Incidenthanteringsrutin för informationssäkerhet och dataskydd

1. Vad är en incident

En incident kan definieras som en oönskad och oplanerad händelse som kan påverka säkerheten i organisationens eller samhällets informationshantering, eller innebära en störning i organisationens förmåga att bedriva sin verksamhet. Se punkt 2 för information om hantering av incidenter.

1.1 Informationssäkerhetsincident

Oftast innebär det en brist i:

- Konfidentialitet - information har exponerats för fel person.
- Riktighet - informationen har brustit i tillförlitlighet, korrekthet eller fullständighet.
- Tillgänglighet - information fanns inte tillgänglig efter behov, i förväntad utsträckning samt för rätt person med rätt behörighet.

1.2 Personuppgiftsincidenter

En personuppgiftsincident är en informationssäkerhetsincident som även innefattar personuppgifter och därför kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. Det kan till exempel handla om oavsiktlig eller olaglig förstöring, förlust, obehörig ändring eller obehörigt röjande av personuppgift.

I vår verksamhet behandlar vi varje dag personuppgifter. Personuppgiftsbehandlingen är reglerad i den EU-gemensamma lagen GDPR/dataskyddsförordningen som bland annat styr hur vi ska agera vid en personuppgiftsincident (artikel 33-34 i GDPR).

Vissa uppgifter är enligt dataskyddsförordningen känsliga personuppgifter och har därför ett starkare skydd. De innefattar uppgifter om etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa, en persons sexualliv eller sexuella läggning samt genetiska och biometriska uppgifter. Om sådana uppgifter ingår i personuppgiftsincidenten är den extra allvarlig.

1.3 Exempel på incidenter

Konfidentialitet

- Ett beslut om bygglov skickas till fel person.
- En person får fel behörighet i ett system och får tillgång till ärenden som innehåller sekretess.
- En medarbetare luras av ett phishingmejl och lämnar ut sina kontaktuppgifter. Det är därför möjligt att någon använt dem för att logga in.
- Ett papper med känsliga personuppgifter glöms i skrivaren.
- En person tar sitt teamsmöte i kontorslandskapet och sekretessklassad information diskuteras.

Riktighet

- En bugg har gjort att flera uppgifter i ett system ändrats.
- Någon har missförstått en uppgift och lagt in ett stort antal felaktiga uppgifter i ett verksamhetssystem.
- Fel version av ett avtal har sparats i diariet.
- Vi har publicerat information om ett vägarbete på hemsidan men råkat skriva fel plats.
- Ett problem med integrationen mellan två system gör att data inte uppdateras som den ska.
- Ett akut ärende registreras som normalprioriterat och hanteras därför inte i tid.

Tillgänglighet

- Ett system ligger nere.
- Efter problem med kommunens mejlservrar kommer flera personer inte åt sin mejl.
- På grund av en överbelastningsattack fungerar inte kommunens hemsida.
- En medarbetare har fel behörighet och kan därför inte se sina ärenden.
- Ett par brev i ett postfack förstörs vid en vattenläcka.

2. Vad ska göras under och efter en incident?

Nedan finns de vanliga typerna av incidenter och en beskrivning av vad man ska göra i varje situation. Notera att en incident kan vara mer än en sak, exempelvis kan något både vara en personuppgiftsincident och en incident i förvaltningens egna verksamhetssystem.

Vid misstanke om personuppgiftsincident, kontakta alltid personuppgiftssamordnaren! Se mer info under 2.4.

Vid osäkerhet kring vad som gäller, kontakta informationssäkerhetsamordnaren som kan hjälpa till med guidning. Se mer info under 2.5.

Det är alltid bättre att höra av sig en gång för mycket än en gång för lite!

2.1 Misstänkt bluffmejl

- Vid misstänkt bluffmejl vidarebefordras mejlet till Supportcenter på supportcenter@helsingborg.se.
- Om information har lämnats ut eller om man har klickat på någon misstänkt länk ska man alltid ringa Supportcenter på telefon 042-10 50 50.

2.2 Incidenter i kommunövergripande system eller kommunövergripande infrastruktur

- Incidenter gällande kommunövergripande teknik såsom Outlook, Teams, internet, nätverksplatser (G:, S:, m.fl.), intranätet, Helsingborg.se eller inloggning med dina användaruppgifter i stadens gemensamma miljö rapporteras till Supportcenter via IT-portalen.
- Vid akuta ärenden ska man alltid ringa Supportcenter på telefon 042-10 50 50.

2.3 Incidenter i förvaltningens egna verksamhetssystem

- Vid misstänkt incident i förvaltningens egna verksamhetssystem kontaktas systemförvaltaren utan dröjsmål. Lista på vilka som är förvaltningens systemförvaltare finns på intranätet.

Systemförvaltaren ansvarar för att incidenten hanteras. Vid behov tar systemförvaltaren hjälp av Supportcenter eller leverantör för att lösa problemet.

2.4 Personuppgiftsincidenter

- Personuppgiftsincidenter rapporteras utan dröjsmål till förvaltningens personuppgiftssamordnare via förvaltningens funktionsbrevlåda för informationssäkerhet, informationssakerhet.sbf@helsingborg.se. Tänk på att inte uppge känsliga personuppgifter i mailet.

Personuppgiftssamordnaren ansvarar för att rapportera incidenten i kommunens e-tjänst för personuppgiftsincidenter samt vid behov till Integritetsskyddsmyndigheten, IMY. Samordnaren kan också behöva informera berörda registrerade.

Efter att händelsen är hanterad kommer personuppgiftssamordnaren att återkoppla till den som anmält incidenten.

2.5 Övriga incidenter, till exempel incidenter som gäller analog information

- Vid övriga incidenter, samt vid osäkerhet om vad som gäller, kontaktas förvaltningens informationssäkerhetssamordnare via förvaltningens funktionsbrevlåda för informationssäkerhet, informationssakerhet.sbf@helsingborg.se.

Informationssäkerhetssamordnaren ansvarar för att involvera rätt personer för att händelsen ska kunna hanteras.