# Säkerhet - riktlinjer för informationssäkerhet och dataskydd

**Hitta i dokumentet**



## Syfte

Denna riktlinje är en konkretisering av Region Hallands säkerhetspolicy och beskriver vad regionen ska arbeta med för att ha ett effektfullt, systematiskt och riskbaserat informationssäkerhetsarbete.

## Bakgrund

Ett ändamålsenligt informationssäkerhetsarbete är en nödvändighet och en förutsättning för att kunna upprätthålla Region Hallands förmåga som en samhällsviktig aktör att nå sina verksamhetsmål samt vara en del av det civila försvaret. Det är även en förutsättning för en god patientsäkerhet, en kvalitativ och säker vård, en framgångsrik digitalisering samt ett ändamålsenligt skydd för den personliga integriteten för såväl invånare som medarbetare.

### Omfattning

Informationssäkerhetsarbetet inkluderar dataskydd, cybersäkerhet och IT-säkerhet. Utöver riktlinjen finns tillhörande rutiner som beskriver hur arbetet inom området ska genomföras, se IT och informationssäkerhet | Styrande dokument.

Roller och ansvar definieras i separata styrande dokument.

## Inledning

Ändamålsenlig informationssäkerhet förutsätter ett systematisk och riskbaserat arbete som är integrerat i det dagliga arbetet i alla verksamheter som hanterar information. Det innebär att säkerställa att informationstillgångar (den information som organisationens olika verksamheter hanterar samt de resurser som behandlar informationen. Exempel på sådana resurser är IT-system, datorer, och skrivare) identifieras, klassificeras och ges en lämplig

skyddsnivå i form av tekniska och administrativa skyddsåtgärder utifrån informationssäkerhetsperspektiven:

- Konfidentialitet - att information inte tillgängliggörs eller avslöjas för obehöriga
- Riktighet - att information är korrekt, aktuell och fullständig
- Tillgänglighet - att information kan nås när den behövs av behöriga användare

Utöver dessa perspektiv är även spårbarhet en viktig säkerhetsåtgärd för att säkerställa att informationens skydd upprätthålls, till exempel att den inte har ändrats, eftersökts eller lämnats ut till obehörig

Som stöd i arbetet att bedriva ett systematiskt och riskbaserat arbete har riktlinjen sin utgångspunkt i standarden för informationssäkerhet SS-ISO/IEC 27000-serie, organisationens verksamhetskrav samt gällande lagar och förordningar.
Informationssäkerhet omfattar skydd av såväl muntlig, pappersbunden och digital information.

## Ansvar och roller

För att uppnå och bibehålla en god informationssäkerhet inom regionen ska roller och ansvar definieras och tilldelas. Ansvaret sträcker sig från den politiska ledningen, genom tjänstemannaledningen till interna och externa medarbetare.
I partnerskapet strävas det att stödja varandra i att på bästa sätt skydda Region Hallands information.

## Förebyggande säkerhetsåtgärder

**Hantera informationssäkerhetsrisker och hot**
Systematiskt informationssäkerhetsarbete måste alltid anpassas efter en organisations specifika omständigheter samt förutsättningarna i omvärlden. Kontinuerliga interna och externa analyser ska genomföras integrerarat i Region Hallands planering och uppföljningsprocess.

**Riskhantering**
Som en leverantör av samhällsviktiga tjänster ska Region Halland kontinuerligt genomföra riskanalyser som ska ligga till grund för val av säkerhetsåtgärder. I analyserna ska det ingå en åtgärdsplan. Analyserna ska dokumenteras och uppdateras årligen.

**Informationsklassificering**
Information har en livscykel, från det att den skapas till att den gallras eller arkiveras. Informationens värde och riskerna kan variera under hela livscykeln. Region Hallands information och system ska vara dokumenterade, klassificerade och riskanalyserade enligt regionens fastställda modell. Resultat från informationsklassning och riskanalys utgör underlag för att tekniska och administrativa skyddsåtgärder införs på rätt nivå. Underlaget ska upprättas och underhållas så att det är aktuell och uppdaterat.
Grundprincipen är att informationsklassificeringen ägs och fastställs ur ett verksamhetsperspektiv.

**Kontinuitetshantering**
Kontinuitetshantering (Kontinuitetshantering) ska bidra till att Region Halland kan upprätthålla samhällsviktig verksamhet på en acceptabel nivå genom att bedöma konsekvenser, acceptabel avbrottstid, identifiera kritiska aktiviteter och ta fram åtgärdsbehov. Verksamheternas kontinuitetshantering bidrar med viktig information till arbetet med informationsklassificering.

