Anvisning för Säkerhet i Drift

Anvisning för säker drift till tjänster som Inera tillhandahåller

Version 1.0

Reviderat och godkänt av Petter Könberg

Datum
2017-11-01

Revisionshistorik

Version	Revision Datum	Komplett beskrivning av ändringar	Ändringarna gjorda av	Definitiv revision fastställd av
1.0	2017-11-01	Beslut att sätta anvisningen till v1.0	Bengt-Göran Andersson, Fredrik Rosenberg, Inera	PK

inera

Innehåll

1. Bakgrund

Anvisning för säkerhet i driftsmiljön anger hur säkerhetsaspekter ska hanteras gällande Inera AB:s IT-drift. Anvisningen gäller hela Inera oavsett om drift sker i egen regi eller om drift lagts ut hos en driftsleverantör. Kraven i denna anvisning ska också finnas med vid upphandlingar av IT-drift. Anvisningens krav ska kompletteras baserat på genomförd riskanalys för att erhålla ett anpassat och effektivt skydd av driftsmiljön.

2. Allmänna krav

En driftsmiljö ska vara utformad så att överenskomna funktions- och prestandakrav uppfylls samt, beroende på tjänstens nivå och krav på tillgänglighet, att Single Point of Failure (SPOF) undviks, se kapitel 8 Tillgänglighet och kapitel 9 Kontinuitet.

2.1 Revidering

Anvisning för Säkerhet i Drift ska revideras årligen eller när skäl finns att uppdatera hela eller delar av dokumentet. Revisionsinformation dvs. nuvarande status på anvisningen finns på första sidan.

Ineras Informations- och IT-säkerhetsfunktion är ägare av denna Anvisning.

2.2 Test

Hänvisning till de specifika dokument (Anvisningar och Instruktioner) som berör Test.

2.3 Dokumentation

Det ska finnas fullständig och aktuell dokumentation omfattande de verktyg, processer och produkter som används i driftsmiljön,

Dokumentationen ska minst omfatta:

- Teknisk IT-driftsrelaterad dokumentation (arkitektur-, konfiguration-, driftsanvisningar och installationsdokumentation).
- Manualer, arbetsbeskrivningar/rutiner och planer för den personal som utför uppgifter som berör utförandet av driften.
- Säkerhetsdokumentation (fysisk säkerhet, teknisk säkerhet, informationssäkerhet).
- Dokumentation om planerade och utförda aktiviteter och åtgärder som påverkar driften eller som utgör en del av driften (förvaltning, support, rättelser, implementering av ny funktionalitet).
- Kontinuitetsplan.

Dokumentation över konfiguration för driftsmiljön ska hållas uppdaterad (tex i CMDB). Konfigurationsinformation ska vara uppdaterad innan förändringar i konfiguration tas i drift.

Dokumentation ska finnas elektronisk och spårbarhet ska finnas från krav/problem till utförd åtgärd.

Dokumentation ska korrekt återge faktiska förhållanden, dvs vara uppdaterad och aktuell vid varje given tidpunkt.

Dokumentation ska vara versionshanterad så att det är möjlig att ta del av tidigare versioner

Dokumentation ska primärt vara författad på svenska.

2.4 Uppföljning

Nyttjandegrad av driftkapacitet ska följas upp. Tillgänglighet ska mätas kontinuerligt.

2.5 Uppdateringar

Uppdateringar avseende komponenter i driftsplattformen ska installeras löpande för att erhålla en nivå som säkerhetsställer stabilitet och säkerhet över tid.

Det ska finnas dokumenterade rutiner för uppdatering med beskrivning av i vilken ordning förekommande typer av uppdatering ska införas i driftsmiljön.

Dokumentation ska utformas i enlighet med Ineras dokumentationsprocess.

Uppdateringar av operativsystem och tredjepartsapplikationer ska omfatta:

- Test i testmiljö innan installation i driftsmiljö.
- Installation i överenskomna servicefönster, utan driftsavbrott.
- Plan för återgång till tidigare konfiguration och version.
- Information om uppdatering ska ske i enlighet med rutinerna för Ändrings- och releasehantering, innan uppdatering genomförs.

