt agerande. I första hand hanteras IT-incidenter av servicedesk på IT-avdelningen, beroende på typ av incident kan den skickas vidare till berörda funktioner. För incidenter som klassas som informations-säkerhetsincidenter finns en särskild definition och hantering, se nedan.

[1] CSIRT står för Computer Security Incident Response Team och är en vedertagen benämning på den grupp som agerar på inkommande IT-relaterade incidenter. CSIRT-gruppen finns inrättad på IT-avdelningen. För mer information se www.hb.se/csirt

1.2.2 Informationssäkerhetsincident

Informationssäkerhetsincidenter är händelser som påverkar, eller kan komma att påverka, säkerheten negativt för högskolans informationstillgångar. Den gemensamma nämnaren är att informationssäkerheten hotas genom t.ex. obehörig åtkomst till information, olaglig hantering av data, felaktig information eller brist på tillgång till information.

Informationssäkerhetsincidenter kan vara en IT-säkerhetsincident, en personuppgiftsincident eller både och.

1.2.2.1 IT-säkerhetsincident

En IT-säkerhetsincident karaktäriseras oftast av att det krävs någon form av omedelbar åtgärd för att hantera situationen och kan många gånger innebära en störning i förmågan att bedriva verksamheten eller att det kan påverka säkerheten för högskolans informationshantering. Några exempel på IT-säkerhetsincidenter kan vara kapad inloggning, dataintrång, angrepp med skadlig kod (virus) på dator, dataläckage, bedrägeriförsök via e-post eller säkerhetsbrist i produkt.

Enligt MSBFS 2020:8 2§ har myndigheten en rapporteringsskyldighet för incidenter enligt följande:

> *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.*

I de fall IT-säkerhetsincidenten faller in enligt ovan definition kommer CSIRT-gruppen att rapportera vidare till Myndigheten för samhällsskydd och beredskap (MSB) enligt MSBFS 2020:8:

> *4 § Myndigheten ska skyndsamt, dock senast sex timmar från det att myndigheten har identifierat att en IT-incident omfattas av rapporteringsskyldighet, lämna en övergripande beskrivning av vad som inträffat(notifiering).*
>
> *5 § Myndigheten ska inom fyra veckor från det att myndigheten identifierat att en it-incident omfattas av rapporteringsskyldighet lämna följande uppgifter (slutrapportering).*
> *1.Myndighetens namn.*
> *2.En beskrivning av inträffad IT-incident, utifrån*
> *a.tidpunkt för när IT-incidenten inträffade och när den upptäcktes,*
> *b.tidpunkt för när drabbade informationssystem återgick till normaldrift,*
> *c.händelseförlopp,*

d.hanteringen av IT-incidenten, och
e.typ, orsak och konsekvenser.
3.Vidtagna och planerade åtgärder med anledning av den inträffade IT-incidenten.

Om misstanke finns att ett brott har begåtts kommer CSIRT-gruppen även att kontakta rättsvårdande myndigheter.

Syftet med obligatorisk IT-incidentrapportering är enligt regeringen att stödja samhällets informationssäkerhet; det möjliggör en förbättrad lägesbild över informationssäkerheten, skapar förutsättningar för att vidta rätt skyddsåtgärder och utvecklar förmågan att förebygga, upptäcka och hantera IT-incidenter. Genom att skyndsamt rapportera till MSB, för att därigenom få en samlad och övergripande bild, finns också möjlighet att samordnat vidta åtgärder för att avvärja eller begränsa konsekvenserna av allvarliga IT-incidenter. Sådana IT-incidenter kan röra exempelvis störningar i mjukvara, hårdvara eller driftmiljö eller förlust av data i olika sammanhang. IT-incidenter kan orsakas av bland annat externa attacker, säkerhetsbrister i IT-produkter eller felaktigt handhavande. [2]

1.2.2.2 Personuppgiftsincident

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.[3]

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har blivit förstörda, gått förlorade på annat sätt eller kommit i orätta händer. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt.

Vid personuppgiftsincidenter kommer dataskyddsgruppen att rapportera vidare till Integritetsskyddsmyndigheten inom 72 timmar enligt gällande föreskrifter.

> *Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till den tillsynsmyndighet som är behörig i enlighet med artikel 55, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter.* [4]

I vissa fall ska den registrerade informeras om incidenten.

---

[2] Regeringens förordning (2015:1052) och MSBFS föreskrifter om statliga myndigheters rapportering av IT-incidenter
[3] Dataskyddsförordningen Artikel 4 p.12
[4] Dataskyddsförordningen artikel 33

Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.[5]

2 Processen

Syftet med incidenthantering är att:

- Synliggöra risker och vidta åtgärder efter att incidenter inträffat i verksamheten
- Genom att analysera incidenter förebygga att liknande incidenter sker på nytt

För att säkerställa att eventuella incidenter får minimal påverkan på högskolans verksamhet finns en incidenthanteringsprocess som visar hur hantering, rapportering och analys av incidenter ska genomföras.

