Informationssäkerhetspolicy

EMPORI
Web application- & solutions

Innehåll

1 Inledning

1.1 Områden inom Informations- och IT-säkerhet

All information som i någon form hanteras eller lagras av Empori skall skyddas mot oönskad förändring, påverkan eller insyn. Det ska inte heller vara möjligt för obehöriga att ta del av information och de användare som har rätt till informationen ska komma åt den efter behov och inom önskad tid. Det är också av vikt att kunna identifiera vem som har gjort vad med informationen.

Krav på IT-säkerhet fastställs av Emporis avtal med kundföretag samt av lagstiftningar bl.a. sekretesslagen och dataskyddsförordningen (”GDPR”). Kraven kan sammanfattas i olika områden:

- **Sekretess** - Säkerställande av att informationen är tillgänglig endast för dem som har behörighet för åtkomst.
- **Riktighet** - Lämpligt skydd av information och behandlingsmetoder så att de förblir korrekta och fullständiga.
- **Tillgänglighet** - Säkerställande av att behöriga användare vid behov har tillgång till informationen och tillhörande tillgångar.
- **Spårbarhet** - Säkerställande av att registrering av avvikelser och andra säkerhetsrelevanta händelser täcker krav på tillförlitlighet och bevisbarhet.

Empori skall följa dels denna interna informationssäkerhetspolicy, dels lagar, förordningar och föreskrifter. Empori skall också följa vad man inom säkerhetsområdet anser vara god sed för att hantera organisation, processer och tekniska system ur ett informationssäkerhetsperspektiv.

1.2 Syfte med detta dokument

Syftet med detta styrdokument är att beskriva de processer och riktlinjer som Empori jobbar utifrån samt tillvägagångssätt för att uppnå de mål som bolaget har fastslagit gällande Informations- och IT säkerhet.