Uppdatering där omständigheterna medför behov av omgående åtgärd (tex akuta säkerhetsuppdateringar), ska införas omgående dock senast inom åtta timmar om inte annat beslutas.

Programfixar av samtliga i driftsmiljön ingående applicerbara delar, exempelvis operativsystem och program inklusive Sabotageprogram, ska installeras omgående dock senast inom åtta timmar efter det att programfixen finns tillgänglig. Normal ändringshantering ska tillämpas.

Uppdateringar ska primärt baseras på automatiserade rutiner.

2.6 Tillgänglighet och prestanda

Det ska finnas dokumenterade överenskomna Tillgänglighetsklasser, se rubriken 8 Tillgänglighetskrav. Nödvändiga åtgärder ska vidtas för att säkerställa att störningar minimeras och att överenskomna servicenivåer upprätthålls. Mätning av tillgängligheten ska göras kontinuerligt under servicetid genom automatisk mätning och övervakning.

2.7 Anslutningar

2.7.1 Fjärranslutning

All fjärranslutning till samtliga driftsmiljöer för administration av servrar och applikationer ska ske via VPN eller motsvarande säker anslutning. Se punkten 3.2 Nätsegmentering.

För Autentisering av fjärranvändare se punkten 3.3.3 Autentisering och Tillitsnivåer.

2.7.2 Internet-anslutning

Anslutning av driftsmiljön till internet ska inkludera internet-access över DMZ med full redundans och bibehållen funktionalitet vid automatisk överlämning av arbetet (failover).

Kapacitet ska inom 45 dagar kunna utökas med 10Gbit/s. Utökning understigande 10 Gbit/s ska kunna genomförs inom 14 dagar. Utökning av internetkapacitet ska inte påverka driftade tjänster, dvs uppgradering ska vara avbrottsfri. Internetförbindelsen ska vara logiskt och fysiskt separerad från en extern leverantörs övriga kunder.

2.7.3 Sjunet-anslutning

Anslutning av driftsmiljön till Sjunet ska inkludera Sjunet-access över DMZ med full redundans och bibehållen funktionalitet vid automatisk överlämning av arbetet (failover). Utökning av Sjunetkapacitet ska inte påverka driftade tjänster, dvs uppgradering ska vara avbrottsfri. Anslutning till Sjunet ska uppfylla de krav som ställs av Sjunets förvaltning.

2.8 Internetprotokoll

Internetprotokollet ska vara version 4 (IPv4) och version 6 (IPv6).
Inera äger och Driver ett eget Local Internet registry, LIR som i dag används på Sjunet men planen är att öppna vissa delar för Internet. Leverantören ska ha stöd för att använda Ineras LIR.
Leverantörens Adresser ska vara ”multihomade” dvs routebara via flera leverantörer.
För att skydda emot svartlistningar (Dåligt tyckte) för IP adresser som användas i leverans skall adresser eller subnät som används till Inera vara segmenterat bort från andra kunder som leverantören har.

2.9 Klocksynkronisering

Samtliga i systemet ingående servrar ska vara klocksynkroniserade med en av Inera Drift och CAB godkänd referenskälla.

2.10 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.

Inera ska ha tillgång, och ha möjlighet att integrera till egen övervakning, till de system som används för övervakning oavsett om drift sker hos extern part. Uppgifterna ska presenteras i realtid. Minimum information från varje system är uptime, CPU load, RAM consumption, web transaction time och database transaction time.

Övervakning och övervakningssystem ska

- Bygga på standardiserade protokoll.
- Innefatta användning av agenter, nätverkstappar och prober.
- Innefatta standardiserat gränssnitt för rollbaserad åtkomst beroende på tjänst/tjänsteobjekt i olika vyer samt en specifik vy för Ineras Kundservice.
- Innefatta standardiserat gränssnitt för extern webbpresentation, tänkt för publik statuspresentation av Ineras tjänster.
- Innefatta meddelandehantering utifrån larm/händelse, sms, mail, webbservice.
- Innefatta schemalagt dämpning/avslagning av larm.
- Innefatta loggning av larm/händelser direkt från själva applikationen eller från övervakningen.
- Innefatta prestandaövervakning av Applikationer (APM.)

