inera

Riktlinje för informationssäkerhet

inera

inera

inera

Version	Datum	Namn	Förändring
0.5	2015-05-05	Leif C	Internremiss
0.98	2016-01-04	Boo & Leif	Hantering av remissvar mm
0.983	2016-01-07	Leif C	Justerat Kap 6.1, 6.2, 8.4 och 11
1.0	*2016-01-12?*	*Leif C*	*Beslutad av vd*
1.1	2019-08-09	Fredrik R	Uppdatering Namnbyte från QLIS till Riktlinje för informationssäkerhet. Förtydligande om kontaktperson i verksamheten Tillägg om Dataskyddsombud Ändring i Riskanalys att en årlig övergripande ska göras Ädnring gällande bakgrundskontroll av personal Förtydligande gällande definition av informationstillgång Ändring gällande märkning i samband med klassificering Ändring gällande mobila enheter Byten av lösenord vid multifaktorautentisering Behörighet för administration av driftsmiljön Avveckling av lagringsmedia Tillägg om öppen källkod Krav på datahall Hantering av personuppgifter inom EU/EES Tillgänglighet och redundans Komponentskiktning Skydd mot skadlig kod Skydd mot överbelastning Säkerhetskopiering Loggning Övervakning Avancerade skalskydd Proaktiv hantering av tekniska sårbarheter Överväganden gällande säkerhetsgranskning Fjärranslutning Transportkryptering Segmentering Kontroll av anslutna enheter Rapportering av informationssäkerhetsincidenter Granskningar Molntjänster
1.1	2019-09-16	Johan A	Beslutad av vd

inera

1 SYFTE MED DETTA DOKUMENT

Att beskriva vad som ska göras för att uppnå ledningens viljeinriktning gällande informationssäkerhet så Ineras kunder, ägare, myndigheter, samarbetspartners samt anställda känner förtroende för vårt arbetssätt och att våra levererade tjänster håller en adekvat säkerhetsnivå.

2 ÖVERGRIPANDE INFORMATION

Dokumentet utgör Ineras riktlinje för informationssäkerhet, ingår i ledningssystemet för kvalitet och informationssäkerhet och är hierarkiskt underställd av Ineras styrelse beslutade Informationssäkerhetspolicy.

2.1 ANVISNINGAR KOPPLADE TILL RIKTLINJEN

Anvisningar förtydligar regelverket i denna riktlinje.

2.2 TERMER

I detta dokument benämns alla informationsbehandlingsresurser, IT-system och Informationssystem som "**informationssystem**".

Termen **"informationssäkerhet"** omfattar skydd av muntlig, pappersbunden och digital information och innebär en strävan att skydda information så att

- endast behöriga personer får ta del av den (konfidentialitet),
- det går att lita på att den är korrekt och inte manipulerad eller förstörd (riktighet),
- den alltid finns när den behövs (tillgänglighet) och
- att hanteringen ska i väsentliga delar vara spårbar (spårbarhet).

För övriga termer och begrepp hänvisas till SIS-TR 50:2015 Terminologi för informationssäkerhet.

2.3 OMFATTNING

Detta dokument gäller för all information och alla informationssystem som Inera förfogar över, beställt eller på annat sätt har tagit ansvar för oavsett var eller i vilken form hanteringen sker.

2.4 REVISION OCH STÄNDIG FÖRBÄTTRING

Dokumentet ska revideras vid större förändringar av Ineras förutsättningar, dock minst en gång per år.

2.5 REFERENSER OCH BILAGOR

- Ineras informationssäkerhetspolicy
- SS-ISO/IEC 27001:2017 Ledningssystem informationssäkerhet)
- SIS-TR 50:2015 Terminologi för informationssäkerhet.

inera

3 POLICY

Ineras riktlinje för informationssäkerhet är underordnad Ineras informationssäkerhetspolicy.

4 ORGANISATION

Detta kapitel beskriver vad som ska omfattas och beaktas organisatoriskt med syfte att säkerställa krav på informationssäkerhet.

4.1 ROLLER OCH ANSVAR INOM LEDNING OCH STYRNING

Roller och ansvar ska följa gällande linje- och förvaltningsorganisation där varje medarbetare ansvarar inom ramen för sitt uppdrag och mandat.

4.1.1 Ineras styrelse

Ineras styrelse fastställer policy för informationssäkerhet och har det övergripande ansvaret för informationssäkerheten inom företaget.

4.1.2 Ineras VD

Ineras VD har på styrelsens uppdrag att tillse att informationssäkerhetsarbetet bedrivs så effektivt som möjligt, genom att visa ett tydligt stöd och fördela resurser.

VD utser ansvarig för samordning av informationssäkerhetsarbetet.

4.1.3 Dataskyddsombud

VD utser ett Dataskyddsombud, DSO, med ansvar att kontrollera att personuppgifter behandlas i enlighet med Dataskyddsförordningen. Dataskyddsombudets ansvar och befogenheter ska följa Datainspektionens direktiv.

4.2 ROLLER OCH ANSVAR I VERKSAMHETEN

4.2.1 Kontaktperson för informationssäkerhet i verksamheten

Tjänsteansvarig, eller om denna roll saknas, enhetschef är kontaktperson för informationssäkerhetsfrågor i verksamheten.

4.2.2 Informationsägare

För varje viktig informationsmängd ska utses en informationsägare med uppdrag att hantera alla delar av informationssäkerheten som är relaterade till denna informationsmängd. För de tjänster som Inera tillhandahåller är detta normalt rollen Tjänsteansvarig.

