Dokumentansvarig
Informationssäkerhetsenheten
Jonas Jensen
Giltig från
2021-11-23
Dokumentnummer
RS-LED20-3246-1
Avser
Processområde: Hantera information
Dokumentkategori
Huvuddokument (styrande dokument)
Beslutad av
Regionstyrelsens beslut den 9 november 2021, § 242/21 för egen del under förutsättning att regionfullmäktige godkände Policy för informationssäkerhet den 23 november 2021, § 131/21

Riktlinje för informationssäkerhet

Innehållsförteckning

Inledning

Riktlinje för informationssäkerhet konkretiserar regionens informationssäkerhetspolicy. Riktlinjerna förtydligar externa krav på informationssäkerhet och omsätter dessa i interna krav.

Syfte och avgränsning

Riktlinjen förtydligar det delegerade ansvaret i linjeorganisationen och till särskilda roller gällande informationssäkerhet samt vilka åtgärder som ska vidtas för att analysera och skydda informationstillgångarna.

Riktlinjen utgår från författningar på området där följande utgör huvuddelen av externa krav, EU:s Dataskyddsförordning, lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, patientdatalag (2008:355), lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster, säkerhetsskyddslag (2018:585) och dess förordningar och föreskrifter.

Informationssäkerhet en introduktion

Informationssäkerhet ska skydda information oavsett hur den hanteras, lagras och kommuniceras. Skyddet utgörs av administrativa, organisatoriska, tekniska eller fysiska skyddsåtgärder.

Informationsmängder utgör informationstillgångar (digitalt eller analogt) som ska skyddas utifrån tre aspekter, att informationstillgången ska vara konfidentiell, riktig och tillgänglig. Lämplig nivå av skydd för en informationstillgång är baserat på säkerhetskrav, aktuell hotbild, risker med informationshanteringen och hur den exponeras.

Olika händelser (incidenter) som är avsiktliga eller oavsiktliga kan påverka informationstillgångarnas konfidentialitet, riktighet eller tillgänglighet på ett oönskat sätt.

Organisatoriska förutsättningar och digitalisering

Region Sörmland ska tillhandahålla vård, kultur och regional utveckling. För att möjliggöra detta i en allt mera digital samtid behöver regionen öka användningen av digitala lösningar.

Det innebär att tjänster som utgör kommunikation med invånarna och patienter ska kunna ske mera digitalt. Det innebär också i allt högre utsträckning att medicinska stödsystem som patienter använder i hemmet kan kommunicera med regionens vårdpersonal vilket stärker patientsäkerheten och förbättrar för patienterna. Processer och dokumentation sker i allt högra grad i informationssystem som medför ökad digital informationshantering inom verksamheten.

Dessa trender innebär också att nya eller förändrade hot riktas mot regionenens verksamhet och dess informationstillgångar. Den ökade informationshanteringen genererar också nya sårbarheter i vårt samhälle och regionens verksamhet.

Region Sörmland ska verka för en trygg och säker digital utveckling som tar hänsyn till de risker och sårbarheter som finns och uppstår i och med digitalisering, samt vidta åtgärder för att minska eller förhindra dem.

Termer och begrepp

Termer	Definition
Auktorisation	Godkännande av informationsbehandlingsstöd
Behörighet	Tilldelade rättigheter att behandla information eller ett systemstöd på avsett sätt
Dataskydd	Skydd av behandlingen av personuppgifter
Information	Data tolkat av människor
Personuppgift	Varje upplysning som avser en identifierad eller identifierbar fysisk person, varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
Informationsägare	Ansvarig för en informationsmängds/informationstillgångs skyddsbehov och avsedd användning och tillika riskägare.
Personuppgiftsansvarig (PuA)	En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.
Personuppgiftsbiträde	En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

Riskägare	Ansvarig för att acceptera risknivå efter vidtagna åtgärder.
Informationsklassning	Bedömning av skyddsvärdet utifrån konfidentialitet, riktighet och tillgänglighet för en informationstillgång
Informationstillgång	Informationsmängd, bärare eller hanterare av information som utgör ett värde för organisationen. Exempelvis informationsmängd hanterad i ett systemstöd eller analogt.
It-resurs	IT-utrustning eller enheter
Systemstöd	Grupp av it-komponenter, tjänster och it-resurser som utgör en sammanhållet system, exempelvis NCS cross, epostsystem, delar av it-infrastruktur.
It-säkerhet	Säkerhet i systemstöd för att uppnå och upprätthålla informationssäkerhet.
Konfidentialitet	Att information inte görs tillgänglig för obehörig
Riktighet	Att information är korrekt, aktuell och fullständig.
Spårbarhet	Möjlighet att entydigt härleda utförd aktivitet med information till användare eller systemstöd.
Tillgänglighet	Att information är åtkomlig och användbar för behörig
SCADA	*(Supervisory Control And Data Acquisition)* system för övervakning och styrning av processer eller kontrollsystem
IoT	*(Internet of things)* lösningar som är anslutna till nätverk eller internet utan användargränssnitt.
MdP	*(Mecinteknisk produkt)* lösning som syftar till att diagnostisera eller vårda patienter.
GDPR	Dataskyddsförordningen (EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679)
PDL	Patientdatalagen (2008:355)
NIS	lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
OSL	Offentlighet och sekretesslagen (2009:400)
HSLF-FS 2016:40	HSLF-FS 2016:40 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården
HSA-P	HSA-policy regelverk för hantering av HSA, gemensam katalog för regioner.
SITHS-P	SITHS-policy och tillitsramverk, gemensamt regelverk för utgivning av SITHS-kort.
Informationssäkerhetspolicy	Regionens gällande Informationssäkerhetspolicy

Informationssäkerhet

1. Regionen ska bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete för behandlingen av all information. Åtgärder ska vidtas som minskar riskerna till en acceptabel nivå.

Hänvisning: GDPR artikel 32, NIS 11§, HSLF-FS 2016:40 3 kap, informationssäkerhetspolicy.

Processer, regler och metoder för att uppnå detta baseras på svensk standard för ledningssystem ISO/IEC 27000. Regionen har som målsättning att ha ett ledningssystem för informationssäkerhet integrerat med övrig styrning och ledning som kan certifieras enligt 27001.

Organisation, roller och ansvar

Ansvarsfördelning

2. Regionen ska vidta organisatoriska åtgärder för att skydda all behandling av information. Organisation ska tydliggöra ansvar och roller för informationssäkerhet i regionen samt vilka uppgifter som åligger ansvarig och skapa förutsättningar för uppföljning och förbättring.

Hänvisning: GDPR artikel 5, 24, 25, 28, 32, PDL 2 kap, HSLF-FS 2016:40 3 kap, NIS 13§, 15§.

3. Regionen ska utse informationsägare som ensamt eller tillsammans med annan informationsägare bestämmer skyddsnivån och ändamålen med behandlingen av information.

Hänvisning: GDPR artikel 4, PDL 2 kap, HSLF-FS 2016:40 3 kap, NIS 13§, 15§.

4. Informationshanteringen i regionen ska vara baserad på behov av informationsbehandling för att tillgodose god kvalitet och patientsäkerhet samtidigt som behandlingen ska vara laglig och värna de registrerades rätt till integritet.

Hänvisning: GDPR artikel 5, PDL 1 kap.

Regionstyrelsen har det yttersta ansvaret för regionens informationssäkerhet och dataskydd. Regionstyrelsen är personuppgiftsansvarig för regionens samlade personuppgiftshantering och utser dataskyddsombud.