Verksamhetens kontinuitetshantering tillsammans med informationsklassificering för aktuell informationstillgång ska utgöra underlag för vilka kontinuitetslösningar som väljs, hur reservrutiner ska utformas i verksamheten vid avsaknad av kritiska funktioner och informationstillgångar samt hur återgång till normalläge ska ske.

## Informationshantering

**Hantering av informationstillgångar vid lagring och överföring**
Säker informationsöverföring är en kritisk del av informationssäkerhet som syftar till att skydda informationen när den förflyttas mellan olika platser och parter. Informationssäkerheten ska vara säkerställd för att skydda information, utifrån klassificering, innan den får överföras. Lagring ska ske enligt informationshanteringsplanen.

**Hantera åtkomster, identiteter och loggning**
Grundprincipen för åtkomst ska baseras på vilken information användare behöver för att kunna utföra sina arbetsuppgifter. Tilldelad åtkomst ska hanteras under hela livscykeln, den ska tillhandhållas, ses över, ändras och tas bort vid behov.

Vid åtkomst till information med höga skyddskrav avseende konfidentialitet och/eller riktighet ska stark autentisering (exempelvis SITHS) användas.

Det ska vara möjligt att identifiera vilka personer och system som har åtkomst till organisationens information och tillgångar, samt vad de har för åtkomsträttigheter. Alla användar-ID ska vara unika och personliga.

Icke personliga inlogg såsom gruppinlogg eller inlogg för ”icke-mänskliga enheter” såsom robotar ska tilldelas restriktivt och ställer högre krav på exempelvis loggning och uppföljning.

Det ska finnas processer, verktyg för att skydda, kontrollera och hantera användare och administratörers identitet- och behörigheter.

**Logghantering**
För att erhålla spårbarhet och möjliggöra incidentutredningar och i efterhand kunna utreda vad som hänt och för att upptäcka avvikelser ska IT-resurser övervakas och loggas avseende användaraktiviteter, avvikelser, fel och informationssäkerhetshändelser. Omfattningen avgörs utifrån resultatet av informationsklassningen.

Loggar ska skyddas mot manipulation och obehörig åtkomst, sparas en viss tid och granskas regelbundet av loggadministratör för att tidigt kunna upptäcka och agera på avvikelser.

**Anskaffning, utveckling och ändring av IT-tjänster**

Anskaffning, utveckling och ändring av IT-tjänster (exempelvis molntjänster, nätverkstjänster eller programvarutjänster) ska i regel föregås av behovsanalys, informationsklassificering med riskhantering samt konsekvensbedömning (DPIA). Lämpliga säkerhetsåtgärder ska införas, dokumenteras, förvaltas och utvärderas så att adekvat skydd uppnås i IT-tjänsten.

**Distansarbete**
När arbete utförs på distans ska informationssäkerheten vara säkerställd för att skydda information på minst likvärdigt sätt som när medarbetaren arbetar inom Region Hallands nätverk.

## Externa samarbetspartners

För extern personal och tjänsteleverantörer ska åtkomster tidsbegränsas så de endast gäller för den tiden som behövs för att utföra uppgiften. Innan någon tilldelas åtkomst till information ska alltid en bedömning av den enskilde personen ske och en tystnads- och sekretessförbindelse upprättas.

**Extern personal**
Extern personal har samma ansvarsprinciper som medarbetare anställda i Region Halland. Den som anlitar entreprenör, inhyrd personal, konsulter eller leverantörer ska se till att dessa externa medarbetare i tillämpliga delar följer Region Hallands beslutade styrning inom informationssäkerhet (riktlinjer och rutiner).

**Hantering av tjänsteleverantörer**
Region Halland ska ha kontroll över vilka tjänsteleverantörer som finns inom organisationen som kan påverka konfidentialiteten, riktigheten och tillgängligheten vad gäller organisationens information. Dokumentation ska upprättas och underhållas så det finns en korrekt förteckning över tjänsteleverantörer.

Innan en extern leverantör får hantera Region Hallands information ska leverantörens lämplighet bedömas utifrån relevanta krav. De informationssäkerhetskrav som gäller för en leverantör ska regleras i avtal och dess efterlevnad ska regelbundet följas upp och utvärderas.

Minst motsvarande informationssäkerhetskrav ska ställas på externa leverantörer samt deras underleverantörer som om Region Halland hade tillhandahållit tjänsten i egen regi.

**Kontakt med myndigheter och särskilda intressegrupper**
Region Halland ska upprätta och upprätthålla kontakter med relevanta myndigheter och intressegrupper för att säkerställa ett lämpligt informationsflöde med avseende på informationssäkerhet.