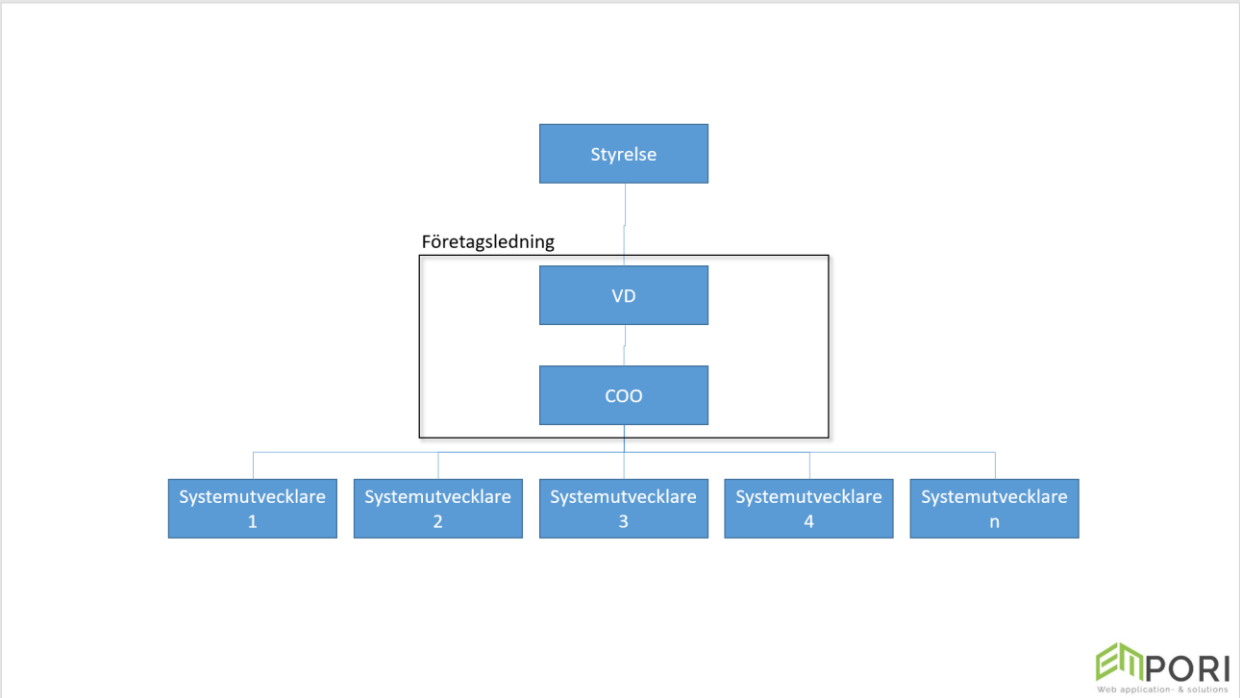
1.3 Omfattning

Emporis styrdokument för informations- och IT säkerhet, innehåller de riktlinjer som gäller för hantering av såväl information som informationsbärare i form av t.ex. datorer och servrar. Information kan finnas lagrad eller hanteras i digital form, men kan också vara i såväl skriftlig som muntlig form. Då Empori hanterar information mest i digital form har detta styrdokument en tyngdpunkt mot datorer och servrar information lagrad på dessa typer av informationsbärare.

1.4 Avgränsning

Det uppsatta regelverket beskriver den informationssäkerhet som ska gälla vid arbete med information, system och program inom Empori AB (benämns härefter ”Empori” eller ”bolaget”).

2 Säkerhetsorganisation – roller, ansvar & rapporteringsvägar



2.1 Allmänt

För att uppnå och bibehålla fastställda regler för informationssäkerhet krävs en tydlig ansvarsfördelning inom organisationen samt att säkerhetsarbetet koordineras.

2.2 Styrelse

Styrelsen för Empori har ansvar för att se till att det finns en väl fungerande organisation för informationssäkerhetsarbetet. Styrelsen ska initiera och stödja säkerhetsarbetet med resurser.

2.3 Företagsledning

Emporis företagsledning är på uppdrag av styrelsen ansvarig för efterlevnaden av Styrdokument för Informations- och IT säkerhet.

2.4 COO

COO har det yttersta säkerhetsansvaret för Empori samt ansvar för att regelverket efterlevs. I korthet omfattar ansvaret att:

- Ansvara för Emporis färdriktning i långsiktiga, strategiska IT- och informationssäkerhetsfrågor.
- Utforma regelverk för informationssäkerhet och uppdatera dessa vid behov.
- Upprätta former för kontinuitetshantering, riskanalys och incidenthantering.
- Utvärdera säkerhetsnivån inom Emporis tjänsteutbud.
- Hantera allvarliga säkerhetsincidenter.
- Rapportera avvikelser från styrdokument och riktlinjer till VD och företagsledning.
- Tillsätta resurser för IT-relaterade säkerhetslösningar inom ramen för den centrala IT-miljön
- Personal är informerad om och efterlever Emporis regler för informationssäkerhet.
- Personal har rätt utbildning för att sköta sina uppgifter i systemen.
- Anlitad tredje part efterlever säkerhetsreglerna i Emporis Informations- och IT säkerhetsdokument.
- Ge personalen möjlighet att delta vid säkerhetsutbildning.
- Avsätta tid för informationssäkerhet i lämpligt forum på arbetsplatsen.

COO har ansvar för alla informationstillgångar, och utrustning som är svår eller kostsam att ersätta. COO ska utfärda rutinbeskrivningar om hur informationen och utrustningen ska och får användas. Informationstillgångar ska vara förtecknade och i vissa fall även märkta.

2.5 Medarbetare

Alla anställda på Empori ska följa det regelverk som finns kring informationssäkerhet inklusive de regler som finns för personligt ansvar vid systemanvändning. Alla ansvarar för att inhämta sådan information och att regelverket följs. Vid oklarheter beträffande tillämpning av detta regelverk ska varje anställd kontakta sin chef. Oavsett om användande sker privat eller i tjänsten ska gällande regler och lagar följas som god moral och etik efterlevas. Endast de IT-verktyg som tillhandahålls via, eller i samråd med, IT-avdelningen samt är godkända av Empori får användas.