2.11 Av Inera godkända server OS och Hypervisors

2.11.1 Godkända OS för servrar

Applikationsservrar för Ineras tjänster, med driftansvar genom Inera Drift, ska drifthållas och Life cycle hanteras på supporterade versioner av Windows Server eller Redhat Linux.

2.11.2 Supporterade Hypervisors

Hypervisors (virtualiseringsplattformar) till Applikationsservrar för Ineras tjänster, med driftansvar genom Inera Drift, ska drifthållas och Life cycle hanteras på supporterade versioner av i första hand VMware ESX/ESXi eller Windows Hyper V eller likvärdiga versioner.

3. Säkerhetskrav och Tekniska skydd

Alla tjänster som tillhandahålls av Inera ska alltid, i sin driftmiljö, ha en lägsta nivå av skydd som beskrivs i detta kapitel.

3.1 Följsamhet till Open Web Application Security Project, OWASP

3.1.1 OWASP Developer Guide

Tjänster, som utvecklas och tillhandahålls genom Inera, med webbgränssnitt, ska i möjligaste mån följa OWASP Developer Guide. OWASP Developer Guide fokuserar på hur man säkert

utvecklar webbapplikationer. OWASP Developer Guide finns att läsa och ladda ner från länkarna nedan:

https://github.com/OWASP/DevGuide och länken ”Current stable is version 2.0.1”

3.1.2 OWASP Testing Guide 4.0 och OWASP Top 10

Tjänster som publiceras med ett webbgränssnitt och som tillhandahålls genom Inera ska minimum säkerhetsgranskas och säkerhetstestas utgående från OWASP Testing Guide 4.0 och OWASP Top 10 – 2013/2017.

OWASP Testing Guide v4 finns att läsa och att ladda hem på länken nedan:

https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

OWASP Top 10 -2013 finns att läsa på länken nedan:

https://www.owasp.org/index.php/Top_10_2013-Introduction

OWASP Top 10 -2017 (OBS 2017 är ej fastlagd än):

https://www.owasp.org/index.php/Top_10_2017-Top_10

3.2 Nätsegmentering

Alla användarnät, tjänster, servar och nät för utvecklare skall, i möjligaste mån, alltid brandväggsepareras i olika nätsegment med explicita åtkomstregler, dvs. endast den access som explicit och uttryckligen har godkänts får trafikera från ett nätsegment till ett annat. Ett rätt segmenterat nät gör det möjligt att begränsa åtkomst baserat på regeln att en användare eller tjänst endast skall ha tillgång till de resurser som den är behörig till.

3.2.1 Frontend miljö

En för användare accessbar tjänst ska alltid ha en tydlig s.k. Frontend miljö som t.ex. kan bestå av en reverse proxy servrar placerad på ett segmenterat och accesskontrollerad DMZ zon. Access från DMZ zon till Backend miljön skall strikt accesskontrolleras och skannas för att förhindra intrång. Endast absolut nödvändiga portar får öppnas mellan DMZ zon och Backend miljö.

3.2.2 Backend miljön

Applikationsserver och lagring skall skyddas av ett Accesslager som hanterar autentisering och accesskontroll på applikationsnivå. Accesslager skall vara separata för varje tjänst.

3.2.3 Management nät

All access för administration och för övervakning av servrar och komponenter i Ineras driftmiljö skall ske från ett eget nätsegment, ett s.k. Managementnät, helt skilt från produktionstrafik. Terminaler/PC som har en direktaccess till Managementnätet ska vara helt skilda från andra nät dvs. det ska vara dedikerad utrustning för administration.
Annan access från icke dedikerad utrustning, till Management nätet, skall alltid följa krav specificerad under rubriken 3.7 Lösenordskrav och lagring av lösenord

3.2.4 VPN nät
Ett specifikt nätsegment skall finnas där all VPN access termineras för användare som behöver access till Ineras driftmiljö.

3.2.5 None Route nät
Ett icke routebart nätsegment skall finnas för att, från Backend miljön, kunna nå t.ex. lagrings- och arkivmiljöer.

