

Anvisningar för informationssäkerhet

Dnr:	L 2026/23
Dokumenttyp:	Anvisningar
Beslutsfattare:	Högskoledirektör
Beslutsdatum:	2026-10-12
Ansvarig avdelning:	IT-avdelningen
Dokumentansvarig:	Anna Frederiksen



Syfte

Detta dokument syftar till att säkerställa en systematisk och enhetlig hantering av informationssäkerhet inom Högskolan.

Bakgrund

Högskolan behöver tydliga anvisningar för att upprätthålla en enhetlig och väl avvägd nivå på informationssäkerhet, baserat på de krav som ställs på Högskolan som myndighet och som organisation.

Resultatet av åtgärderna nedan dokumenteras i Högskolans metodstöd för informationssäkerhet.

Informationsklassning

Informationsklassning ska revideras årligen för system som i någon aspekt uppnår nivå 2 eller högre.

Informationsklassning ska göras utifrån följande aspekter:

- Konfidentialitet – möjliga konsekvenser om icke behöriga personer får tillgång till informationen
- Riktighet – möjliga konsekvenser om informationen är felaktig
- Tillgänglighet – möjliga konsekvenser om behöriga personer inte kan nå informationen
- Spårbarhet – möjliga konsekvenser om möjligheten att se vem som läst eller ändrat informationen försvinner

Utifrån varje aspekt klassas informationen i fyra nivåer:

Nivå 1

Uppgifter där brister i säkerhet ger ingen, försumbar eller måttlig risk för skada på Högskolans verksamhet eller registrerade individer. Inga ytterligare säkerhetskrav ställs.

Nivå 2

Uppgifter som kan leda till risk för kännbar skada för Högskolans verksamhet eller registrerade individer. Exempel på sådana uppgifter är harmlösa personuppgifter, arbetsmaterial och uppgifter som används vid myndighetsutövning. De säkerhetskrav som ställs på informationen är att personuppgifter endast får hanteras inom Högskolans centrala IT-system och de tjänster där Högskolan tecknat personuppgiftsbiträdesavtal med leverantören.

Nivå 3

Uppgifter som kan leda till risk för allvarig skada för Högskolans verksamhet eller registrerade individer. Exempel på sådana uppgifter är känsliga och integritetskänsliga personuppgifter och uppgifter som omfattas av sekretess. Uppgifter inom nivå 3 ska skyddas av minst tvåstegsverifiering, får inte lämnas obevakade, och får endast lagras och bearbetas inom Högskolans nätverk eller i de molntjänster som Högskolan erbjuder för detta syfte. Material kan skickas som säkra meddelanden och i undantagsfall som krypterad e-post. Om en mottagare utanför Högskolan kräver att informationen överlämnas på ett specifikt sätt är detta i normalfallet tillåtet.

Nivå 4

Uppgifter som skulle kunna utnyttjas för att hota Sveriges säkerhet. Kontakta snarast Högskolans säkerhetsansvarig vid misstanke om uppgifter i Nivå 4.

Riskbedömning

Inom ramen för detta dokument förekommer två olika typer av riskbedömning, dels bedömning med informationssäkerhetsperspektiv, dels riskbedömning som ett delsteg inom konsekvensbedömning enligt dataskyddsförordningen.

Riskbedömning med informationssäkerhetsperspektiv

Denna riskbedömning ska identifiera, bedöma och hantera risker för Högskolans verksamhet. Riskbedömningen ingår som ett första steg i Högskolans samlade risk- och sårbarhetsbedömning av säkerhetsrisker, och syftar till att identifiera om ytterligare säkerhetsåtgärder behöver vara på plats för att ett IT-system ska kunna användas eller en behandling ska kunna utföras på ett säkert sätt. Säkerhetsåtgärderna kan vara tekniska, organisatoriska, fysiska eller personella.

Riskbedömning ska göras för system som innehåller information som i någon informationsklassningsaspekt uppnår nivå 2 eller högre och revideras årligen för de system som innehåller information som i någon informationsklassningsaspekt uppnår nivå 3 eller högre.

Konsekvensbedömning med integritetsperspektiv

Enligt dataskyddsförordningen måste Högskolan göra en konsekvensbedömning innan en behandling inleds om behandlingen sannolikt leder till en hög risk för individers rättigheter och friheter.

Konsekvensbedömningen består av två delar där steg 1 är en riskbedömning där konsekvens och sannolikhet bedöms utifrån den planerade tekniska lösningen för behandlingen. Båda stegen utförs inom Högskolans metodstöd för informationssäkerhet och i samråd med Dataskyddsgruppen. Steg 1 utförs för behandlingar som omfattar känsliga personuppgifter, mycket stora mängder personuppgifter, uppgifter om lagöverträdelser eller andra typer av behandlingar där risken preliminärt bedöms hög. Steg två utförs endast för de behandlingar där steg 1 visar att det faktiskt finns en hög risk för individernas fri- och rättigheter.