Regiondirektören ansvarar för att informationssäkerhet bedrivs i linje med informationssäkerhetspolicy och riktlinje för informationssäkerhet.

Ansvar för information och dess hantering följer det ordinarie verksamhetsansvaret. Detta gäller från regionstyrelsen ner till medarbetare. Detta innebär att den som är ansvarig för en verksamhet också är ansvarig för informationssäkerhet inom dennes verksamhet. Möjlighet finns för en verksamhetsansvarig att fördela arbetsuppgifter men inte att delegera ansvaret till annan.

För information som hanteras inom en verksamhet är denna verksamhet också informationsägare.

Exempelvis: Fastighetsverksamheten har ritningar över fastigheter, dessa används inom verksamheten och delas till andra men produceras och ägs enbart inom fastighetsverksamheten varför informationsägare är chefen för fastigheter eller motsvarande.

För information som hanteras inom flera eller alla verksamheter är den verksamhet alternativt stab eller verksamhetsområde som styr eller möjliggör informationshantering också informationsägare.

Exempelvis: HR tillhandahåller stöd för hantering av medarbetare och kräver att dessa hanteras i bland annat Heroma, informationsinnehållet finns i hela verksamheten och produceras och konsumeras i hela verksamheten men chefen för HR-staben är ansvarig och informationsägare.
Exempelvis: IT tillhandahåller stöd för e-posthantering inom och mellan organisationer för medarbetare och grupper i regionen genom epostsystem, informationsinnehållet finns i hela organisationen och produceras och konsumeras men chefen för IT är ansvarig och informationsägare.

När flera verksamheter inom ett eller flera verksamhetsområden, en stab eller motsvarande hanterar samma typ av information så är den överordnade verksamheten i form av verksamhetsområde, stab eller motsvarande chef informationsägare.

Exempelvis: Folktandvården har ett stort antal kliniker som alla hanterar tandvårdsjournaler, producerar och konsumerar, men för att skapa tydligt ansvar är chefen för folktandvården informationsägare.
Exempelvis: I Hälso- och sjukvården innebär det att chefen för detta verksamhetsområde är informationsägare för den journalinformation som hanteras i hela verksamhetsområdet. Det innebär också att för exempelvis journalsystem som används i flera verksamhetsområden och av privata aktörer finns det flera informationsägare som chefen för Karsudden, chefen för HoS och Chefen för Folktandvården, chef för PVC, m.fl.

När information hanteras inom ett projekt/uppdrag är beställaren informationsägare för informationen inom projekt/uppdrag. Beställaren är

också informationsägare för information och informationssystem som är ett resultat av ett projekt/uppdrag till dess att det överlämnats till verksamheten.

Exempelvis: Projekt A genomförs där känsliga personuppgifter kommer hanteras för att utarbeta ett resultat i form av verksamhetsförändring, då är beställaren informationsägare för denna behandling.
Exempelvis: It-projekt utarbetar ett systemstöd för verksamheten som ska tas i drift under projektet, då är beställaren informationsägare fram tills en verksamhet tar över resultatet och ett förvaltningsobjekt tar över drift och förvaltning.

Om otydlighet råder utifrån dessa principer om vem som är informationsägare för en specifik informationstillgång har regiondirektören rätt att tilldela informationsägarskap.

För informationsinnehållet ansvarar respektive verksamhet inom, av informationsägare, givna ramar.

Exempelvis: Kommunikationsstaben kräver att verksamheten anger viss information på regionens intranät som också tillhandahålls tekniskt vilket medför att chefen för staben är informationsägare. Det innebär att denne ska ange vilken typ av information och hur den ska hanteras, samt vilken skyddsnivå som ska uppnås ställs som krav mot it-förvaltningen. Däremot är respektive verksamhetschef innehållsansvarig för det som publiceras.
Exempelvis: I Hälso- och sjukvården där chefen för Hälso- och sjukvården är informationsägare för journalföring medan respektive verksamhet ansvarar för att producera och konsumera informationen enligt fastställda rutiner och alltså innehållsansvarig.

Ansvar i verksamheten

5. Ansvaret för informationssäkerheten är kopplat till det delegerade verksamhetsansvaret.

Hänvisning: Informationssäkerhetspolicy

Verksamhetsansvarig oavsett nivå ansvarar för informationssäkerhet inom sin verksamhet och för att informationssystem används i enlighet med avsedd användning och är innehållsansvarig.

Verksamhetsansvarig ansvarar för att utarbeta verksamhetsspecifika anvisningar, instruktioner, rutiner, checklistor om behov finns. Dessa får inte avvika mot regionövergripande styrande dokument.

6. Regionen ska säkerställa att medarbetare och chefer har kännedom, kunskap och förmåga att agera säkert utifrån de risker och hot som finns med informationshanteringen.

Hänvisning: Informationssäkerhetspolicy

Verksamhetsansvarig ansvarar för att alla medarbetare ges introduktion i informationssäkerhet och följer regler, rutiner och har en tillräcklig nivå av kompetens.

7. Regionen ska ha förmåga att identifiera och rapportera incidenter avseende informationshanteringen som kan komma att påverka verksamhetens kontinuitet, individers integritet eller skydd av informationstillgångar.

Hänvisning: GDPR artikel 33, HSLF-FS 2016:40 3 kap, NIS 14§, 16§, 18§, Informationssäkerhetspolicy

Verksamhetsansvarig ansvarar för att avvikelser och incidenter rörande informationshantering rapporteras.

8. Regionen ska föra register över alla personuppgiftsbehandlingar som genomförs.

Hänvisning: GDPR artikel 30.

Verksamhetsansvarig ska säkerställa att verksamhetens behandlingar av personuppgifter finns förtecknade i registerförteckning.

Medarbetarens ansvar

9. Regionen ska fördela ansvaret för informationssäkerheten där möjlighet att påverka säkerheten är som störst.

Hänvisning: GDPR artikel 5

Medarbetare inom verksamheten har ett ansvar för verksamhetens informationssäkerhet och att följa styrande dokument och verksamhetsspecifika instruktioner.

Medarbetaren har ett ansvar för att rapportera avvikelser, incidenter eller felaktig hantering av informationstillgångar.

Informationsägarens ansvar

10. Regionen ska vidta ändamålsenliga och proportionerliga åtgärder för att skydda information, nätverk och informationssystem gentemot de risker som hotar säkerheten.

Hänvisning: GDPR artikel 32, NIS 13§, HSLF-FS 2016:40 3 kap

Informationsägaren ansvarar för informationssäkerheten för aktuell informationstillgång och att hantera de risker som den utsetts för.

Informationsägaren ansvarar för att säkerställa att objekt, verksamhet eller leverantör som tillhandahåller systemstöd uppfyller kraven.

11. Regionen ska ha dokumenterade beslut om användning av informationssystem.

Hänvisning: GDPR artikel 4, 5, 32, NIS 13§, HSLF-FS 2016:40 3 kap.

Informationsägaren ska fatta beslut om auktorisation av informationssystem med fastställd skyddsnivå och avsedd användning innan det används i projekt/uppdrag eller verksamheten.

Informationssäkerhetschef

12. Regionen ska ha en utsedd person som samordnar informationssäkerhetsarbetet i regionen och rapporterar en sammanställning om informationssäkerhetsarbetet i regionen till ledningen.

Hänvisning: GDPR artikel 39, NIS 11§, HSLF-FS 2016:40 3 kap, Informationssäkerhetspolicy.