3.2.6 Console access
Ev. nätverk för Console terminaler eller för access till s.k. Out-of-band Management t.ex. HP:s Integrated Lights-Out, iLO får endast vara åtkomligt från behörig driftpersonal hos Ineras driftleverantör,

3.3 Säkerhetskrav på Hypervisors

3.3.1 Härdat grundsystem
Hypervisorns grundsystem ska vara härdat, med referens till punkten 3.8 nedan, Härdning av server i driftmiljö. Driftleverantör ska redogöra för hur Hypervisorns grundsystem är härdat och säkerhetsapassat samt hur grundsystemet underhålls.

3.3.2 Administrationsaccess
Administrationsaccess ska följa punkt 3.2.3 Management nät. SSH access direkt mot Hypervisor host bör vara inaktiverat och endast aktiveras tillfälligt, dvs. vid behov.

3.3.3 Lockdown Mode
För att begränsa direktaccessen till Virtual Machine, VM från Hypervisorns administrationsklienter ska en ”Lockdown mode” teknik appliceras som ska förhindra att en icke ”root” administratör, via CLI eller script, kan få direktaccess en VM. Normal administration av en virtuell miljö ska alltid ske med administrationskonton som har en lägre behörighet än Hypervisorns ”root” administratör.

3.3.4 Virusskydd på instansernas OS
Vid användning av virusskydd på instansernas OS så skall dessa vara anpassade till att köras på virtuella servrar, exempelvis ska inte alla scanningar köra samtidigt på alla virtuella maskiner.

3.3.5 Nätverkskort

Det virtuella nätverkskortet i en virtuell värd skall hindras från att lyssna på all nätverkstrafik (Promiscous mode). Det inte vara tillåtet att skicka datapaket med annan Länkadress (MAC adressen) än den tilldelade avsändaradressen, dvs en virtull maskinen får inte modifiera sitt tilldelade MAC-nr (MAC Change) och inte skicka paket med MAC adressen ändrad i IP-headern (Forged transmit). Detta skydd kan uppnås med Hypervisorns virtuella switchar.

3.4 Access inom och mellan tjänster

- Informationsklassificeringen avgör om kryptering krävs inom eller mellan tjänster, applicering av kryptering bör ske Applikationsspecifikt.
- Inom en för Inera isolerad serverhall eller låst serverutrymme där ingen server eller nätverkskomponent delas med någon annan kund, kan information inom en tjänst hanteras och transporteras okrypterad.
- Inom dedikerade switchar i en väl skyddad Backend miljö kan trafik transporteras okrypterad.
- Shared infrastruktur kräver transportkryptering beroende på innehållets informationsklassificering och skyddsvärde.

3.4.1 Transportskydd

För kraven på Transportskydd hänvisas till dokumentet senaste och nu gällande **Anvisning för Transportkryptering**.

3.4.2 Kryptografiska moduler

När höga krav på säkerhet erfordras, med tillitsnivå Väsentlig enligt eIDAS, ska kryptografiska moduler följa lägst FIPS 140–2 Level 2. När krav på följsamhet till tillitsnivå Hög, enligt eIDAS, ska kryptografisks moduler följa lägst FIPS 140–2 Level 3

3.4.3 Autentisering och Tillitsnivåer

För krav på autentisering, identifiering och tillitsnivåer hänvisas till dokumentet **Anvisning Autentisering.**

3.5 Komponentskiktning

Krypterad klientaccess bör termineras i Accesslagret. Om ovanstående isolationsvillkor gäller finns även möjlighet att analysera trafik mellan Access och Applikationslager mha. Web Application Firewall, WAF. Tjänst i Applikationslagret ska utvecklas för att fungera i en klustrad HA miljö. Komponenter i tjänsten ska vara skiktade.
Alla lager frontas med lastdelare.

3.6 Säkerhetstester

I begreppet Säkerhetstester innefattar Inera Sårbarhetsskanningar och Penetrationstester.

Sårbarhetsskanningar utförs normalt sett som automatiserade skanningar, antingen att Inera utför dessa i egen regi eller genom driftleverantörens avtal. Sårbarhetsskanningar ske genomföras med hjälp av erkända skannerprodukter som marknaden erbjuder.

För Penetrationstester anlitas väl kvalificerade och renommerade säkerhetskonsulter som aktivt, och samverkan med Inera, genomför tester och försök till att hitta svagheter i kritiska tjänster.