## Personuppgiftsbehandling – dataskydd

Vid behandling av personuppgifter är det nödvändigt att ha en rättslig grund för den specifika personuppgiftsbehandlingen, samt ange syfte och ändamål. Region Halland ska efterleva de grundläggande dataskyddsprinciperna:

- Laglighet, korrekthet och öppenhet,

- Ändamålsbegränsning,
- Riktighet,
- Uppgiftsminimering,
- Korrekthet,
- Lagringsminimering,
- Integritet och konfidentialitet,
- Ansvarsskyldighet.

De registrerade har vidare ett antal fri- och rättigheter de kan åberopa, som Region Halland har en skyldighet att tillmötesgå.

**Personuppgiftsbiträdesavtal eller datadelningsavtal**
När externa aktörer behandlar personuppgifter för Region Hallands räkning eller när Region Halland behandlar andra parters personuppgifter ska behandlingen regleras i ett avtal. Syftet med dessa avtal är att klargöra rollfördelning och fastställa vem som är ansvarig för vad, i personuppgiftsbehandlingen

**Registerförteckning**
Dataskyddsförordningen ställer krav på Region Halland ska föra ett register över alla pågående samt utförda personuppgiftsbehandlingar under dess ansvar, så kallad registerförteckning.

**Konsekvensbedömning**
När Region Halland planerar personuppgiftsbehandling som sannolikt leder till en hög risk för de registrerade behöver det genomföras en konsekvensbedömning (DPIA). Det finns flera faktorer som kan anses öka risken för den registrerade vid en personuppgiftsbehandling, t.ex. användning av innovativ teknik, att personer övervakas eller att behandlingen omfattar känsliga personuppgifter. Syftet med en konsekvensbedömning är att förebygga risker och göra en bedömning avseende vilka säkerhetsåtgärder som krävs för behandlingen.

## Personrelaterad informationssäkerhet

Medarbetares kunskap och medvetenhet är ett av de viktigaste skydden mot informationssäkerhetsincidenter. Region Halland ska arbeta löpande med att skapa hög säkerhetsmedvetenheten hos verksamhetens anställda, för att stärka säkerheten i beteenden och arbetsuppgifter.

**Anställning och kompetensutveckling**
Vid rekrytering ska den anställdes samt eventuell konsults lämplighet prövas i förhållande till den tilltänkta rollen. Vid behov görs bakgrundskontroll och i förekommande fall även säkerhetsprövning.  Det ska även säkerställas att en ny medarbetare (såväl anställd som konsult) har fått information om eventuell sekretess och tystnadsplikt.

Vid avslut eller förändring av anställning eller uppdrag ska informationstillgångar återlämnas samt ska den anställde informeras om eventuell fortsatt tystnadsplikt.

Alla anställda ska få utbildning i informationssäkerhet utifrån vad som är relevant för medarbetarens arbetsuppgifter. Lämplig kunskapsnivå ska bibehållas under medarbetarens hela anställnings- eller uppdragstid.

Disciplinära åtgärder kan komma att vidtas när anställda brutit mot gällande regler för informationssäkerhet och dataskydd.

## Fysisk och miljörelaterad säkerhet

Region Hallands informationstillgångar ska skyddas genom att lokaler, som inhyser den utrustning som används för informationshantering, uppfyller nödvändiga säkerhetsåtgärder. Lokalen ska ha ett fysiskt skydd, skalskydd och tillträdeskontroll samt skydd mot angrepp, olyckor och naturkatastrofer. Nivån på säkerhetsåtgärder identifierats genom informationsklassning och riskhantering.

Utrustning som innehåller lagringsmedier bör granskas för att säkerställa att all känslig information och licensierade program har avlägsnats, överskrivits eller destruerats på ett säkert sätt före avveckling, före återanvändning samt vid eventuell stöld.

## IT-teknisk säkerhet

Verksamhetsinformation ska skyddas mot förlust, destruktion, förfalskning, obehörig åtkomst och otillåten utgivning.

**Inventering och hantering av hårdvaru- och mjukvarutillgångar.**
Verksamhetens samtliga fysiska och virtuella enheter som är anslutna till Region Hallands nätverk ska vara dokumenterade och godkända samt ha adekvat säkerhetskonfiguration. Detta gäller även den mjukvaran som används i våra system. Konfigurationen och dokumentationen ska vara aktuell och uppdaterad.

**Skydd av data**
Adekvata skyddsåtgärder (brandväggar, antivirus och säkerhetskopiering etc.) appliceras för att säkra informationen i de applikationer som förekommer på verksamhetens enheter. Detta innebär inte fullständig säkerhet då utvecklingen inom detta område är oerhört snabb. Alla medarbetare ska också bidra till ett gott skydd av data genom att följa de användarinstruktioner som finns.