Informationssäkerhetsarbetet inom regionen samordnas av en informationssäkerhetschef som utgör en rådgivande roll och ansvarar för att:

- skapa förutsättningar för informationsägaren att ta sitt ansvar genom att tillhandahålla utbildningar, processer och metodstöd för riskbaserad skydd av informationstillgångar,
- utveckla och förvalta regionövergripande styrande dokument, processer, metodstöd, vägledningar eller rutiner för ett riskbaserat skydd av informationstillgångar,
- utveckla och förvalta utbildningskoncept och utbildningar för en tillräcklig säkerhetsmedvetenhet hos medarbetare och chefer,
- uppföljning av informationssäkerhet och rapportering till ledning och styrelse.

Dataskyddsombud

13. Regionen ska som personuppgiftsansvarig organisation ha en utsedd person som agerar dataskyddsombud med särskild oberoende ställning.

Hänvisning: GDPR artikel 37, 38.

14. Regionens dataskyddsombud ska stötta verksamheten i hur personuppgifter ska hanteras, vid konsekvensbedömning, övervaka efterlevnad, samarbeta med tillsynsmyndighet och var kontaktpunkt för de registrerade.

Hänvisning: GDPR artikel 38, 39.

Dataskyddsombudet utgör en oberoende rådgivande och kontrollerande funktion som ska agera i de registrerades intresse för att stärka dataskyddet i regionen. Denne ansvarar för att:

- ge råd och stöd i dataskyddsfrågor till ledning och verksamhet
- ta emot synpunkter och stötta de registrerade gentemot regionen
- följa upp dataskyddsarbetet i regionen
- vara kontaktperson gentemot tillsynsmyndighet för dataskydd

IT-säkerhetsansvarig

15. Regionen ska ha en utsedd ansvarig för att samordna och upprätthålla en teknisk säkerhetsnivå som motsvarar kraven för informationshanteringen och verksamheten som ska stödjas.

Hänvisning: NIS 13§.

Det ska finnas en utpekad it-säkerhetsansvarig som samordnar arbetet med säkerhetsarbetet i it-verksamheten och upprätthåller en tillräcklig teknisk säkerhetsnivå för it-drift och it-infrastruktur.

Den it-säkerhetsansvarig ansvarar för att it-verksamheten samverkar med statliga myndigheter som MSB:s CERT, Inera AB och SKR inom teknisk säkerhet.

It-säkerhetsansvarig utses av chefen för regionens it-verksamhet.

Objektägare eller motsvarandes ansvar

16. Regionen ska säkerställa att objektägare eller motsvarande stödjer informationsägaren i skyddet av informationstillgångarna.

Hänvisning: Informationssäkerhetspolicy

Objektägare eller motsvarande som tillhandahåller informationssystem har ansvar för att uppfylla de krav som informationsägaren ställer.

Objektägaren ska rapportera om informationsägare inte finns utsedd eller inte fastställer kraven och avveckla informationssystemet.

Kontakt med särskilda intressegrupper

Informationssäkerhetsforum syftar till att samverka och samordna it-verksamhetens arbete med informationssäkerhet. Forumet ska träffas fyra gånger per år med särskild fokus på incidenter, identifierade svagheter och sårbarheter.

Informationssäkerhetsgruppen i Sjukvårdsregionen Mellansverige ska främja samverkan inom informationssäkerhet mellan regionerna.

Kontakt med myndigheter och andra organisationer

17. Regionen ska säkerställa att etablerade metoder, rapporteringsvägar och kontakter finns med statliga myndigheter och andra organisationer när så krävs.

Hänvisning: GDPR artikel 33, NIS 18§, SITHS-P, HSA-P.

Regionen ska ha etablerade kontakter som främjar informations- och IT-säkerhetsarbetet i regionen och möjliggör kontakt för stöd och rapportering av händelser

Lämpliga kontakter för samverkan och stöd bör upprätthållas med andra myndigheter och organisationer av informationssäkerhetschef och IT-säkerhetsansvarig.

Dokumentstruktur informationssäkerhet

18. Regionen ska ha ett etablerat ledningssystem för att styra och följa upp informationssäkerheten.

Hänvisning: GDPR artikel 32, NIS 11§, HSLF-FS 2016:40 3 kap. SITHS-P, HSA-P.

Informationssäkerhetspolicy är regionfullmäktiges beslutade inriktning och målsättning kring informationssäkerhet.

Riktlinje för informationssäkerhet konkretiserarar roller och ansvar, processer och metoder för att analysera behov av skydd och fastställa skyddsnivå.

Handlingsplan för informationssäkerhetsarbetet är en tidsbegränsad handlingsplan med mätbara mål som ska omarbetas varje påbörjad mandatperiod som utgår från övergripande riskbedömning.

Anvisningar, instruktioner eller rutiner och checklistor utarbetas för att förtydliga hur processer och arbetet ska bedrivas.

Kravkatalog med föreslagna säkerhetsåtgärder som motsvarar behovet för respektive informationsklass utgör grund för informationsägaren vid kravställning internt och externt.

Handböcker, vägledningar och andra stöddokument tas fram centralt eller lokalt för att underlätta tillämpning och efterlevnad av styrande dokument.

Uppdelning av arbetsuppgifter

19. Regionen ska säkerställa att arbetsuppgifter och ansvarsområden som står i konflikt med varandra eller medför ökad risk för informationshanteringen utförs av olika personer.

Hänvisning: GDPR artikel 32, NIS 11§, HSLF-FS 2016:40 3 kap. och 4 kap. SITHS-P.

Arbetsuppgifter som utgör en för informationssäkerheten stor risk ska delas mellan olika personer som inte står i beroendeställning till varandra.

Exempelvis: Beställning av behörighet får inte genomföras av den vars behörighet det avser, beställningen ska sedan utföras antingen automatiserat och dokumenterat eller genom annan person.
Exempelvis: Tekniker som kan påverka it-stöd ska inte också kunna påverka loggar av vilka åtgärder som denne vidtar.

Personalsäkerhet

Före anställning

20. Regionen ska förvissa sig om att medarbetare kommer vara lojala gentemot svensk författning och interna regelverk för informationshantering.

Hänvisning: GDPR artikel 39, NIS 15§, Informationssäkerhetspolicy.

Medarbetare är den viktigaste resursen för att upprätthålla en god informationssäkerhet administrativt, organisatoriskt och tekniskt. Innan anställning eller avtal tecknas ska individens lojalitet och pålitlighet bedömas utifrån ett säkerhetsperspektiv, för att hantera de för tänkt uppdrag aktuella informationstillgångarna.

Vid särskilt kritiska arbetsuppgifter ur ett säkerhetsperspektiv ska hänsyn tas till behov av bakgrundskontroll inför anställning eller tilldelning av arbetsuppgift.

Exempelvis: Attesträtter till stora belopp bör föregås av bakgrundkontroll.
Exempelvis: Åtkomst som driftstekniker med möjlighet till stor påverkan på regionens förmåga att upprätthålla teknisk informationsinfrastruktur bör föregås av bakgrundskontroll.

21. Regionen ska säkerhetspröva den som ska delta i uppdrag som placerats i säkerhetsskyddsklass.

Hänvisning: Säkerhetsskyddslagen (2018:585).

Säkerhetsskyddschef ansvarar för säkerhetsprövning av individen och beslut om placering i säkerhetsklass. Säkerhetsprövning ska ske innan anställning eller kontraktering.

Under anställning

22. Regionen ska förvissa sig om att medarbetare har kännedom om vilket ansvar denna har för att skydda den information som hanteras under och efter att uppdraget avslutats.

Hänvisning: GDPR artikel 32, OSL, NIS 15§, SITHS-P, informationssäkerhetspolicy.