5 RISKHANTERING

5.1.1 Riskanalys

Riskanalyser ska vara en naturlig del i Ineras hela verksamhet, från utveckling till avveckling.

Övergripande riskanalyser ska genomföras minst årligen.

Därutöver ska riskanalyser göras i då det kan förväntas att riskerna förändras, till exempel vid:

- nyutveckling av IT-system eller nya funktioner
- förändring av arbetsprocesser
- konfigurationsförändringar
- organisationsförändringar som kan påverka informationshantering

Riskanalyser är också ett viktigt verktyg som underlag till säkerhetsrelaterade beslut. Innan beslut tas ska eventuella risker analyseras.

Inera ska ha en fastställd modell för riskhantering.

Lämpliga åtgärder ska fastställas och implementeras utifrån resultaten av riskbedömningen.

6 PERSONALSÄKERHET

Detta kapitel beskriver vad som ska omfattas och beaktas i samband med rekrytering, anställning och avslutande av anställning.

6.1 FÖRE ANSTÄLLNING

6.1.1 Bakgrundskontroll

Bakgrundskontroll gällande sökande för anställning ska utföras där det beslutats vara lämpligt. Det ska ske i enlighet med relevanta författningar och etiska krav. Beslutet ska stå i proportion till verksamhetskraven samt klassificeringen av den information som den anställde ska ges åtkomst till samt de bedömda riskerna.

6.1.2 Anställningsvillkor

Samtliga medarbetare ska göras medvetna om sina skyldigheter enligt anställnings- eller annat tillämpligt avtal samt om gällande regler för informationssäkerhet och sekretess.

Inom Inera är sekretess lagstadgad för medarbetare (anställda och underleverantörer). En sekretessförbindelse är därför inte möjlig att använda, utan ersätts av sekretesserinran.

Deltar personen inte i verksamheten på sådant sätt att offentlighets- och sekretesslagen blir tillämplig, ska tystnadsplikten regleras civilrättsligt, dvs. i ett sekretessavtal.

Det ska vara tydligt att informationen ägs av Inera och inte får förstöras eller kopieras vid till exempel avslutande av anställning eller uppdrag.

6.1.3 Bisysslor

Lagen om offentlig anställning innehåller bestämmelser om skyldighet för offentliga arbetsgivare att informera anställda om vilka slags förhållanden som kan göra en bisyssla otillåten, enligt bestämmelsen om förbud mot förtroendeskadliga bisysslor. Denna vägledning ska finnas lätt tillgänglig för arbetstagaren.

Den anställde är skyldig att lämna de uppgifter som behövs för att arbetsgivaren ska kunna bedöma den anställdes bisysslor. Uppgiftsskyldigheten omfattar alla slags bisysslor.

I kollektivavtalet, Allmänna bestämmelser, finns ytterligare regler om bisysslor.

6.2 UNDER ANSTÄLLNING

6.2.1 Ledningens ansvar

Samtliga medarbetare ska uppfylla sina skyldigheter och tillämpa gällande regler för informationssäkerhet och sekretess.

6.2.2 Medvetenhet och utbildning vad gäller informationssäkerhet

Ineras målsättning är att en god säkerhetskultur ska genomsyra organisationen. Med detta menas inte bara att medarbetarna har god kunskap om vilka säkerhetsregler som gäller utan att de också använder gott omdöme och kritiskt ifrågasätter händelser som kan påverka säkerheten.

Samtliga anställda inom Inera ska få den utbildning i informationssäkerhet som krävs för att de ska kunna utföra sina arbetsuppgifter och för att säkerställa informationssäkerhetsmålen. Utbildningens omfattning ska vara anpassad till det ansvar och de befogenheter som gäller för befattningen.

6.2.3 Disciplinära åtgärder

Om en medarbetare gör sig skyldig till fel eller försummelse tilldelas berörd person en erinran. En erinran är en påminnelse om att medarbetaren har vissa skyldigheter och åtaganden som följer av anställnings- eller uppdragsavtalet samt övrig styrande dokumentation inom Ineras verksamhet. Erinran ska även innehålla en upplysning om att fortsatt misskötsel kan leda till uppsägning.

6.3 AVSLUT ELLER ÄNDRING AV ANSTÄLLNING

6.3.1 Avslut eller ändring av anställds ansvar

Det ska finnas en rutin som hanterar när medarbetare (anställda, praktikanter och inhyrda konsulter) slutar sin anställning eller uppdrag inom Inera och hur ansvarsuppgifter ska avlämnas och åtkomsträttigheter upphöra vid anställningens eller uppdragets slut. Nycklar, tjänstekort och eventuell övrig utrustning ska återlämnas.

inera

7 KLASSIFICERING

7.1 INFORMATIONSKLASSIFICERING

Klassificering av information och informationssystem ska genomföras på ett metodiskt och strukturerat sätt.

Ägare av informationstillgångar ansvarar för dess informationsklassificering.

Vid förändring av informationssystemets hantering av information eller ändamål, ska klassningen revideras.

7.2 DOKUMENTATION AV KLASSIFICERING

Resultat av genomförd informationsklassificering ska dokumenteras

Resultat av informationsklassificering ska inkluderas i dokumentation som upprättas kring informationssystem.

7.3 HANTERING

All hantering av informationstillgångar och informationssystem ska ske i överensstämmelse med dess klassificering så att rätt säkerhetsnivå upprätthålls. Säkerhetsåtgärder ska stå i paritet med informationens klassificering så att ett väl avvägt och kostnadseffektivt skydd uppnås.

8 HANTERING AV INFORMATIONSTILLGÅNGAR

Med informationstillgång avses här tillgångar som är relaterade till information och informationssystem. Exempel på tillgångar är tjänster, programvaror, information och datorer.

