Informationssäkerhetspolicy för IIS (Stiftelsen för Internetinfrastruktur)

Antagen av stiftelsens styrelse 2016-09-19. Senast fastställd 2018-09-18.

Bakgrund

IIS informationssäkerhetsarbete ska bedrivas på ett systematiskt, formaliserat och riskorienterat sätt och ta sin utgångspunkt i den internationella ledningssystemstandarden för informationssäkerhet, SS-ISO/IEC 27001:2017.

Syfte

Det övergripande syftet med IIS informationssäkerhetsarbete är att säkerställa ett väl avvägt skydd för IIS informationstillgångar så att rätt information är tillgänglig för rätt person vid rätt tidpunkt och på ett spårbart sätt.

Policyn omfattar alla informationstillgångar inom verksamheten utan undantag, oavsett om den behandlas manuellt eller automatiskt, och oberoende av i vilken form eller miljö den förekommer. All information ska vara klassificerad med avseende på känslighetsgrad.

Policy

Informationssäkerhetsarbetet ska ta sin utgångspunkt i regelbundna riskanalyser som syftar till att avväga rätt skyddsnivå i alla delar av verksamheten, samt motivera investeringar eller utbildningsinsatser för att:

- förhindra eller försvåra för obehöriga att få tillgång till information (sekretess)
- säkerställa att den information som produceras och bearbetas är korrekt, aktuell och fullständig (riktighet)
- bidra till att informationen är åtkomlig vid behov (tillgänglighet)
- säkerställa ursprunget av varje transaktion (spårbarhet)

För vart och ett av dessa områden ska organisatoriska, administrativa och tekniska skyddsåtgärder vidtas och dokumenteras på ett sådant sätt att det går att kontrollera att en tillfredsställande skyddsnivå uppnåtts.

Informationssäkerhetsskyddet ska granskas regelbundet. Avvikelser och incidenter ska systematiskt dokumenteras och följas upp, så att erfarenheter från dessa kan tas till vara som en del av det kontinuerliga förbättringsarbetet. Resultatet av säkerhetsarbetet ska årligen redovisas vid ledningens genomgång.

Ansvar

IIS vd är ytterst ansvarig för informationssäkerheten och för övergripande säkerhetsfrågor av styrande karaktär. Ansvaret omfattar att säkerställa att det finns ekonomiska och personella resurser med rätt kompetens för informationssäkerhetsarbetet.

Informationsägare (som exempelvis tjänsteägare, projektägare med flera enligt IIS rolldokument) ansvarar för informationssäkerheten inom sin respektive tjänst.

Varje medarbetare som hanterar informationstillgångar i någon form har också ansvar för att upprätthålla informationssäkerheten och förbinder sig att följa de säkerhetsföreskrifter som finns beslutade.