23. Regionen ska förvissa sig om att medarbetare har genomfört obligatoriska moment innan de tilldelas åtkomst till information.

Hänvisning: GDPR artikel 32, OSL, NIS 15§, SITHS-P, informationssäkerhetspolicy.

I samband med anställning eller kontraktering ska medarbetaren ges en introduktion och utbildning i informationssäkerhet och hur informationen i verksamheten ska hanteras. Närmaste chef ansvarar för att medarbetare genomför nödvändiga utbildningar och introduktioner.

Innan tilldelning av certifikat (SITHS-kort) för åtkomst till informationstillgångar eller grundläggande behörighet tilldelas till informationssystem eller lokaler där information hanteras ska grundläggande informationssäkerhetsutbildning och introduktion kring informationssäkerhet vara genomförd och godkänd.

Medarbetare ska inför varje förnyelse av certifikat (SITHS-kort) för åtkomst till informationstillgångar repetera grundläggande informationssäkerhetsutbildning.

24. Regionen ska förvissa sig om att ingen medarbetare som hanterar information eller säkerhetsåtgärder på ett felaktigt sätt har åtkomst till informationstillgångar.

Hänvisning: GDPR artikel 32, OSL, NIS 15§, 16§, HSLF-FS 2016:40 4 kap, SITHS-P, informationssäkerhetspolicy.

Medarbetares åtkomst till informationssystem, nätverk och informationstillgångar ska stängas av om medarbetaren bryter mot regelverk eller användningen utgör en allvarlig risk för it-infrastrukturen och eller informationstillgångar.

Avslut eller ändring av anställds ansvar

25. Regionen ska säkerställa att medarbetare endast har behörighet att komma åt uppgifter eller lokaler/utrymmen som behandlar information eller kan påverka informationshanteringen som är absolut nödvändig.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, 14§, PDL, HSLF-FS 2016:40 4 kap, SITHS-P.

Vid ändring av medarbetares ansvar, arbetsuppgifter eller organisatorisk placering ska aktuell chef säkerställa att åtkomst till informationssystem och lokaler är begränsat till behov och risk med åtkomst.

När medarbetare avslutar sin anställning eller uppdrag i regionen ansvarar chef för att all åtkomst till informationssystem och lokaler/utrymmen inaktiveras omgående och att all utrustning och alla informationstillgångar medarbetaren kontrollerar omgående återlämnas.

Exempelvis: Åtkomst till journalsystem eller epost inaktiveras, SITHS-kort klipps itu och avregistreras, mobiltelefoner, USB-minnen, pärmar med papper, datorer återlämnas.

Hantera informationstillgångar

26. Regionen ska hålla alla informationstillgångar dokumenterade och ordnade där ägare av informationstillgång framgår.

Hänvisning: GDPR artikel 30, OSL, NIS 11§, PDL 2 kap.

27. Regionens informationstillgångar, inklusive utrustning och enheter ska enbart användas för regionens verksamhet.

Hänvisning: GDPR artikel 5, 6, NIS 11§, PDL 2 kap.

Informationstillgångar som tillhandahålls av regionen är avsedda att användas som arbetsredskap vid tjänsteutövning. De får inte användas till annan verksamhet och endast i ringa omfattning användas i privat syfte under förutsättning att det inte negativt påverkar verksamheten.

Alla informationstillgångar ska vara inventerade och dokumenterade där det framgår vem som är informationsägare, med vilket syfte informationstillgången behandlas, vilket skyddsbehov samt vilket skydd som uppnås för informationstillgången.

28. Regionen ska säkerställa att alla informationstillgångar har ett riskbaserat skydd.

Hänvisning: GDPR artikel 32, OSL, NIS 11§, 13§, HSLF-FS 2016:40 3 kap, SITHS-P.

29. Regionen ska säkerställa att alla informationstillgångar skyddas mot otillgänglighet, oriktighet och spridning till obehöriga.

Hänvisning: GDPR artikel 32, OSL, NIS 11§, 13§, HSLF-FS 2016:40 3 kap, SITHS-P.

30. Regionen ska säkerställa att informationstillgångar och de risker som finns identifierade samt de skyddsåtgärder som genomförs är dokumenterade.

Hänvisning: GDPR artikel 5, NIS 12§, HSLF-FS 2016:40 3 kap, SITHS-P.

Riskbaserat skydd uppnås genom att skyddsåtgärder som vidtas står i proportion till risken som informationstillgången utsätts för. Åtgärder som ska vidtas för att uppnå ett dokumenterat och riskbaserat skydd för informationstillgångarna är att:

- kartlägga informationstillgångar,
- rättslig analys,
- informationsklassning,
- kravanalys och kravuppfyllnad,
- riskanalys.

Kartlägga informationstillgångar

Informationskartläggningen ska identifiera alla informationsmängder som behandlas och vad dessa innehåller för information, vilka verksamheter den stödjer och vad syftet med behandlingen är. Ansvarig ska framgå och kartläggningen ska hållas uppdaterad. Det ska framgå av förteckningen vilka informationstillgångar som krävs för återställning efter störning eller incident.

31. Regionen ska säkerställa att all behandling av personuppgifter är känd och dokumenterad.

Hänvisning: GDPR artikel 30, OSL, NIS 11§, 13§, HSLF-FS 2016:40 3 kap, SITHS-P.

Behandling av personuppgifter ska dokumenteras i regionens registerförteckning.

Rättslig analys av informationstillgångar

En rättslig analys ska genomföras och dokumenteras i syfte att identifiera de författningsmässiga kraven som ställs på aktuell informationsbehandling.

32. Regionen ska säkerställa att all behandling av personuppgifter är laglig.

Hänvisning: GDPR artikel 6, PDL 2 kap.

Förekommer personuppgifter ska laglig grund för behandlingen fastställas och dokumenteras i registerförteckningen.

33. Regionen ska säkerställa att personuppgiftsbiträden garanterar att den registrerades rättigheter skyddas och att kraven i Dataskyddsförordningen uppfylls för behandlingen.

Hänvisning: GDPR artikel 28.

34. Regionen ska säkerställa att behandling av personuppgifter av ett biträde ska regleras av ett avtal med instruktioner.

Hänvisning: GDPR artikel 28.

När personuppgifter hanteras av biträde ska detta regleras genom regionens avtal med tillhörande instruktioner.

35. Regionen ska säkerställa att personuppgifter endast överförs till tredjeland utanför EU/EES under förutsättning att det finns rättsligt stöd för överföringen.

Hänvisning: GDPR artikel 44.

Informationsägaren ska identifiera alla pågående och planerade överföringar av personuppgifter till tredjeland, utanför EU/EES. Dessa ska sedan analyseras för att möta de rättsliga kraven på överföringen.

36. Regionen får överföra personuppgifter till tredjeland utanför EU/EES som godkänts av kommission som ett land eller område som har adekvat skyddsnivå.

Hänvisning: GDPR artikel 45.

37. Regionen ska om avsaknad av beslut av EU kommissionen om att adekvat skyddsnivå råder i tredjeland säkerställa att lämplig skyddsnivå kan upprätthållas och att lagstadgade rättigheter för den registrerade kan omhändertas.

Hänvisning: GDPR artikel 46.

38. Regionen kan göra undantag när en överföring inte kan grunda sig på adekvat skyddsnivå eller lämplig skyddsnivå inte kan uppnås om det saknas alternativ.

Hänvisning: GDPR artikel 49.

Informationsägaren ansvarar för att bedöma, analysera och vidta åtgärder för att skydda personuppgifterna vid en överföring.