Medarbetare ska hantera sina inloggningsuppgifter på ett sätt så att obehörig åtkomst undviks, samt se till att IT-utrustning inte utsätts för obehörig användande av t.ex. familjemedlemmar. Pappersdokument och övriga lagringsmedia hanteras i enlighet med hur information har klassats.

2.6 Roller

Emporis anställda har tydliga Roller för att på ett säkert, effektivt och strukturerat sätt driva och utveckla bolagets tjänst.

Roll	Beskrivning
Systemutvecklare	Har hög teknisk kompetens som dagligen arbetar med att underhålla, förvalta och utveckla Emporis tjänster mot kunder. Innehar förmågan att driva och ta fram förslag om åtgärder vid incidenter. Har även kundkommunikation och delar av administration gällande Emporis tjänsteutbud. Aktiverar kundärenden och incidentaktivering av Empori ärendehanteringssystem. Emporis kundsupport är öppen helgfria vardagar 09.00 – 15.00 med lunchstängt 12.00 – 13.00. Dock finns möjligheten att via epost support@empori.se alltid starta ett supportärende.
COO	Operativt ansvarig för Emporis IT-miljö och kontakten med underleverantörer.
VD	Operativt ytterst ansvarig för Empori.

3 Informationssäkerhetspolicy

3.1 Samordning av informationssäkerhet

Emporis COO har ansvaret för att utarbeta, förvalta och följa upp regelverket för informationssäkerheten. Efter förankring från Emporis företagsledning godkänns och publiceras rutiner av COO.

3.2 Hantering av utomstående parter

Samverkan med externa leverantörer och konsulter ska regleras genom avtal och alla ska ha kännedom om Emporis regelverk kring i Informations- och IT säkerhet samt följa detta. Vid behov skall Personuppgiftsunderbiträdesavtal tecknas med leverantörer som hanterar information som klassats som personuppgifter.

3.3 Hantering av informationstillgångar

Tillgångar i detta sammanhang är det som för Empori har ett värde i form av information (till exempel utbildningsmaterial, systemdokumentation, utvecklingsverktyg etc.) och fysiska tillgångar (till exempel datorutrustning, telefoner, lagringsmedia, servrar mm.).

3.4 Klassificering av information

Informationsklassning är en delprocess i den administrativa säkerheten i arbetet med informationssäkerhet. Informationsklassning utgör grunden för hanteringen och behandlingen av information i Emporis informationssystem. För att komma fram till rätt skyddsnivå för information i informationssystem och databaser måste man veta vilken information som är viktig och varför den är viktig. Utifrån klassningen avgörs vem som har behörighet till informationen och hur information ska hanteras i olika situationer samt vilka delar av verksamheten som är ömtåligast för störningar och dess konsekvenser.

Företagsledningen för Empori ansvarar för att information som hanteras inom bolaget på ett korrekt sätt och ges ett adekvat skydd. Informationsklassning ska genomföras vid all form av utveckling av nya och befintliga system. En informationsklassnings hållbarhet är kortvarig eftersom informationen fortlöpande förändras. Därför skall informationen klassas årligen eller oftare vid behov. Vid klassificering av information skall extra beaktande ges information som kan klassas som personuppgift.

Klassificering av information skall ske i fyra nivåer

- Personuppgift (uppdelat på integritetskänslig eller icke-integritetskänslig)
- Konfidentiell
- Intern
- Publik

Hantering av klassificerad information skall ske enligt specificerade rutiner. Logisk eller fysisk separering av information skall i så hög grad som praktiskt möjligt tillämpas för information eller informationsresurser med olika klassificering. Det är standard att all information som inte klassats som Personuppgift skall klassas som Konfidentiell intill dess att den eventuellt får en lägre klassificering.

3.5 Märkning och hantering av information

Emporis informationstillgångar och utrustning som är svår eller kostsam att ersätta ska ha en utsedd ansvarig. Den ansvarige ska utfärda rutinbeskrivningar om hur informationen och utrustningen ska och får användas. Informationstillgångar ska vara förtecknade och i vissa fall även märkta.