3.6.1 Sårbarhetsskanningar

Automatiserade Sårbarhetsskanningar av Ineras driftmiljö ska ske, på alla tjänster, minst 2 ggr/år, gärna 4 ggr/år i regi av Ineras driftleverantör. Sårbarhetsskanningar kommer även att genomföras av Ineras IT-säkerhetsfunktion i samverkan med Inera Drift.

Resultat och åtgärder hanteras, revideras och följs upp av Ineras IT-säkerhetsfunktion.

3.6.2 Penetrationstester

Fullödiga Penetrationstester ska, på alla nivåer och i utvalda tjänster baserat på informationsklassningsnivå och bedömd risk, genomföras i Ineras driftmiljön, minst en gång per år. Resultat och åtgärder hanteras, revideras och följs upp av Ineras Informationssäkerhetschef.

Vilka tjänster som ska penetrationstestas avgörs i Ineras Informations- och IT Säkerhetsråd där Ineras Informationssäkerhetschef har det övergripande ansvaret.

3.7 Informationsskydd

3.7.1 Skydd mot dataintrång

Det ska finnas ett implementerat och kontinuerligt aktiverat skydd för att upptäcka dataintrång, Intrusion Detection (IDS) samt för att förhindra dataintrång, Intrusion Prevention (IPS). IDS och IPS ska även klara av att upptäcka och förhindra s.k. Zero Days attacker mha. Advanced Threat Protection (ATP) teknik.

Det ska vara möjligt att göra uppföljningar av loggar från dessa system.

Det ska finnas ett implementerat och aktiverat brandväggsskydd för att motverka dataintrång. Skyddet ska minst omfatta en brandväggslösning

- med full redundans
- för Sjunet-anslutning
- för Internet-anslutning

3.7.2 Skydd mot överbelastningsattack

Det ska finnas ett kontinuerligt uppdaterat skydd för att upptäcka och förhindra överbelastningsattacker, DDOS/DOS-skydd (mitigera).

Temporär nedstängning av Driftstjänsten vid överbelastningsattacker ska inte leda till att data eller information förvanskas eller försvinner.

3.7.3 Skydd mot skadlig kod

Det ska för samtliga delar i Driftstjänsten ingående applicerbara delar, exempelvis program och operativsystem, finnas installerat skydd mot Sabotageprogram.

Uppgraderingen av skydd mot Sabotageprogram ska installeras inom åtta (8) timmar från det att ny uppdaterad version finns tillgänglig.

3.7.4 Skydd av lagringslagret

För att säkerställa att endast godkända anrop från applikationer (SQL statement) sker mot databaser ska en applikations brandvägg anpassad för SQL el. IDP kunna lyssna, analysera och godkänna SQL anrop,
Exempel på Databas Brandväggar/Filter
http://www.greensql.net/gioi-thieu/
https://www.mysql.com/products/enterprise/firewall.html

http://www.oracle.com/technetwork/database/database-technologies/audit-vault-and-database-firewall/overview/overview-1877404.html

https://www.imperva.com/Products/SecureSphereforData

Målsättning är att Applikationsförvaltningen ska redogöra för driften om vilka SQL-frågor som applikationen behöver kunna göra emot databasen. Till exempel bör SQL-frågan ”**dump * from users**;” betraktas som ett ogiltigt anrop från en applikation och ska inte gå att genomföra. En SQL Brandvägg kan förhindra ett intrång om någon skulle lyckas med en SQL-injection eller liknande.

3.8 Lösenordskrav och lagring av lösenord

En administratorsaccess till Ineras driftmiljö ska i möjligaste mån passera ett Privileged Account Security Solutions, PAS typ CyberArk med personliga lösenord för att erhålla full spårbarhet i aktiviteter i driftmiljön. RDP klienter och SSH proxy som ska Alltid användas. Grupp eller gemensamma lösenord får Ej förkomma.
För kontohantering, se rubrik 4 Behörighet.

3.9 Härdning av server i driftmiljö

En server, för tjänst som Inera tillhandahåller, ska alltid genomgå en härdningsprocess som innefattar t.ex. att installera senaste OS uppdateringar, avinstallera eller inaktivera icke önskade tjänster, inaktivera eller ta bort onödiga konton, sätta lösenordspolicy, konfigurera brandvägg, aktivera diskkryptering, installera övervakningskomponenter etc.