Genom auktorisationsbeslut beslutar informationsägaren om att överföringen ska ske. Som del i beslutsunderlaget ska en risk- och sårbarhetsanalys och konsekvensbedömning bifogas.

39. Regionen ska om inte rättsliga förutsättningar för överföring av personuppgifter utanför EU/EES i nya eller befintliga informationssystem finns utreda alternativ och fasa ut eller ersätta informationssystemet.

Hänvisning: GDPR artikel 44.

Om ett informationssystem ska ersättas med ett alternativ bör utredningen innehålla verksamhetens dokumenterade behov, risker med att fasa ut eller risker med att ersätta informationssystemet som grund för beslut.

Informationsklassning och riskklassning av informationstillgångar

Att klassificera informationstillgångar är att genomföra en teoretisk riskanalys som bygger på erfarenheter från tidigare riskanalyser och ger ett stöd för hur informationstillgångar ska skyddas.

40. Regionen ska klassificera alla informationstillgångar och dokumentera detta.

Hänvisning: GDPR artikel 32, OSL, NIS 11§, HSLF-FS 2016:40 3 kap.

Alla informationstillgångar ska analyseras och tilldelas en dokumenterad klassificering som motsvarar konsekvenserna för verksamhet och individ om informationen sprids till obehörig, är oriktig eller inte finns tillgänglig.

41. Regionens informationstillgångar ska klassificera enligt fastställd modell.

Hänvisning: GDPR artikel 32, OSL, NIS 11§, HSLF-FS 2016:40 3 kap.

Regionens modell för informationsklassning baseras på Myndigheten för samhällsskydd och beredskap (MSB) vägledning men har modifierats för att passa vår verksamhet. Modellen ska användas vid all klassificering av informationstillgångar för att möjliggöra informationsdelning inom och utanför regionen.

	Konfidentialitet (K)	Riktighet (R)	Tillgänglighet (T)
Synnerligen allvarlig konsekvens	**K4** Konsekvensen av obehörig åtkomst till information kan skada Sveriges säkerhet mer än i ringa omfattning.	**R4** Konsekvensen av obehörig förändring av informationen kan skada Sveriges säkerhet mer än i ringa omfattning.	**T4** Konsekvensen av obehörig otillgängliggörande av information kan skada Sveriges säkerhet mer än i ringa omfattning.
Mycket allvarlig konsekvens	**K3** Information som vid obehörig spridning kan leda till allvarlig skada för organisationen, tredje person eller enskild individ	**R3** Konsekvensen av obehörig förändring av informationen är allvarlig.	**T3** Information där förlust av tillgänglighet innebär allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Allvarlig konsekvens	**K2** Information som vid obehörig spridning kan leda till betydande skada för organisationen, tredje person eller enskild individ.	**R2** Konsekvensen av obehörig förändring av informationen är betydande.	**T2** Information där förlust av tillgänglighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Måttlig konsekvens	**K1** Information som vid obehörig spridning kan leda till betydande skada för organisationen, tredje person eller enskild individ.	**R1** Konsekvensen av obehörig förändring av informationen är betydande.	**T1** Information där förlust av tillgänglighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Ringa konsekvens	**K0** Information som vid obehörig spridning kan leda till ringa skada/obehag för organisationen, tredje person eller enskild individ.	**R0** Konsekvensen av obehörig förändring av informationen är ringa.	**T0** Konsekvensen av förlust av tillgänglighet är ringa.

Klassificeras informationen så att följderna får synnerliga konsekvenser för regionen och påverkan på Sveriges säkerhet ska särskild hantering ske.

Ostrukturerad information är pappershandlingar och elektronisk information som hanteras som dokument eller filer utanför strukturerade informationsmängder.

42. Regionens medarbetare ska klassificera ostrukturerad information som hen hanterar enligt fastställd modell.

Hänvisning: GDPR artikel 32, OSL, NIS 11§, HSLF-FS 2016:40 3 kap.

Medarbetaren ska klassificera ostrukturerad information som hen hanterar i generella systemstöd eller analogt. Den klassificeringen ska ske utifrån aspekten konfidentialitet och informationen ska märkas med klass.

Exempelvis: Ska alla dokument som skrivs och lagras i dokumenthanteringsverktyg eller på filarier klassificeras och märkas.

Exempelvis: Ska all e-post som skickas klassificeras och märkas.

	Konfidentialitet (K)	Riktighet (R)	Tillgänglighet (T)
Synnerligen allvarlig (SÄKERHETSSKYDD KÄNSLIGT)	**K4** Konsekvensen av obehörig åtkomst till information kan skada Sveriges säkerhet mer än i ringa omfattning.	**R4** Konsekvensen av obehörig förändring av informationen kan skada Sveriges säkerhet mer än i ringa omfattning.	**T4** Konsekvensen av obehörig otillgängliggörande av information kan skada Sveriges säkerhet mer än i ringa omfattning.
Allvarlig konsekvens (MYCKET KÄNSLIGT)	**K3** Information som vid obehörig spridning kan leda till allvarlig skada för organisationen, tredje person eller enskild individ	**R3** Konsekvensen av obehörig förändring av informationen är allvarlig.	**T3** Information där förlust av tillgänglighet innebär allvarlig negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Betydande konsekvens (KÄNSLIGT)	**K2** Information som vid obehörig spridning kan leda till betydande skada för organisationen, tredje person eller enskild individ.	**R2** Konsekvensen av obehörig förändring av informationen är betydande.	**T2** Information där förlust av tillgänglighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.
Måttlig konsekvens (INTERN)	**K1** Information som vid obehörig spridning kan leda till måttlig skada för organisationen, tredje person eller enskild individ.	**R1** **Konsekvensen av obehörig förändring av informationen är betydande.**	**T1** **Information där förlust av tillgänglighet innebär betydande negativ påverkan på egen eller annan organisation och dess tillgångar, eller på enskild individ.**
Ringa konsekvens (ÖPPEN)	**K0** Information som vid obehörig spridning kan leda till ringa skada/obehag för organisationen, tredje person eller enskild individ.	**R1** Konsekvensen av obehörig förändring av informationen är ringa.	**T1** Konsekvensen av förlust av tillgänglighet är ringa.

43. Regionens medarbetare ska hantera informationen i avsett informationssystem som har en säkerhetsnivå som motsvarar informationsklass.

Hänvisning: GDPR artikel 32, OSL, NIS 11§, HSLF-FS 2016:40 3 kap.

Information ska hanteras i systemstöd som tillhandahålls av regionen där säkerhetsnivå motsvarande informationens klassning. Egna eller alternativa lösningar får inte användas för att behandla regionens information.

Exempelvis: Ska alla dokument som innehåller SÄKERHETSSKYDDSKÄNSLIG information hanteras i avsett system frånskilt övriga IT-stöd.

Exempelvis: Ska e-post som innehåller MYCKET KÄNSLIG eller KÄNSLIG information skickas så ska denna krypteras så att endast avsedd mottagare kan ta del av innehållet.

Kravanalys och kravuppfyllnad för informationstillgångar

44. Regionens skyddsåtgärder för informationstillgångar ska utgå från kravkatalog för skydd av informationstillgångarna.

Hänvisning: GDPR artikel 32, OSL, NIS 11§, HSLF-FS 2016:40 3 kap.

Regionens kravkatalog anger säkerhetskrav för hur informationstillgångar ska hanteras utifrån resultatet från rättslig analys och informationsklassning.

Kravkatalogen är utformad med krav som tillsammans skyddar informationstillgångarna på en tillräcklig nivå.