8.1 ANSVAR FÖR INFORMATIONSTILLGÅNGAR

8.1.1 Inventering av informationstillgångar

Tillgångar som är relaterade till information och informationssystem ska identifieras och förteckningar över viktiga tillgångar ska upprättas och underhållas.

8.1.2 Ägarskap av informationstillgångar

Informationstillgångar i förteckning över informationstillgångar ska tilldelas ägare.

8.1.3 Tillåten användning av informationstillgångar

Anställda och externa användare som använder eller har tillgång till Ineras informationstillgångar ska göras medvetna om de krav på informationssäkerhet som gäller för tillgångarna.

inera

8.1.4 Återlämnande av informationstillgångar

Vid avslutning av anställning eller vid uppdrags avslutande ska alla tidigare utställda fysiska och elektroniska tillgångar som ägs av, eller har anförtrotts Inera, återlämnas.

8.2 HANTERING AV LAGRINGSMEDIA

8.2.1 Hantering av flyttbara lagringsmedia

Flyttbara lagringsmedia ska användas endast om det finns verksamhetsskäl för detta.

Alla medier ska hanteras enligt Ineras anvisningar.

8.2.2 Avveckling av lagringsmedia

Lagringsmedia ska, när de inte längre behövs, avvecklas på ett sätt som säkerställer skyddet av den information som lagrats.

8.2.3 Transport av fysiska lagringsmedia

Lagringsmedia som innehåller information ska skyddas i överensstämmelse med sin informationsklass.

8.3 MOBIL UTRUSTNING OCH DISTANSARBETE

8.3.1 Regler för mobil utrustning

Mobil utrustning avser all utrustning som är avsedda för att och kan användas utanför Ineras lokaler och skalskydd. Vid användning av mobil utrustning ska särskild försiktighet iakttas för att säkerställa att verksamhetsinformation inte äventyras.

Regler och instruktioner för hantering av mobil utrustning och utrustning för distansarbete ska vara samma som för all Ineras utrustning. Då skillnaden mellan mobila enheter och bärbara datorer är väldigt liten ska all utrustning hanteras på samma sätt.

8.3.2 Distansarbete

Distansarbete avser alla former av arbete utanför Ineras lokaler och skalskydd.

Information som nås, bearbetas eller lagras på distansarbetsplatser ska skyddas på samma sätt som om arbetet utfördes i Ineras lokaler.

9 STYRNING AV ÅTKOMST

9.1 BEHÖRIGHETSSYSTEM

Det ska finnas behörighetssystem för att styra och kontrollera att användare har behörighet för åtkomst och ändring av data.

9.2 VERKSAMHETSKRAV FÖR STYRNING AV ÅTKOMST

9.2.1 Regler för styrning av åtkomst

Regler för åtkomst till information ska fastställas av informationsägaren. Det kan innefatta åtkomstbegränsningar för specifika roller, hur åtkomst beställs, tilldelas och tas bort samt olika typer av begränsningar för olika typer av information.

Om informationsägare är kund eller annan organisation ska informationssäkerhetsaspekter regleras i instruktioner och avtal.

Åtkomstkontroller ska motsvara informationens klassificering.

9.2.2 Tillgång till nätverk och nätverkstjänster

Användare ska endast ges tillgång till de nätverk och nätverkstjänster som de beviljats åtkomst till.

9.2.3 Behörighet för administration av Ineras driftmiljö

Administration av Ineras driftmiljö ska ske från Sverige.
Anlitande av eventuell underleverantör till Ineras driftleverantör, som behöver ha access för administration in i Ineras driftmiljö, måste godkännas av Inera drift.

9.3 HANTERA ANVÄNDARÅTKOMST

9.3.1 Registrera och avregistrera användare

Användare ska vara unikt identifierade
Gruppkonton är enbart tillåtna om spårbarhetkan erhållas på annat sätt, alternativt inte bedöms vara nödvändigt.

9.3.2 Tilldelning av användaråtkomst

Tillgång till alla informationssystem ska styras med hjälp av åtkomstkontroll. Det är användarens linjechef som ytterst beslutar om vilken åtkomst som behövs för att kunna utföra de arbetsuppgifter som ålagts användaren.

9.3.3 Hantering av privilegierade åtkomsträttigheter ("Admin")

Åtkomst med utvidgade rättigheter, så kallade administratörsrättigheter, ska begränsas till så få personer som möjligt. Åtkomsträttigheter ska alltid vara tidsbegränsade.

9.3.4 Hantering av användares inloggningsuppgifter

Hantering av användares inloggningsuppgifter ska ske på ett sådant sätt att dessa inte röjs.

9.3.5 Granskning av användares åtkomsträttigheter

Linjechef eller person som fått detta uppdrag delegerat ska granska användarnas åtkomsträttigheter med jämna mellanrum och efter ändringar, i syfte att säkerställa att de alltid är korrekta

9.3.6 Borttagning eller justering av åtkomsträttigheter

Åtkomsträttigheter till information och informationssystem ska tas bort vid avslutande av anställning, avtal eller uppdrag och justeras vid förändringar.

Åtkomsträttigheter vara tidsbegränsade.

9.4 ANVÄNDARANSVAR

9.4.1 Användning av inloggningsuppgifter

Användarens inloggningsuppgifter är personliga och ska hanteras så att annan person inte får tillgång till dem.

9.5 STYRNING AV ÅTKOMST TILL INFORMATIONSSYSTEM

Den som är inloggad i ett informationssystem ansvarar för vem som tar del av informationen som aktuell inloggning ger åtkomst till.