3.6 Arkivering och gallring

Den information som hanteras i Emporis informationssystem skall bevaras, gallras och arkiveras som all annan information enligt bestämmelserna i lagar och dokumenthanteringsplaner.

3.7 Ändringsarbete

Allt ändringsarbete rörande informationsleveranser skall utföras med informationssäkerhetsaspekter i beaktande. Det skall också vara planerat, utvärderat och spårbart.

3.8 Åtkomstkontroll

En formell process för tilldelning av åtkomsträttigheter skall finnas. Åtkomsträttigheter till information och informationsresurser skall vara individuella och unika. Användandet av god säkerhetssed skall tillämpas vid utfärdande och hantering av autentiseringsmekanismer som t.ex. lösenord. Regelbunden uppföljning av åtkomsträttigheter skall genomföras för att säkerställa deras giltighet. Rutiner och kontroller för att förebygga otillbörlig åtkomst av nätverk, tjänster eller resurser skall finnas. Tilldelning och användning av privilegierad åtkomsträtt skall begränsas och styras. Höga behörigheter som avser enskilda system, t.ex. operativsystem, databassystem och individuella applikationer hanteras enligt särskilda rutiner.

3.9 Informationssystem och säkerhet

Rutiner skall finnas för att inhämta underrättelse om uppdateringar avseende tekniska sårbarheter och rutiner för att vidta adekvata åtgärder. Informationssystem skall, så långt det är möjligt, vara härdade för att minimera tekniska sårbarheter. Säkerhetsnivån på informationssystemen skall regelbundet kontrolleras för att uppdatera med de senaste mjukvarurättningarna och antivirusuppdateringarna mm. Ändringar av system och miljöer, inklusive dess komponenter, som används för leverans till kunden skall hanteras enligt etablerad ändringshanteringsprocess. Empori skall säkerställa att hantering av kundens information sker i enlighet med såväl de lagar, regler och avtalade krav som gäller för kunden.

3.10 Nätverk

Nät och nätverkstjänster skall säkras t.ex. med nätseparation både fysiskt och logiskt. Brandväggshantering skall användas för separation av åtkomstnivåer mellan nät. Nätverkstrafik skall krypteras överallt där det anses applicerbart. Intrångsskydd skall finnas i känsliga system.

3.11 Säkerhetskopiering

Säkerhetskopiering skall utföras och förvaras enligt säkra fördefinierade rutiner. Det skall utföras regelbundna slumpmässiga återläsningskontroller som säkerställer funktionalitet

3.12 Loggning och övervakning

Loggning och övervakning av Tjänster och funktioner skall utföras med hänsyn tagen till informationssäkerhet.

4 Rekrytering, anställning och avslut av personal

Insatser för att minska riskerna för mänskliga misstag samt bedrägeri och missbruk av informationstillgångar är en viktig del av Emporis personalarbete.

4.1 Säkerhet vid rekrytering av anställd och inhyrd personal

En kontroll av den sökandes identitet genomförs, för att klargöra att personen verkligen är den som utger sig för att vara. Detsamma gäller vid anlitande av tillfällig personal.
Följande steg genomförs inför anställning:

- Bakgrundskontroll av CV med tillhörande bilagor
- Utbildning med klargörande om det ansvar rollen innebär
- Kontroll av referenser
- Undertecknande av informationssäkerhetspolicy med tillhörande riktlinjer

Det skall framgå tydligt av anställningskontrakt en anställds ansvar avseende informationssäkerhet och vad följderna kan bli om någon bryter mot Emporis informationssäkerhetspolicy och riktlinjer. Empori skall ha återkommande utbildningar i säkerhet för personal och konsulter minst årligen för att upprätthålla gällande informationssäkerhetspolicy. Varje anställd skall kunna förstå och redogöra för Emporis informationssäkerhetshantering inom de områden personen verkar. Utbildningen skall även innehålla delar om hur de tekniska systemen skall användas på bästa sätt.