Urval och uppfyllnad av krav ska dokumenteras. Krav som är relevanta men inte kan uppfyllas ska analyseras vid riskanalys.

Riskanalys av informationstillgångar

45. Regionens informationstillgångar ska ha en dokumenterad riskanalys inför beslut om auktorisation.

Hänvisning: GDPR artikel 32, NIS 11§, HSLF-FS 2016:40 3 kap.

Riskanalys ska genomföras och dokumenteras för att identifiera, analysera och omhänderta risker utifrån verksamhetsspecifika eller lösningsspecifika förutsättningar. I det ingår att analysera risken med att krav från kravkatalog inte är uppfyllda.

46. Regionen ska årligen revidera och fastställa informationstillgångarnas dokumenterade riskanalys.

Hänvisning: GDPR artikel 32, NIS 11§, HSLF-FS 2016:40 3 kap.

Riskanalys och riskhantering av informationstillgångar ska vara en kontinuerlig process som genomförs eller revideras minst årligen eller vid förändrade förutsättningar.

47. Regionen ska vid riskanalys av informationstillgångar analysera och dokumentera vård och tandvårds beroende till informationssystem för att upprätthålla kontinuiteten i verksamheten.

Hänvisning: NIS 3§, HSLF-FS 2016:40 3 kap.

Vård- och tandvårdsverksamhetens beroende till informationssystem eller nätverk för upprätthållande av kontinuitet av samhällsviktig verksamhet ska analyseras.

Regionens beroende till informationssystem för att upprätthålla verksamhet vid fredstida kriser, höjd beredskap eller i krig ska identifieras vid säkerhetsskyddsanalys.

För medicintekniska produkter är CE-märkningen en del i riskanalysarbetet då leverantörens riskanalys utgörs av det som denne kan kontrollera. Regionen ansvarar för att den medicintekniska produkten används i enlighet

med avsedd användning, risken med användningen i den lokala miljön (nätverk) och hur den används ska regionen analysera.

Om produkter som inte är CE-märkta ska användas på ett sätt som definierar det som en medicinteknisk produkt, alternativt att en CE–märkt produkt inte används i enlighet med avsedd användning ska regelverket för egentillverkning av medicinteknisk produkt följas.

48. Regionens ska om behandlingen medför hög risk för de registrerades fri- och rättigheter genomföra en konsekvensbedömning.

Hänvisning: GDPR artikel 35.

Personuppgiftsbehandlingar ska under vissa förutsättningar analyseras utifrån dess påverkan på den registrerades fri- och rättigheter i en konsekvensbedömning. En konsekvensbedömning ska göras om minst två av följande kriterier med behandlingen uppfylls:

1. utvärderar eller poängsätter människor,
2. i syfte att fatta automatiserade beslut som har rättsliga följder eller liknande betydande följder för den registrerade,
3. systematiskt övervakar människor,
4. behandlar känsliga personuppgifter enligt artikel 92 eller uppgifter som är av mycket personlig karaktär,
5. behandlar personuppgifter i stor omfattning
6. kombinerar personuppgifter från två eller flera behandlingar på ett sätt som avviker från vad de registrerade rimligen kunnat förvänta sig,
7. behandlar personuppgifter om personer som av något skäl befinner sig i ett underläge eller i beroendeställning,
8. använder ny teknik eller nya organisatoriska lösningar,
9. behandlar personuppgifter i syfte att hindra registrerade från att få tillgång till en tjänst eller ingå ett avtal.

Auktorisation

49. Regionens informationsägare ska innan informationssystem används i verksamhet, eller projekt/uppdrag fatta ett dokumenterat auktorisationsbeslut.

Hänvisning: GDPR artikel 5, NIS 11§, 13§ HSLF-FS 2016:40 3 kap, SITHS-P.

Inför användning av informationssystem ska informationsägaren besluta om auktorisation (driftsgodkännande).

Auktorisationsbeslut ska dokumenteras och innehålla ett underlag där informationssystemets syfte och avsedd användning framgår och validera att det lever upp till informationssäkerhetskrav. Auktorisationsbeslut hanteras i regionövergripande process.

50. Regionens informationsägare ska om auktorisationsbeslut fattas trots att skyddsnivån inte lever upp till krav analysera risken med beslutet och informera överordnad chef samt informationssäkerhetschef.

Hänvisning: GDPR artikel 5, NIS 11§, 13§ HSLF-FS 2016:40 3 kap, SITHS-P.

Om skyddsnivån inte lever upp till kraven eller att åtgärder från riskanalys inte åtgärdas och informationsägaren avvägt mot behovet behöver besluta om auktorisation ändå ska analys av bristerna och motivering till avsteg dokumenteras. Beslutet ska informeras till överordnad chef, övriga berörda och informationssäkerhetschef.

Objektägare ska säkerställa att auktorisationsbeslut finns innan denne tar över informationssystemet till förvaltning.

Dispenser och undantag

51. Regionens informationsägare ska om nödvändigt besluta om undantag gentemot informationssäkerhetskrav.

Hänvisning: GDPR artikel 5, NIS 11§, 13§ HSLF-FS 2016:40 3 kap, SITHS-P.

Undantag gentemot informationssäkerhetskrav och regler ska hanteras strukturerat och dokumenterat och beslutas av informationsägaren.

För att få besluta om undantag ska det bedömas vara absolut nödvändigt för att kunna bedriva verksamheten.

52. Regionens undantagsbeslut ska dokumenteras och överordnad chef samt informationssäkerhetschef ska informeras.

Hänvisning: GDPR artikel 5, NIS 11§, 13§ HSLF-FS 2016:40 3 kap, SITHS-P.

Undantagsbeslutet ska dokumenteras och överordnad chef samt informationssäkerhetschef ska informeras.

Undantag får aldrig vara permanenta eller bryta mot lag och bör maximalt ha en giltighetstid på 2 år.

Styrning av åtkomst

53. Regionen ska tilldela individuell behörighet för åtkomst till informationstillgångar.

Hänvisning: GDPR artikel 32, PDL 4 kap, NIS 13§ HSLF-FS 2016:40 4 kap, SITHS-P.

Alla identiteter i systemstöd och all åtkomst ska ske med unik identitet över tid, spårbar till fysisk person eller system.

Exempelvis: Identitet utgörs av HSA-id eller personnummer.

54. Regionen ska bestämma villkoren för tilldelning av behörighet för åtkomst till information som begränsar den till vad som är nödvändigt för att utföra arbetsuppgiften.

Hänvisning: GDPR artikel 32, PDL 4 kap, NIS 13§ HSLF-FS 2016:40 4 kap.

55. Regionen ska analysera behovet av behörighet och risken med behörighetsmodellen för informationssystem.

Hänvisning: GDPR artikel 32, PDL 4 kap, NIS 13§ HSLF-FS 2016:40 4 kap.

Regionen har anvisningar som anger hur och under vilka villkor som behörigheter tilldelas och behovs- och riskanalyser genomförs.
Analysen ska utgå från verksamhetens behov, uppdrag, kategorier av medarbetare, legitimation eller delegation, behandlingens omfattning och hur känslig information som görs åtkomlig samt om det finns särskilda omständigheter.

56. Regionen ska besluta om tilldelning av behörighet efter att en individuell behovs och riskanalys har genomförts.

Hänvisning: GDPR artikel 32, PDL 4 kap, NIS 13§ HSLF-FS 2016:40 4 kap.

57. Regionen ska dokumentera beslut om tilldelning av behörighet.

Hänvisning: GDPR artikel 32, PDL 4 kap, NIS 13§ HSLF-FS 2016:40 4 kap.