9.5.1 Begränsning av åtkomst till information

Tillgång till information och informationssystem ska vara begränsad till det som behövs för att kunna utföra arbetsuppgiften.

9.5.2 Autentisering

Metoder för autentisering till ett informationssystem ska utformas i enlighet med Ineras anvisning för detta.

9.5.3 Lösenordshantering

Som grundprincip ska multifaktorautentisering användas istället för enbart användarnamn och lösenord. Lösenordet behöver då inte bytas med periodicitet, såvida inte genomförd riskanalys stipulerat annorlunda.

Ett lösenords komplexitet ska följa Ineras anvisningar med mål att lösenord ska vara svåra att röja samtidigt som de är möjliga för användare att minnas.

9.5.4 Användning av privilegierade verktygsprogram

Användning av verktygsprogram som kan ha förmåga att kringgå säkerhetsåtgärder i informationssystem ska begränsas och styras strikt.

9.5.5 Åtkomstkontroll till källkod för program

Källkod ska skyddas mot förvanskning och spridning, och endast vara tillgänglig för behöriga. Källkod som beslutas vara öppen ska vara tillgänglig.

Organisationen ska vid behov säkerställa åtkomst till källkod som annan part förfogar över.

inera

10 KRYPTERING OCH PSEUDONYMISERING

Detta kapitel beskriver vad som ska omfattas och beaktas vid kryptering och pseudonymisering.

Med kryptering avser vi här att göra information som lagras eller överförs omöjlig att läsa för alla som inte ska kunna läsa den. För att göra informationen läslig igen krävs dekryptering.

Med pseudonymisering avses att byta ut för en person unika identifierare mot löpnummer.

10.1 KRYPTOGRAFISKA SÄKERHETSÅTGÄRDER

10.1.1 Regler för användning av kryptografiska säkerhetsåtgärder

Beslut om krypteringslösning ska tas om det bedöms som en lämplig säkerhetsåtgärd baserad på informationsklassning och riskbedömning.

Vilka krypteringssätt som är godkända ska beslutas. Anvisningar för detta ska revideras löpande och hållas aktuella.

10.1.2 Nyckelhantering

Rutiner för hantering av kryptografiska nycklar ska vara dokumenterad och belysa aspekter som hur nycklarna tas fram, hur de lagras och hur åtkomst ska ske.

10.1.3 Pseudonymisering

Där det är möjligt ska personuppgifter pseudonymiseras. Personuppgifterna, exempelvis personnumret, byts då ut mot ett löpnummer. Speciellt gäller detta när uppgifter lagras i statistiksyfte.

11 MOLNTJÄNSTER

Grundprincipen är att av molntjänster ska hanteras på samma sätt som övriga driftsformer och omfattas av Ineras säkerhetskrav i form av riktlinjer och anvisningar. Begreppet molntjänst är brett och innefattar olika typer av molntjänster med olika möjlighet till kontroll. Innan användning av en molntjänst ska ett beslut tas baserat på en sammanlagd bedömning om lämpligheten att använda sig av den specifika molntjänsten. I bedömningen ska ett flertal aspekter tas med. Exempelvis men inte uteslutande:

- legala aspekter
- informationens känslighet
- om molntjänsten befinner sig inom EU/EES
- vilken typ av molntjänst det är
- säkerhetsåtgärder för molntjänsten
- autentisering
- möjlighet till revision

- avtalets innehåll
- risker med behandlingen

12 FYSISK OCH MILJÖRELATERAD SÄKERHET

Detta kapitel beskriver vad som ska omfattas och beaktas angående fysisk och miljörelaterad säkerhet för informationssystem och informationstillgångar i egna lokaler såväl som extern drift.

12.1 SKALSKYDD

12.1.1 Skalskydd (mekaniskt och tekniskt skydd) ska utformas i enlighet med informationens och informationsbehandlingsresursens skyddsbehov, i enlighet med informationsklassificering.

12.1.2 Utformning av skalskydd ska föregås av en riskbedömning avseende även informationssäkerhet.

12.1.3 Inom skalskyddet ska lämplig kontroll finnas av exempelvis rätt anpassad temperatur, fuktförhållanden och strömförsörjning

12.2 KRAV PÅ DATAHALL

12.2.1 Datahalls placering

[redacted]

Det ska vid utlagd drift alltid vara känt för Inera var data och information fysiskt finns lagrade.

12.2.2 Hantering av personuppgifter

Data och information som innehåller personuppgifter får inte lagras eller behandlas i tredje land, dvs utanför Europeiska unionen och EES, i annat fall än där EU-kommissionen har fattat beslut om att ett land har en adekvat skyddsnivå.

12.3 UTRUSTNING

12.3.1 Kraven på fysisk säkerhet ska tillämpas för alla lokaler där information hanteras, samt för all utrustning som används för informationshantering exempelvis servrar, nätverk och kablar för strömförsörjning.

12.3.2 Inera ska med utgångspunkt i sin informationsklassning definiera kraven på fysisk säkerhet för informationstillgångar och därefter säkerställa att dessa hanteras och förvaras inom ett säkert utrymme som motsvarar kraven.

13 DRIFTSÄKERHET

Detta kapitel beskriver drift och underhåll av informationssystem.

13.1 DRIFTRUTINER OCH ANSVAR

För att upprätthålla säker och tillförlitlig tillgång till information och funktion ska administration, drift och underhåll av informationssystem ske på ett strukturerat och systematiskt sätt, enligt processer och anvisningar baserade på tillämpliga delar av ITIL.