4.2 Säkerhet vid avslutande av anställning

När medarbetare avslutar sin anställning ansvarar COO för att behörigheter avslutas.
Vid avslut av anställning eller avslutande av konsultkontrakt skall fördefinierade processer finnas för att avveckla rättigheter och åtkomst. Rutiner skall finnas för att återlämna tillgångar t.ex. datorer, mjukvaror och annan media som kan innehålla säkerhetsklassad information.
Utöver ovan skall

- Information som inte behövs för Emporis framtida verksamhet tas bort från servrar och datorer.

5 Fysisk säkerhet

Den fysiska säkerheten syftar till att skydda mot obehörigt tillträde och åtkomst, skador och störningar. Ett bra fysiskt skydd av lokaler, utrustning och dokument ska eftersträvas. Därför ska Emporis lokaler förses med passagekontroll, inbrottsskydd och brandskydd i den omfattning som krävs.

5.1 Riktlinjer för skydd av utrustning och information

Nivån på det fysiska skyddet ska baseras på genomförda riskanalyser och stå i proportion till identifierade risker. Grundregeln är att information aldrig ska lämnas oskyddad. Utrustning som är

känslig i sig själv eller behandlar känslig information, ska placeras så att tillträde minimeras och utformningen av lämpliga skyddsåtgärder underlättas.
Emporis kritiska IT-infrastruktur, IT-system och informationstillgångar ska inrymmas i säkra utrymmen, omgärdade av skalskydd, med lämpliga tillträdesspärrar och kontroller.

5.2 Tillträdeskontroll till byggnader och lokaler

Vid behov ska tillträdeskontroll till viktiga byggnader och lokaler finnas, för att säkerställa att endast behörig personal ges tillträde.
För Empori ska det finnas rutiner så att det säkerställs att endast anställda och övriga behöriga personer vistas i lokalerna. Vilka som är behöriga att vistas i lokalerna avgörs av företagsledningen för Empori.

5.3 Säkerhet för utrustning utanför egna lokaler

Risker i samband med hantering av utrustning utanför de egna lokalerna ska beaktas. Detta gäller för informationsbärare i vid mening och omfattar bland annat servrar och annan hårdvara.
Rutiner/instruktioner skall fastställas för hur sådan utrustning skall hanteras. Viktigt är att även beakta riskerna då utrustning lämnas ut för extern service. Utförsel av utrustning och information ska vara godkänd av COO.

5.4 Avveckling av utrustning

Lagringsmedia, som innehåller känslig information eller licensierade program, ska förstöras, avmagnetiseras eller överskrivas på ett säkert sätt, i samband med avveckling eller återanvändning.

5.5 Skalskydd och tillträde

Skalskydd skall finnas för de lokaler där informationsbehandling sker med minst skyddsklass 2. Lokaler där centraliserade informationsbehandlingsresurser finns skall ha utökat skydd i form av begränsad åtkomst. Lokaler där informationsbehandlingsresurser finns skall vara anpassade för ändamålet och tillhandahålla adekvat skydd vad gäller den fysiska miljön. Skalskydd skall övervakas så att larmöverföring sker automatiskt och att fördefinierad åtgärdsplan finns fastställd.

5.6 Hantering av media

Det skall finnas tydliga rutiner för hantering av datamedia som säkerställer att media alltid befinner sig inom fördefinierade områden.
Empori skall uppfylla följande krav avseende lagring av datamedia:

- Utrymmet skall bestå av skalskydd med minst larmklass 2.
- Passage till som specifikt utvalda personer kan genomgå.
- Utrymmet skall videoövervakas med lagringstid på 90 dagar.
- Hanteras som egen brandcell.
- Använda kassaskåp med minst brandklass 120DIS.
- Destruering av media sker genom fördefinierad sluten process med spårbarhet tills dess att destruktionskvitto erhålles.