Vid behov ska godkända krypteringslösningar och instruktioner hur dessa ska användas tillhandahållas. Krypteringslösningar ska bygga på etablerade standarder som t.ex. NIST 140-2 eller ISO/IEC 18033. Behov av kryptering ska baseras på informationsklassning.

**Sårbarhetshantering och penetrationstester**
Det ska genomföras regelbunden sårbarhetsskanning av verksamhetens enheter och applikationer för att säkerställa att våra processer och rutiner för regelbunden uppdatering och patchning (mindre rättning) följs.

Penetrationstester ska genomföras för att identifiera och utnyttja svagheter i människa, teknik och organisation och simulera en angripares mål och metoder.

**Lagring och säkerhetskopiering**

Det är viktigt att information lagras på ett säkert sätt och säkerhetskopieras så att den kan återskapas i händelse av haveri, oavsiktlig radering, kryptering av antagonist etcetera. Konfidentiell information får endast lagras i avsedda och godkända system och lagringsytor. Lagringsenheter tillhandahållna av Region Halland som är uppkopplade till nätverket säkerhetskopieras automatiskt. Lokal lagring av konfidentiell information, till exempel på en persondator, får endast ske om lagringsenheten eller filerna är krypterade av Region Halland godkänd metod för kryptering. Medarbetare som använder lokala lagringsmedier ansvarar själva för säkerhetskopieringen. Fysiska dokument som innehåller konfidentiell information ska förvaras inlåsta.

Säkerheten för informationen som ska överföras inom organisationen eller till andra aktörer ska upprätthållas och dokumenteras.

**Hantering av nätverksinfrastruktur**
Skyddsåtgärder och övervakning ska användas för att nå säkerhet för information i nätverk och anslutna tjänster det vill säga krav på konfidentialitet, riktighet och tillgänglighet. Krav på skydd ska inkluderas i avtal för nätverkstjänster om dessa tjänster tillhandahålls som outsourcade tjänster.

En grundläggande segmentering av nätverket ligger i att skilja interna nät från internet, samt att utvecklings-, test- och produktionsmiljöer ska vara skilda från varandra. Ytterligare segmentering av det interna nätet ska göras då det är motiverat av säkerhetsskäl genom att logiskt eller fysiskt skilja dem från varandra.

Dokumenterade driftsrutiner ska finnas och göras tillgängliga för de användare som behöver dem.

**Säkerhet i applikationer**
För systemutvecklings- och integrationsåtgärder ska informationssäkerhet designas och införas under utvecklingscykeln.

Outsourcad systemutveckling ska övervakas och styras och säkerhetsfunktionalitet ska säkerställas vid utveckling.

Endast godkända applikationer ska vara aktiverade och möjliga att använda i organisationens IT-miljö. Alla applikationer ska förvaltas av utsedd ansvarig som säkerställer livscykelhantering och distribution av säkra versioner.

## Informationssäkerhets- och personuppgiftsincidenter och avvikelser

Process, organisation och resurser ska finnas för att hantera incidenter och avvikelser på ett effektivt sätt, både internt och med externa leverantörer.  Informationssäkerhets- och personuppgiftsincidenter ska rapporteras, dokumenteras, eskaleras och följas upp inom respektive styrelse, nämnd och bolag, enligt gällande avvikelseprocess.

Rapporteringsskyldighet finns kopplat till olika myndigheter och samverkan. Denna skyldighet ställer krav på att rapportering kan ske både skyndsamt och samordnat då en och samma händelse ofta berör mer än en rapporteringsskyldighet.

Vid incidenter ska insamling och bevarande av bevis hanteras på ett verkningsfullt sätt för eventuella disciplinära och rättsliga åtgärder.

Lärdomar ska dras av inträffade incidenter för att stärka och förbättra säkerhetsåtgärderna.

## Efterlevnad och uppföljning

Informationssäkerhetsarbetet ska, som en del av den ordinarie verksamhetsredovisningen, regelbundet följas upp på central nivå och inom respektive nämnd, styrelse och bolag.

Uppföljningen ska ligga till grund för det ständiga förbättringsarbetet med en ändamålsenlig styrning och ett väl fungerande verksamhetsstöd kopplat till Region Hallands systematiska informationssäkerhetsarbete.

## Referenser

Rutiner kopplat till riktlinjen hittas på följande sida: IT och informationssäkerhet | Styrande dokument.

## Definitioner

Termbank för informationssäkerhet (msb.se).

## Uppdaterat från föregående version

Omgjord i sin helhet.