13.1.1 Dokumenterade driftsrutiner

Det ska finnas systemdokumentation för varje informationssystem. Dokumentationen ska normalt bestå av system-, drift- och användardokumentation och omfatta all information som behövs för att informationssystemet ska kunna användas på ett säkert och korrekt sätt.

13.1.2 Ändringshantering

Förändringar som påverkar patient-, informationssäkerhet, organisation och verksamhetsprocesser ska hanteras formellt och spårbart.

13.1.3 Kapacitetshantering

Kapacitetsplanering syftar till att förutse och förebygga kapacitets- eller prestandaproblem. Regelbunden mätning och uppföljning av kapaciteten ska genomföras.

13.1.4 Separation av utvecklings-, test- och driftmiljöer

Inera ska ha en systemmiljö med åtskilda produktions-, utvecklings-, test- och utbildningsmiljöer. Säkerhetsreglerna för produktionsmiljöerna ska i relevanta delar även gälla för utvecklings- och testmiljöerna.

13.2 TILLGÄNGLIGHET

13.2.1 Tillgänglighet för informationssystem

Olika nivåer av tillgänglighet ska definieras för Ineras system och drift ska anpassas efter dessa nivåer i syfte att erhålla en kostnadseffektiv och säker drift.

13.2.2 Redundans

För vissa utvalda kritiska tjänster som Inera tillhandahåller, ska en tillgänglighet som är i det närmaste 100% kunna erbjudas. För att kunna säkerställa detta ska tjänsten byggas

redundant med extern lastbalanserare eller i en egen klustrad miljö. Tjänsten ska vara möjlig att uppgradera eller patcha utan påverkan på tillgänglighet.

13.2.3 Komponentskiktning

[redacted]

13.3 SKYDD MOT SKADLIG KOD

13.3.1 Säkerhetsåtgärder mot skadlig kod

Det ska finnas ett implementerat och kontinuerligt aktiverat skydd för att upptäcka och förhindra dataintrång och skadlig kod och som i möjligaste mån förhindrar

[redacted]

Uppgraderingen av skydd mot skadlig kod och sabotageprogram ska alltid installeras med kortast möjlig fördröjning.

En lämplig nivå av medvetenhet hos användarna ska säkerställas som innebär att de ska identifiera, åtgärda och rapportera möjliga virusangrepp.

Generellt ska försiktighet och restriktivitet iakttas när det gäller t.ex. bifogade filer i e-post, användning av CD/DVD, USB-minnen och annan flyttbar media samt ned-laddning av filer och program från Internet.

13.3.2 Skydd mot överbelastningsattack

[redacted]

13.4 SÄKERHETSKOPIERING

13.4.1 Säkerhetskopiering av information

Säkerhetskopiering av information och programvara ska utföras regelbundet.

Säkerhetskopior ska lagras fysiskt åtskilda från produktionsmiljön.

Säkerhetskopior ska skyddas på likvärdigt sätt som data i produktionsmiljön.

Lagringstid för säkerhetskopior ska vara beslutad.

Säkerhetskopior ska vid behov kunna krypteras.

Tester för att återskapa information från säkerhetskopior ska genomföras regelbundet och resultatet ska dokumenteras.

inera

13.4.2 Arkivering

Data och information, inklusive patientinformation ska kunna arkiveras för långtidslagring i ett arkivsystem. Arkivering ska uppfylla lagenligt ställda krav.

13.5 LOGGNING OCH ÖVERVAKNING

13.5.1 Loggning av händelser

Nivå av loggning ska följa Ineras beslutade anvisningar kring detta.

Det är informationsägarens ansvar att loggning sker så att det i efterhand minst går att följa enskilda användares aktiviteter.

Loggar ska sparas i enlighet med krav på spårbarhet för det aktuella informationssystemet och i förekommande fall enligt lagkrav. Beslut om lagringstid ska alltid finnas och ska säkerställa att loggar innehållande personuppgifter inte sparas längre än nödvändigt Loggar ska i möjligaste mån vara avidentifierade.

Inera ska proaktivt följa upp, värdera och korrelera logginformation från perimeterskydd och anslutna tjänster.

13.5.2 Skydd av logginformation

Loggarna ska vara skyddade mot obehörig åtkomst och manipulation samt finnas tillgängliga utifrån verksamhetens behov.

13.5.3 Administratörs- och operatörsloggar

Systemadministratörers och systemoperatörers aktiviteter ska loggas.

[redacted]

Grupp- eller gemensamma konton får Ej förkomma då spårbarheten går förlorad.

13.5.4 Övervakning

Samtliga Driftsmiljöer, Tjänsteobjekt, fysiska miljöer, enheter, processer etc. ska övervakas kontinuerligt. Övervakning ska syfta till att upptäcka fel respektive symptom som indikerar att fel kan förekomma i syfte att proaktivt undvika avbrott och brister.

13.5.5 Synkronisering av tid

Systemklockorna i alla relevanta informationsbehandlingssystem ska synkroniseras mot en och samma referenskälla för tid.

13.6 STYRNING AV INFORMATIONSSYSTEM

13.6.1 Installation av program

Uppdatering av operativsystem, tillämpningar och programbibliotek ska endast utföras av utbildade administratörer efter beslut från Inera.

Program som används ska underhållas på en nivå som stöds av leverantören.

Beslut om att uppgradera till en ny version ska väga in verksamhetskraven för ändringen och säkerheten i den nya versionen.

Ändringar ska testas i separat testmiljö som underlag för driftgodkännande och produktionssättning.