6 Kontinuitetshantering

Kontinuitetshantering syftar till att säkerställa rutiner för att minimera avbrott i Emporis verksamhet. Alla IT-system och organisationer har risker. En riskanalys ska identifiera tänkbara störningar, allvarliga händelser samt extraordinära händelser. Arbetet syftar till att skapa robusta IT-verktyg samt identifiera och analysera skyddsvärda system och kritiska områden inom företaget. Emporis företagsledning ska inventera, analysera, värdera, förebygga och åtgärda oönskade händelser inom sina ansvarsområden. (Se mer under avsnittet för riskanalys nedan.) Kontinuitetsarbetet skall baserat på riskanalysen fokusera på förebyggande insatser och konkreta skyddsåtgärder för människor, information och egendom/verksamhet.

Emporis kontinuitetshantering fokuserar på att:

- säkerställa att i första hand driftkritiska processer ska kunna fungera på en acceptabel nivå vid eventuella störningar
- avbrutna ordinarie processer ska kunna återupptas inom en acceptabel tidsrymd under vilken alternativa rutiner upprätthåller prioriterad, kritisk verksamhet
- säkra verksamheten vid olika typer av risker
- lägga ansvaret för åtgärder på ansvarig för den driftkritiska processen

6.1 Driftrutiner och ansvar

Målet är att säkerställa korrekt och säker drift av IT-miljön så att informationens sekretess, tillgänglighet, riktighet och spårbarhet bibehålls.
Ansvar och rutiner för incidenthantering skall vara etablerad. (Mer information om detta finns senare i dessa riktlinjer för informationssäkerhet.)
Driftansvar ska fördelas på olika personer för att minska risken för oavsiktligt eller avsiktligt missbruk.

6.2 Kontroll av utomstående tjänsteleverantör

Informationssäkerheten och utförandet av tjänster från extern leverantör ska ske i enligt avtal och med bibehållen nivå av informationssäkerhet.
Det ska finnas en rutin för hur uppföljning och granskning ska göras på externa leverantörers tjänster. I händelse av att rutinerna ändras eller att utförandet ändras på annat sätt ska en förnyad riskanalys göras.
Alla informationssystem ska godkännas av systemägaren innan produktionssättning och vid förändringar i systemet ska en bedömning göras ifall godkännandet ska förnyas. En viktig parameter i ett godkännande är systemets klassning och dess skydd av informationen avseende sekretess, tillgänglighet, riktighet och spårbarhet.

7 Riskanalys

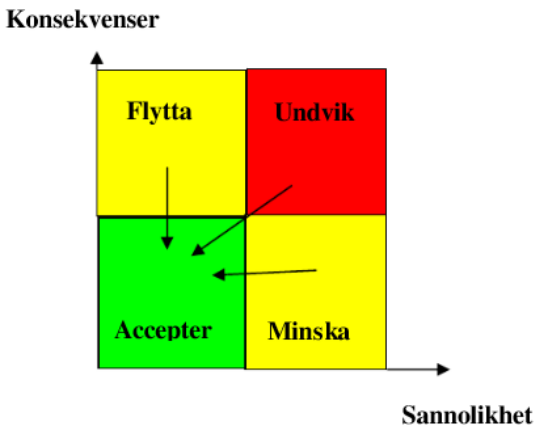
Riskanalysens syfte är att förenkla hantering av risker och därmed minimera frekvensen av möjliga oönskade händelser eller skador som Empori kan drabbas av. Riskhanteringen görs enligt nedan riskhanteringsprocess.

7.1 Emporis riskhanteringsprocess

1) Kommunikation med interna och externa intressenter
2) Grov listning av oklassificerade risker samt etablering av miljö; intern eller extern
3) Individuell riskbedömning som består av
   a) Riskanalys (se nedan)
   b) Riskutvärdering (se nedan)
   c) Riskbearbetning (se nedan)
4) Löpande utvärdering och koppling till incidentrapportering
5) Årlig iteration av steg 1-4

7.1.1 Riskanalys – analysering av risker

Vid analysering av risker definieras risknivå och nivå av konsekvens. Det ger input till ett senare beslut om hur risken skall hanteras. Riskanalysen skall innehålla alla riskkällor samt negativa och positiva konsekvenser med hänsyn till intressenterna. Analysering av risken skall ske genom att kombinera konsekvenser och intressenter.