Behörigheter till information och informationstillgångar ska tilldelas efter en dokumenterad process som tilldelar minsta möjliga behörighet och där riskerna med tilldelning bedömts.

58. Regionen ska kontrollera tilldelad behörighet regelbundet minst 1 ggr/år och för behörighetsstyrande katalogen 4 ggr/år.

Hänvisning: GDPR artikel 32, PDL 4 kap, NIS 13§ HSLF-FS 2016:40 4 kap HSA-P.

Tilldelade behörigheter ska dokumenteras och vara spårbara samt följas upp regelbundet, minst en gång per år eller efter beslut från informationsägare.

59. Regionen ska kontrollera åtkomst till information genom regelbundna och återkommande stickprov.

Hänvisning: GDPR artikel 32, PDL 4 kap, NIS 13§ HSLF-FS 2016:40 4 kap.

Åtkomstkontroll ska dokumenteras och ske på sådant sätt att stora delar av personalen blir en del av kontrollerna under ett år.

60. Regionens informationsägare ska stänga av åtkomstmöjligheten för individer som bryter mot interna regler, medför en stor risk för regionen eller vid misstanke om brott.

Hänvisning: GDPR artikel 32, PDL 4 kap, NIS 13§ HSLF-FS 2016:40 4 kap,

Tillgång till informationstillgångar stängs av efter beslut av informationsägare eller medarbetarens chef.

Kryptering

61. Regionen ska skydda informationstillgångar som måste överföras eller lagras genom kryptering på sådant sätt att åtkomsten kan begränsas till behöriga.

Hänvisning: GDPR artikel 32, PDL 4 kap, OSL 7 kap, NIS 13§, HSLF-FS 2016:40 4 kap,

Vid kryptering av information vid lagring och överföring ska algoritmer och nyckellängder som bedöms pålitliga och etablerade enligt god standard användas.

Vid kryptering ska det finnas administrativa och tekniska skyddsåtgärder som säkerställer att krypteringsnyckeln hanteras säkert över sin livscykel.

Fysisk säkerhet

62. Regionen ska begränsa tillträde till utrymmen där informationstillgångar förvaras eller lagras till behörig medarbetare.

Hänvisning: GDPR artikel 32, OSL, NIS 13§ HSLF-FS 2016:40 3 kap,

Utrymmen där informationstillgångar förvaras eller bearbetas ska skyddas genom lämpliga tillträdesbegränsningar som säkerställer att endast behöriga får tillträde till informationstillgångarna. Endast medarbetare som har behov av att få tillträde för att kunna utföra sina arbetsuppgifter ska få tillträde.

Tillträdesbegränsningar bör baseras på informationstillgångarnas klassning och indelas i zoner. Tillträdesbegränsningar bör vara spårbar och kopplas till olika övervakningsfunktioner tekniskt och manuellt.

63. Regionen ska säkerställa ett proportionerligt fysiskt skydd mot miljömässiga och antagonistiska hot.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, HSLF-FS 2016:40 3 kap,

Informationstillgångar med stort skyddsbehov hanteras, lagras och bearbetas i utrymmen med skydd mot naturkatastrofer, olyckor eller angrepp.

Driftsäkerhet

Test, utveckling och utbildnings i systemstöd

64. Regionen ska säkerställa att informationssystem för test, utveckling och utbildning är skilda från informationssystem som används i verksamheten.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, HSLF-FS 2016:40 3 kap,

65. Regionen ska säkerställa att information för test av informationssystem inte består av produktionsdata.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, HSLF-FS 2016:40 3 kap.

Test-, utbildnings- och utvecklingsmiljöer ska skiljas från verksamhetens informationssystem och ska innehålla information som är fingerad.

Rutiner för drift och förvaltning

66. Regionen ska säkerställa att driftsdokumentation finns tillgänglig för den som behöver den för drift av informationssystem.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, HSLF-FS 2016:40 3 kap.

Driftsdokumentation är tillgänglig, fullständig och aktuell. Ändringar av dokumentationen, och kopior av dessa, bör ske strukturerat och enligt fastställd process.

67. Regionen ska säkerställa att säkerhetskopia av driftsdokumentation finns tillgängliga.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, HSLF-FS 2016:40 3 kap.

Det ska finnas en kopia av driftsdokumentation, liksom av andra dokument för systemstödets användning och drift viktiga dokument som förvaras

åtskilda från originalen. Dessa ska vara tillgängliga även i händelse av störningar i ordinarie drift.

Loggning och övervakning

68. Regionens informationssystem ska logga säkerhetspåverkande händelser.

Hänvisning: GDPR artikel 32, OSL, PDL 4 kap, NIS 13§, HSLF-FS 2016:40 4 kap.

Säkerhetspåverkande händelser utgörs av händelser som kan påverka informationens tillgänglighet, riktighet eller konfidentialitet i informationssystemet. Dessa händelser ska loggas och rutiner för hantering av dessa loggar ska finnas som säkerställer att åtgärder för att skydda informationssystem finns etablerade.

Ändringshantering

69. Regionen ska säkerställa att ändringar i informationssystem planeras, analyseras och införs strukturerat.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, HSLF-FS 2016:40 3 kap.

Ändringar i informationssystem planeras, analyseras och sker strukturerat där informationssäkerhetsaspekter på förändringen har analyserats. Större förändringar är att likställa med nytt informationssystem medan mindre ändringar kan begränsa analysen till den aktuella ändringens påverkan.

Säkerhetsuppdateringar

70. Regionen ska säkerställa att nödvändiga säkerhetsuppdateringar kan genomföras för informationssystemet.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, 3 kap.

Informationssystem och dess delkomponenter ska ha stöd av leverantörer genom support som omfattar säkerhetsuppdateringar. Om informationssystemet utvecklas internt ska förvaltning och utveckling inklusive säkerhetsuppdateringar tillhandahållas internt. Om support saknas ska kompensatoriska åtgärder vidtas.

Säkerhetsuppdateringar ska genomföras snarast och enligt fastställd rutin.

Skydd mot skadlig kod

71. Regionen ska skydda informationssystem och informationstillgångar mot skadlig kod.

Hänvisning: GDPR artikel 32, NIS 13§.

Informationssystem och informationstillgångar ska skyddas genom tekniska mekanismer för att identifiera skadlig kod och avlägsna den eller hålla den avskilt från informationssystem.

Säkerhetskopiering

72. Regionen ska säkerställa att säkerhetskopiering sker av informationstillgång och att den förvaras åtskild samt testas regelbundet.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, H HSLF-FS 2016:40 3 kap.

Säkerhetskopiering sker enligt rutin fastställd av informationsägaren. Dessa förvaras åtskilda från originalet och tester av dessa ska utföras regelbundet.

Sårbarheter och penetrationstest

73. Regionen ska säkerställa att tekniska sårbarheter och luckor i skyddet av informationstillgångar identifieras.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, H HSLF-FS 2016:40 3 kap.

Informationssystem ska kontrolleras gentemot kända tekniska sårbarheter regelbundet.

Penetrationstest ska genomföras för informationssystem med högt skyddsbehov.

Kommunikationssäkerhet

74. Regionen ska säkerställa att informationssystem skyddar överföring av information över nätverk.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, H HSLF-FS 2016:40 3 kap.

Informationsöverföring över nätverk som inte kan kontrolleras med stor säkerhet, det vill säga som inte är fysiskt avgränsat till en mindre grupp individer ska vara krypterad.