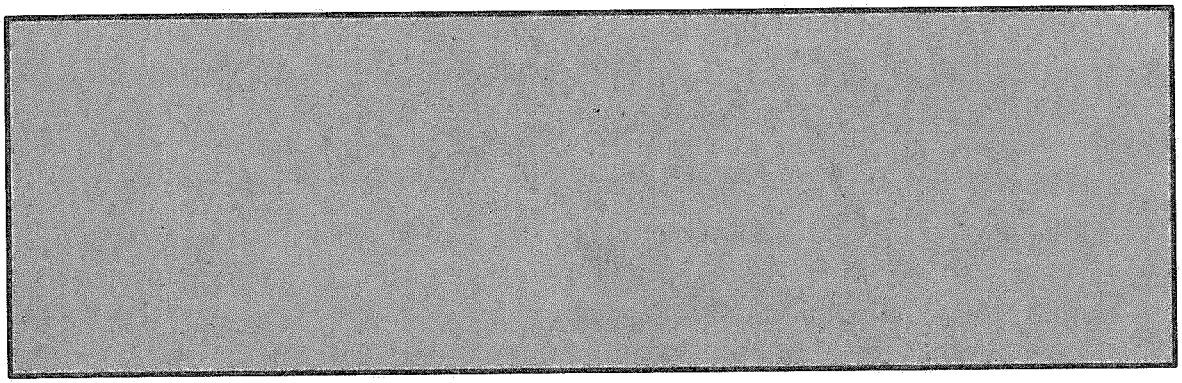
En plan för återställning (roll-back) ska finnas innan förändringar genomförs.

Gamla versioner av program ska arkiveras, tillsammans med all information och de parametrar som krävs, rutiner, konfigurationsinformation och supportprogram så länge data lagras i arkivet.

13.7 HANTERING AV TEKNISKA SÅRBARHETER

13.7.1 Proaktiv hantering av tekniska sårbarheter

Inera ska bedriva ett proaktivt säkerhetsarbete men även kunna agera reaktivt och kraftfullt och med noggrannhet vid eventuella uppkomna säkerhetsincidenter.



13.7.2 Restriktioner för installation av program

Okontrollerad installation av program kan leda till införande av sårbarheter och leda till obehörig åtkomst till information, förlust av riktighet, andra säkerhetsincidenter eller överträdelse av immateriella rättigheter.

- Användare ska tillåtas installera uppdateringar och säkerhetskorrigeringar till befintliga program.
- Användare ska tillåtas installera program som finns listade på "White List".
- Användare ska inte tillåtas installera program för privat bruk.

Installation av programvara som inte uppfyller något av kriterierna ovan ska ske i samråd med Intern-IT. Avsteg från whitelist görs efter riskbedömning.

13.8 ÖVERVÄGANDEN GÄLLANDE SÄKERHETSGRANSKNING

13.8.1 Åtgärder för att minimera påverkan vid säkerhetsgranskningar

Revision av informationssystem ska planeras noga för att minimera störningar i verksamhetsprocesser.

Tester som kan påverka tillgänglighet ska i möjligaste mån göras i produktionslika testmiljöer.

Behov av åtkomst till data i samband med revision ska analyseras och regler för åtkomst ska tillämpas.

Resultat från säkerhetsgranskningar ska hanteras som konfidentiell information och enbart delges de som bedöms vara behöriga.

Extern personal som ingår i säkerhetsgranskningar ska underteckna sekretessavtal omfattande den information som hanteras under granskningen.

14 KOMMUNIKATIONSSÄKERHET

Detta kapitel beskriver vad som ska omfattas och beaktas vid kommunikations- och nätverkssäkerhet.

14.1 HANTERING AV NÄTVERKSSÄKERHET

14.1.1 Säkerhetsåtgärder för nätverk

Nätverk ska hanteras och styras på ett sådant sätt att information i informationssystem skyddas.

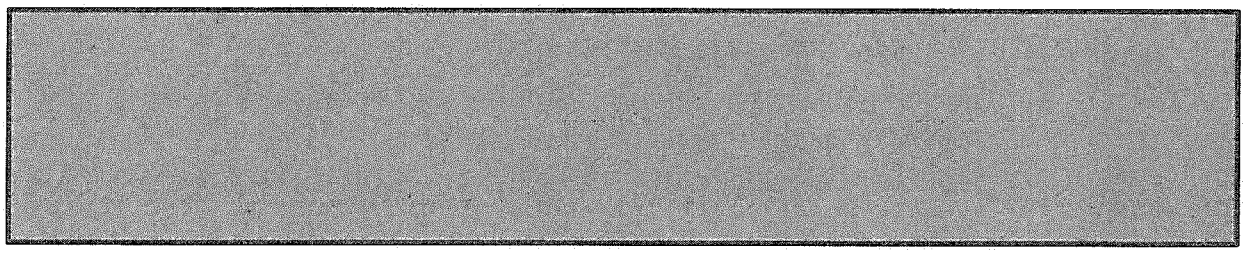
14.1.2 Fjärranslutning

Inera ska ha en för Inera gemensam teknisk lösning för fjärranslutning, VPN, för åtkomst till Ineras interna resurser. Andra lösningar för fjärranslutningar får inte användas.

14.1.3 Transportkryptering

Krypteringsmetoder och krypteringsnivåer ska väljas i enlighet med Ineras anvisningar för detta.

14.1.4 Segmentering av nätverk



14.1.5 Kontroll av anslutna enheter

Det är inte tillåtet att till Ineras nätverk ansluta enheter som inte tillhandahållits från Inera. Detta gäller inte gästnätet eller konsultnätet.

inera

14.2 INFORMATIONSÖVERFÖRING

14.2.1 Regler och rutiner för informationsöverföring

För alla typer av kommunikationsmedel ska formella regler, rutiner och skyddsåtgärder användas för att skydda överföringen och informationen.