För Empori skall en riskanalys omfatta:

- Vilken applikation som måste fungera oavsett påfrestningar och vilka system som stöder denna funktion.
- Vilka system som säkerställer att kärnvärdena uppfylls - både organisatoriska och tekniska system samt sårbarheten i dessa system.
- Tänkbara risker och hot som på ett avgörande sätt kan utmana förmågan att upprätthålla Empori grundtjänster samt sannolikheten för att de inträffar.

7.1.2 Riskanalys – Klassificering

Klassificering av risk

	Intern			Extern			Frekvens		
	Låg	Mellan	Hög	Låg	Mellan	Hög	Låg	Mellan	Hög
Risk 1									
Risk 2									
Risk 3									
Risk 4									

Varje enskild risk skall ges en klassificering där dimensionen intern/extern samt riskens förväntade frekvens sammanvägs med resultatet från riskanalysen. Klassificeringen ger input till hur risken skall bearbetas.

7.1.3 Riskanalys – bearbetning av risker

De risker som identifieras skall bearbetas för underlätta hantering om risken skulle realiseras. Detta görs genom att bearbeta risken utifrån dess klassificering:

- Genomföra förberedande åtgärder som minskar riskerna till en acceptabel nivå.
- Acceptera riskerna om de inte strider mot lagstiftning eller informationsleverantörers regler.
- Undvika den aktivitet som orsakar att den identifierade risken blir verklighet.

8 Hantering av incidenter

En utvecklad Incidenthantering skall finnas avseende informationssäkerhet.

8.1 Rapportering av säkerhetshändelser och svagheter

Incidenter och säkerhetsmässiga svagheter ska snarast rapporteras så att åtgärder kan påbörjas för att minimera skada och åtgärda brister. En effektiv och genomarbetad process är en nödvändighet för att:

- öka möjligheten att identifiera Incidenter innan de inträffar
- öka möjligheten att avhjälpa framtida Incidenter.
- leverera en förbättrad tjänstekvalitet
- informera intressenter som privatpersoner, kunder och informationsleverantörer på ett korrekt och tydligt sätt

8.2 Roller vid incidenthantering

Roll	Beskrivning
Incidentansvarig	Incidentansvarig är teknisk kompetent anställd utsedd av COO att kommunicera och dokumentera omfattning och bakgrund till incident.

Systemutvecklare	Har hög teknisk kompetens som dagligen arbetar med att underhålla, förvalta och utveckla Emporis tjänster mot kund. Innehar förmågan att driva och ta fram förslag om åtgärder vid Incidenter.
COO	Innehar rollen att vara ytterst ansvarig för att incident kommuniceras, hanteras, åtgärdas, återkopplas externt mot kund och vid personuppgiftsincident privatperson. Även att intern uppföljning och incidentrapportering genomförs, dokumenteras och att åtgärdsplan implementeras.

8.3 Incidentrapport

Incidentrapporter skapas för varje Incident där klassificering av risk är nivå hög samt vid andra relevanta fall. Incidentrapporten skall innehålla:

- Beskrivning av incidenten
- Påverkade system
- Påverkan för organisationen
- Ungefärlig Start och stopptid
- Nuvarande status med eventuell hänvisning till ärende för problemhantering
- Kortsiktiga åtgärder
- Långsiktiga åtgärder

Sida 1 av 1

EMPORI Web application- & solutions

Incidentrapport

Kund:

Tjänsteområde:

Utfärdat av:

Område	Nivå
Incident	
Tjänst	
Prioritet	
Start	
Slut	
Status	

Incidentsbeskrivning

Text.

Akut åtgärdsbeskrivning

Text.

Långsiktig åtgärdsbeskrivning

Text.