Funktioner som normalt sett hanterar incidenter är servicedesk, drifts-, utvecklings- och supportfunktionen på IT-avdelningen för incidenter som berör respektive ansvarsområde, CSIRT för IT-säkerhetsincidenter och Dataskyddsgruppen för personuppgiftsincidenter. Respektive funktion som mottar en incident gör inledningsvis en analys för att avgöra potentiell påverkan på information, individer och högskolans verksamhet och hur den eventuellt ska eskaleras vidare i organisationen. Berörd funktion avgör löpande vilka chefer och övrig ledning som behöver informeras om incidenten. Incidenterna hanteras i prioritetsordning i relation till den potentiella påverkan som incidenten kan orsaka verksamheten.

Hanteringen av incidenter ska omfatta:

- Begränsa incidenten
- Identifiera och åtgärda rotorsak
- Dokumentera information om incidenten innehållande, tidpunkt, vad som inträffat, omständigheter m.m.
- Rapportera incident till MSB respektive Integritetsskyddsmyndigheten utifrån fastställda direktiv
- Fastställa bevis genom exempelvis granskning av loggar
- Vid incident som även har fysisk påverkan ska funktion ansvarig för fysisk säkerhet informeras

Efter att incidenten hanterats och åtgärdats ska en analys genomföras och dokumenteras:

- Summering incident
- Gjorda erfarenheter
- Kortsiktig lösning
- Långsiktig lösning
- Om nödvändigt komplettera informationen till MSB respektive Integritetsskyddsmyndigheten
- Uppdatering av rutiner, processer etc. för att minimera risken för upprepad incident

[5] Dataskyddsförordningen artikel 34

3 Incidentrapportering till MSB

CSIRT-funktionen ansvarar vid behov för att rapportera till MSB enligt nedan.

Steg 1: Notifiering till CERT-SE på telefonnummer 010-240 40 40 inom 6 timmar.

Steg 2: Skapa slutrapport inom fyra veckor i rapporteringsformuläret.

Steg 3: Skicka in IT-incidentrapporten till MSB via e-post: rapport@it-incident.se.

För information där skyddsvärdet kräver extra säkerhet tillhandahåller MSB en kryptolösning som avser att ge skydd vid överföring via e-post.

4 Incidentrapportering till Integritetsskyddsmyndigheten

Dataskyddsombudet ansvarar vid behov för att rapportera till Integritetsskyddsmyndigheten enligt nedan.

Inom 72 timmar från det att man upptäckt en personuppgiftsincident ska det rapporteras till Integritetsskyddsmyndigheten. Anmälan behöver dock inte göras om det är osannolikt att incidenten leder till några risker för enskildas fri- och rättigheter. De risker man tänker på är till exempel att enskilda förlorar kontrollen över sina uppgifter eller att deras rättigheter inskränks, att man utsätts för diskriminering, identitetsstöld eller bedrägeri, finansiell förlust, skadlig ryktesspridning samt brott mot sekretess eller tystnadsplikt.

Incidenten ska rapporteras via Integritetsskyddsmyndighetens e-tjänst och innehålla uppgifter om:

- Vilken typ av incident det är fråga om
- Vilka kategorier av personer som kan komma att beröras
- Hur många personer det berör
- Vilka konsekvenser incidenten kan få
- Vilka åtgärder man vidtagit för att motverka eventuellt negativa konsekvenser

5 Ansvarsroller i processen

5.1 Verksamma

Rapporterar incident enligt denna riktlinje.

5.2 Servicedesk

Analyserar och hanterar inkomna incidenter och vid behov vidarebefordrar till berörd funktion.

5.3 Berörd funktion inom IT-avdelningen

Analyserar och hanterar inkomna incidenter och vid behov vidarebefordrar till berörd funktion.

5.4 CSIRT

Analyserar och hanterar informationssäkerhetsincidenter och bedömer allvarlighetsgrad samt rapporterar IT-säkerhetsincident till MSB vid behov. Om misstanke att ett brott har begåtts kommer CSIRT-gruppen även att kontakta rättsvårdande myndigheter. Vid övriga typer av incidenter vidarebefordras dessa till berörd funktion.

5.5 Dataskyddsgruppen/Dataskyddsombud

Analyserar, hanterar samt rapporterar personuppgiftsincident till Integritetsskyddsmyndigheten vid behov. Vid övriga typer av incidenter vidarebefordras dessa till berörd funktion.

5.6 Ledning

Bistår vid behov med beslut om personella, materiella och ekonomiska resurser.

5.7 Avdelning kommunikation

Bistår vid behov med att informera intressenter.

5.8 Incident Manager

Loggar incident, identifierar nödvändiga resurser för att hantera incidenten, samordnar och informerar nödvändiga intressenter samt genomför slutanalys av incidenten efter slutförd åtgärd.

5.9 Incident Handler

Samordnar Incident Responders och informerar Incident Manager.

5.10 Incident Responder

Samlar in nödvändig data, begränsar incidenten, identifierar och åtgärdar rotorsak samt återställer normal drift.