14.2.2 Överenskommelser om informationsöverföring

Överföring av verksamhetsinformation mellan Inera och externa parter ska vara reglerad i överenskommelser som återspeglar informationens klassning.

14.2.3 Elektronisk meddelandehantering

Information som hanteras genom elektronisk meddelandehantering ska skyddas från obehörig åtkomst, från ändring eller från avbrott i tjänsten enligt den säkerhetsnivå som motiveras av informationens säkerhetsklassning.

15 SÄKER LIVSCYKEL HOS INFORMATIONSSYSTEM

Detta kapitel beskriver vad som ska omfattas och beaktas vid anskaffning, utveckling och underhåll av informationssystem.

15.1 SÄKERHETSKRAV PÅ INFORMATIONSSYSTEM

Informationssystem ska skyddas för att uppnå den konfidentialitet, riktighet och tillgänglighet som beslutad säkerhetsnivå anger under hela sin livscykel

Utförlig system-, användar- och driftdokumentation ska innehålla all information som behövs för att informationssystemet ska kunna installeras, driftas och användas på ett säkert och korrekt sätt.

Inga informationssystem får anskaffas eller utvecklas utan att det har gjorts en analys av hur systemet förhåller sig till lagar, avtal och regler som styr Ineras och Ineras kunders verksamhet.

15.1.1 Analys och specifikation av informationssäkerhetskrav

Krav som rör informationssäkerhet ska inkluderas i kraven för nya informationssystem och vid förbättringar av befintliga informationssystem.

Krav på informationssäkerhet ska utformas redan i projektplaneringsstadiet-

15.1.2 Säkerställande av informationssystem på Internet

Informationssystem på publika nätverk kräver specifika säkerhetsöverväganden mot typiska nätverksrelaterade hot som röjande av information för obehöriga, bedrägliga transaktioner och belastningsattacker. Det ska ske genom detaljerade riskbedömningar och val av motiverade säkerhetsåtgärder.

Transaktioner ska skyddas för att förhindra ofullständig överföring, felaktig styrning av nätverkstrafik, obehörig ändring av meddelanden eller obehörigt röjande.

inera

15.2 SÄKERHET I UTVECKLINGS- OCH SUPPORTPROCESSER

15.2.1 Regler för säker utveckling

Säker utveckling är en förutsättning för att bygga upp säkra informationssystem. Med säker utveckling avses:

- Säkerhetskrav ska identifieras och dokumenteras i design fas.
- Säkerhet i utvecklingsmiljön.
- Kontrollpunkter för säkerhet ska finnas i samband med milstolpar inom projekt.

15.2.2 Rutiner för hantering av ändringar i informationssystem

Införandet av nya informationssystem och större ändringar i befintliga informationssystem ska följa en formell process för ändringshantering som ska omfatta riskbedömning, analys av konsekvenser av ändringar och specificering av de säkerhetsåtgärder som kan motiveras.

15.2.3 Teknisk granskning efter ändringar i driftsmiljö

När driftmiljö ändrats ska informationssystem granskas och testas för att säkerställa att det inte innebär negativ påverkan informationssäkerheten.

15.2.4 Restriktioner för ändringar av informationssystem

Ändringar av informationssystem ska beslutas, styras och dokumenteras noggrant.

15.2.5 Principer för utveckling av säkra informationssystem

Processer för projektstyrning, systemutveckling och systemförvaltning ska finnas i ledningssystemet och tillämpas.

15.2.6 Säker utvecklingsmiljö

I utvecklingsprojekt ska informationssystem skyddas. Utvecklings- och testmiljöer ska vara separerade från produktionsmiljön.

15.2.7 Outsourcad utveckling

Inera ska övervaka och styra outsourcad systemutveckling.

15.2.8 Acceptanstestning av informationssystem

Process för acceptanstest, driftgodkännande och produktionssättning ska finnas och användas.

Informationssystem ska genomgå acceptanstest före driftgodkännande av beställare. I driftgodkännandet ska det ingå en uppföljning av säkerhetskraven.

15.3 TESTDATA

15.3.1 Skydd av testdata

Den information som används i utvecklings- och testmiljöer måste vara avidentifierad så att det inte går att utläsa uppgifter om personer eller annat data som kan leda till negativa konsekvenser för informationsägare.

16 LEVERANTÖRSRELATIONER

Detta kapitel beskriver vad som ska omfattas och beaktas angående leverantörsrelationer för att säkerställa skydd av de av Ineras informationstillgångar som leverantörer har åtkomst till.

16.1 INFORMATIONSSÄKERHET I LEVERANTÖRSRELATIONER

16.1.1 Informationssäkerhetsregler för leverantörsrelationer

När Inera köper IT-tjänster av extern part eller förlägger drift av informationssystem hos en sådan, ska minst samma regler för informationssäkerhet gälla som när driften hanteras i egen regi.

16.1.2 Hantering av säkerhet inom leverantörsavtal

Informationssäkerhetskrav ska avtalas med varje leverantör som kan tillgå, behandla, lagra, kommunicera eller som tillhandahåller infrastrukturkomponenter för Ineras information. Kraven ska spegla Ineras regelverk för det aktuella området samt hantera de risker som identifierats i upphandlingsprocessen. Informationssäkerhetskrav ska inkluderas tidigt och vara en del i hela upphandlingsprocessen.