75. Regionen ska säkerställa att informationssystem skyddas mot angrepp.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, H HSLF-FS 2016:40 3 kap.

Skyddet mot angrepp ska kunna övervaka, upptäcka, identifiera, analysera och vidta åtgärder vid angrepp mot regionens informationssystem.

Utveckling, anskaffning och underhåll av systemstöd

76. Regionen ska säkerställa att vid utveckling, anskaffning eller förändring analyseras behovet av skydd.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, H HSLF-FS 2016:40 3 kap.

Vid utveckling, anskaffning eller större förändringar, exempelvis ny version eller nya moduler eller delkomponenter, ska informationstillgångarna analyseras för att fastställa skyddsnivå.

77. Regionen ska säkerställa att vid utveckling, anskaffning eller förändring av krav att skyddsnivå uppnås.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, H HSLF-FS 2016:40 3 kap.

Skyddsnivå med tillhörande informationssäkerhetskrav ska ingå i anskaffning/upphandling eller avtal samt vid utveckling och i förvaltning.

När informationssystem hanteras av annan part genom utkontraktering gäller samma regler och krav som för intern drift, men de särskilda riskerna det innebär ska omhändertas. En värdering om det är lämpligt med beaktande av regionens samhällsbärande uppdrag ska göras inför utkontraktering.

Vid utkontraktering av informationssystem för vårdverksamheten ska det bedömas om det är lämpligt där särskild hänsyn tas till vårdens samhällsviktiga tjänst och dess förmåga till kontinuitet vid bortfall av systemstöd.

Leverantörsrelationer

Upprättande och förvaltning av avtal

78. Regionen ska säkerställa att vid avtal med annan part som kommer hantera regionens informationstillgångar ska krav på informationssäkerhet regleras.

Hänvisning: GDPR artikel 32, OSL, NIS 13§, H HSLF-FS 2016:40 3 kap

Vid upprättande av kommersiellt avtal med annan part som ska hantera informationstillgångar åt verksamheten ska kraven på informationssäkerhet regleras. Om personuppgifter också behandlas ska särskilt avtal med instruktion reglera denna behandling.

Avtalet ska reglera avtalsuppföljning avseende informationssäkerhet och möjligheten till revision av informationssäkerheten.

Leverantörsberoenden

79. Regionen ska säkerställa att beroenden till externa parter minimeras.

Hänvisning: GDPR artikel 32, NIS 13§.

Risker som följer av beroendet av en leverantör ska minimeras och åtgärder vidtas för att hantera konsekvenserna av att leverantören inte kan fullfölja sitt uppdrag

Incidenthantering

80. Regionen ska säkerställa att det finns processer, metoder och rapporteringsvägar som identifierar och hanterar incidenter i informationssystem och informationstillgångar.

Hänvisning: GDPR artikel 33, OSL, NIS 14§, H HSLF-FS 2016:40 3 kap, SITHS-P, Informationssäkerhetspolicy.

Medarbetare och chefer ska rapportera incidenter och avvikelser som rör informationstillgångar eller informationssystem snarast och vid allvarliga incidenter ska dessa eskaleras.

81. Regionen ska säkerställa att incidenter dokumenteras, där omständigheter, dess effekter och de åtgärder som vidtagits framgår.

Hänvisning: GDPR artikel 33, OSL, NIS 14§, H HSLF-FS 2016:40 3 kap, SITHS-P, Informationssäkerhetspolicy.

Incidenter utgörs av avvikelser gentemot regelverk, processer, metoder eller tekniska brister alternativt av bedrägerier, stölder och tekniska angrepp.

82. Regionen ska säkerställa att incidenter rapporteras till myndigheter och till avtalsparter när så krävs.

Hänvisning: GDPR artikel 33, OSL, NIS 18§, SITHS- P.

Incidenter i hantering av personuppgifter ska rapporteras snarast eller senast inom 72 h till Integritetsskyddsmyndigheten.

Incidenter i tjänster som är nödvändiga för att regionen ska kunna utföra sin samhällsviktiga tjänst ska rapporteras till IVO via MSB snarast.

Incidenter i hantering av säkerhetsskyddskänslig verksamhet eller information ska rapporteras till Säkerhetspolisen.

Incidenter i hantering av SITHS-kort eller SITHS certifikat eller vid utfärdande av dessa ska rapporteras till Inera.

Kontinuitetshantering

83. Regionen ska planera för att kunna upprätthålla samhällsviktig verksamhet och viktiga funktioner för samhället vid bortfall av informationstillgångar och eller informationssystem.

Hänvisning: GDPR artikel 32, NIS 11§, 13§, 14§, HSLF-FS 2016:40 3 kap, SITHS-P, Informationssäkerhetspolicy.

Kontinuitetsplaneringen ska möjliggöra för samhällsviktig verksamhet eller annan funktion viktig för samhället ska kunna upprätthållas, på tillräcklig nivå, vid olika allvarliga händelser, störningar och oplanerade avbrott i tillgång till informationstillgångar.

Tillgång till informationstillgångar ska vara en integrerad del av verksamhetens kontinuitetsplanering.

Kontinuitetsplanerna ska testas regelbundet samt efter större organisationsförändringar eller nya informationssystem. Planerna ska underhållas genom regelbunden granskning och övning.

Uppföljning och mätning

84. Regionen ska säkerställa att regionens styrning omfattar informationssäkerhet.

Hänvisning: Informationssäkerhetspolicy.

Anpassning av regionens styrande dokument för informationssäkerhet sker utifrån förändrade författningar, rekommendationer på området och resultat från analyser av sårbarheter och risker. Även förändrad hotbild och förändrade förutsättningar, organisation eller verksamhet ska omhändertas vid utveckling av styrande dokument.

Uppföljning av efterlevnad

85. Regionen ska mäta och följa upp det systematiska och riskbaserade informationssäkerhetsarbetet.

Hänvisning: GDPR artikel 32, NIS 11§, 13§, 14§, HSLF-FS 2016:40 3 kap, SITHS-P, Informationssäkerhetspolicy.

Verksamhet ska genomföra egenkontroller, mätningar, uppföljning och revisioner där en analys av hur skyddsåtgärderna värderas i förhållande till aktuell hotbild.

Regionstyrelsen och bolagsstyrelsen ska följa upp status på informationssäkerhet inom dennes verksamheten genom ledningens genomgång.

Revisioner avseende informationssäkerhet ska göras regelbundet, och då driften finns hos extern leverantör ska det i avtalet finnas inskrivet krav på motsvarande revision.

Versionshantering

Datum	Kommentar
2021-09-22	Slutjustering skriftliga ändringar
2021-09-15	Stora förändringar av kravställningen med hänvisning till lagstiftning på området.
2021-09-03	Justering vad som krävs inför anställning/kontraktering
2021-08-30	Justeringar och rättningar språkligt och förtydligande av ansvar.
2021-05-27	Mindre justering i rättslig analys.
2021-05-10	Mindre justering i godkännande av skyddsnivå.
2021-04-29	Justering av auktorisationsbeslut för att stärka ansvaret i verksamheten.
2021-03-26	Justering av ansvar och informationsägarskap enligt dialog med verksamhetsområdena och rensning av krav och detaljerade instruktioner.
2021-01-20	Revidering efter remissrunda, samt justering av titel och tillägg kring analys av informationstillgångar och personuppgiftebehandling
2021-01-05	Revidering utifrån granskning
2020-12-22	Första utkast för granskning
2020-12-16	Rensning av hur krav på IT-nivå.
2020-12-15	Utkast till justering från aktuellt styrdokument riktlinje för informationssäkerhet