16.2 HANTERING AV LEVERANTÖRERS TJÄNSTELEVERANS

16.2.1 Övervakning och granskning av leverantörstjänster

Inera ska regelbundet övervaka, granska och revidera leverantörers tjänste-leverans bl.a. avseende att informationssäkerhetsvillkor och bestämmelser i avtalen följs och att informationssäkerhetsincidenter och problem hanteras korrekt.

16.2.2 Ändringshantering av leverantörers tjänster

Vid ändring av leverantörers tjänster eller avtal ska en förnyad riskbedömning genomföras.

17 HANTERING AV INFORMATIONSSÄKERHETSINCIDENTER

Detta kapitel beskriver vad som omfattas och ska beaktas avseende förmåga att hantera fel som påverkar patientsäkerheten, användningen eller informationssäkerheten.

17.1 HANTERING AV INCIDENTER OCH FÖRBÄTTRINGAR

17.1.1 Ansvar och rutiner

I ledningssystemet ska det finnas processer som stödjer snabb, verkningsfull och korrekt hantering av informationssäkerhetsincidenter.

Processen för hantering av incidenter ska övas regelbundet.

17.1.2 Rapportering av informationssäkerhetsincidenter

Alla användare, anställda och leverantörer ska göras medvetna om sitt ansvar att rapportera informationssäkerhetsincidenter så snabbt som möjligt.

Incidentrapportering av informationssäkerhetsincidenter som följer av lagstiftning ska inkluderas i Ineras incidentprocess.

17.1.3 Rapportering av sårbarheter gällande informationssäkerhet

Allvarliga sårbarheter gällande informationssäkerhet ska hanteras som en informationssäkerhetsincident.

17.1.4 Bedömning av och beslut om informationssäkerhetsincidenter

Inera ska utvärdera varje informationssäkerhetsincident och bedöma och besluta hur de ska klassificeras. Resultaten av bedömningar och beslut ska dokumenteras detaljerat för framtida referens och verifiering.

17.1.5 Hantering av säkerhetsincidenter

Säkerhetsincidenter ska hanteras enligt Ledningssystemets processer.

17.1.6 Att lära av incidenter

Utvärdering av hanterade säkerhetsincidenter ska göras baserat på bevarade digitala spår för att minska sannolikheten eller påverkan av framtida incidenter.

17.1.7 Insamling av bevis

Digitala spår kan vara potentiella bevis och ska därför sparas minst till dess att allvarlighetsgraden i händelsen är helt klarlagd.

18 VERKSAMHETENS KONTINUITET

Detta kapitel beskriver vad som ska omfattas och beaktas vid hantering av verksamhetens kontinuitet.

Begreppet "kontinuitet" ska enbart användas ur ett verksamhetsperspektiv. För informationssystem ska begreppet "tillgänglighet" användas.

18.1 KONTINUITET FÖR INFORMATIONSSÄKERHET

18.1.1 Kontinuitetsplan

Det ska finnas en kontinuitetsplan inkluderat kontinuitetslösningar och avbrottsplaner som visar vilka åtgärder som vidtagits för att upprätthålla kontinuitet samt hur drift ska återgå till normal nivå efter ett avbrott.

18.1.2 Införa kontinuitet för informationssäkerhet

Ineras processer, rutiner och säkerhetsåtgärder ska säkerställa den nivå av kontinuitet för informationssäkerhet som anges i avbrottsplanen.

18.1.3 Styra, granska och utvärdera kontinuitet för informationssäkerhet

Inera ska verifiera de fastställda och införda åtgärderna för kontinuitet av informationssäkerhet med jämna mellanrum för att säkerställa att de är giltiga och verkningsfulla under störningar.

19 EFTERLEVNAD

Detta kapitel beskriver vad som ska omfattas och beaktas vid efterlevnad av informationssäkerhet för att säkerställa korrekt och säker drift av Informationssystem.

19.1 EFTERLEVNAD AV JURIDISKA OCH AVTALSMÄSSIGA KRAV

19.1.1 Identifiering av gällande lagstiftning och avtalsmässiga krav

All lagstiftning, relevanta författningsenliga och avtalsmässiga krav som berör Inera ska identifieras och dokumenteras i syfte att uppfylla kraven.

19.1.2 Immateriella rättigheter

Immateriella rättigheter inkluderar upphovsrätt till program eller dokument, mönsterrätt, varumärken, patent och licenser för källkod.

Ledningssystemet ska säkerställa efterlevnad av författningsenliga och avtalsmässiga krav relaterade till immateriella rättigheter och användning av proprietär programprodukter.

19.1.3 Skydd av dokumenterad (lagrad) information

Dokumenterad (lagrad) information ska skyddas från förlust, förstörelse, förfalskning, obehörig åtkomst enligt informationens säkerhetsklassning, oavsett media.

19.1.4 Skydd av personlig integritet och personuppgifter

Enligt personuppgiftslagen ska Inera som personuppgiftsansvarig vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna.

19.2 GRANSKNINGAR AV KVALITET OCH INFORMATIONSSÄKERHET

19.2.1 Extern granskning

Ineras ledningssystem för informationssäkerhet ska med jämna mellanrum eller när betydande förändringar sker genomgå oberoende granskning.

Resultatet av den oberoende granskningen ska dokumenteras och rapporteras till beställaren av granskningen. Dokumentation om genomförd granskning ska arkiveras.

inera

19.2.2 Intern revision av efterlevnad av ledningssystemet

Inera ska regelbundet granska efterlevnaden av policy, riktlinjer och anvisningar samt andra eventuella säkerhetskrav

19.2.3 Granskning av teknisk efterlevnad

Informationssystem ska granskas regelbundet avseende efterlevnad av Ineras styrande dokument.