I dokumentet **Instruktion härdning av server i driftsmiljön** beskrivs hur en Windows Server eller Linux Server i Ineras driftmiljö ska härdas innan den tas i drift.

4. Behörighet

4.1 Behörighetssystem

Det ska finnas behörighetssystem för att styra och kontrollera att användare har behörighet för åtkomst och ändring i driftsmiljö och där ingående data.

Hantering av användarkonton för Ineras användare i driftsmiljön ska uppfylla följande krav:

- Beställning av konto/behörighet ska attesteras av Behörig beställare.

- Extern åtkomst till specifika servrar ska separeras från åtkomst till beställningsfunktion.
- Behörighet ska kunna begränsas till ett eller flera Tjänsteobjekt.
- Behörighet ska kunna anpassas till Tjänsteobjektets driftsmiljöer.
- Konto/Behörighet ska ha tidsbegränsad giltighetstid.
- Det ska vara möjligt att välja en valfri giltighetstid för ett visst konto/behörighet.
- Det ska finnas minst tre behörighetsnivåer för konto.
- Byte av lösenord ska kunna initieras baserat på en förutbestämd valfri periodicitet, exempelvis var tredje månad.
- Det ska vara möjligt att ställa krav på hög lösenordsstyrka, dvs lösenord med minst tolv tecken och krav på specialtecken.
- Det ska vara möjligt att ge information om användarkonton i driftsmiljön, och därtill knutna behörighetsnivåer och roller. Informationen ska innehålla Roll, Tjänsteobjekt, Ansvarig TA, namn, e-postadress, telefonnummer, aktuell tjänst och behörig på Inera.
- Förändringar av behörighet ska löpande kunna anpassas till faktiska förhållanden, exempelvis ska behörighet för en viss person som vars behörighet upphör, upphöra vid den tidpunkt som meddelats.
- Inloggning med tvåfaktorsautentisering ska vara möjlig att införa där den inte redan är införd.
- Det ska finnas rutiner för hantering av behörigheter i driftsmiljön.
- Behörighet för användaren till ett visst system ska kunna styras beroende på roll och autentiseringsprincip.
- Ett låst användarkonto till Ineras driftmiljö ska alltid generera ett larm både internt till driftleverantörens övervakning och till Ineras egen övervakning.
- Alla användarkonton är personliga. Inera tillåter inte grupp- eller gemensamma konton.

Användare av VPN eller motsvarande säker anslutning ska inte få ”nät till nät”-kommunikation med någon server.

4.2 Skydd mot obehörig åtkomst

Skydd ska finnas mot att person obehörig att ta del av Driftsmiljön får åtkomst till personuppgifter och annan känslig data.

All access till, från och mellan servrar och servermiljöer, mellan olika tjänster eller delar av tjänster ska vara segmenterade, redundanta och kunna klassificeras och accessstyras med explicita brandväggsregler.

4.2.1 Behörighet för administration av Ineras driftmiljö

Administration av Ineras driftmiljö ska ske från Sverige. Undantag får endast ske efter skriftligt medgivande från Tjänsteansvarig i samverkan med Inera drift.

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

4.3 Beställningsfunktionalitet

Delegering av rätten att agera Behörig beställare och Behörighet att godkänna en beställning av en förändring i Ineras driftmiljö hos en av Ineras driftleverantörer avgörs alltid av Inera Drift.

5. Loggning

Två övergripande typer av loggar ska kunna hanteras

1. Transaktionsloggar. Baseras på loggning av applikationsorienterade förändringar av innehållet i en tjänst, t.ex. loggar för uppföljning enligt Patientdatalagen, PDL.
2. Administrations- och systemloggar. Visar status på operativsystem och applikationer samt ev. förändringar som utförts i systemet av administratörer.

Samtliga uppgifter om vem som läser, registrerar, ändrar samt tar bort data ska loggas. Kravet omfattar samtliga informationskällor och samtliga personer som använt berörda miljöer och tjänster.

Alla incidenter och övervakningslarm ska loggas. Det ska vara möjligt att spåra bakåt i tiden vilka incidenter som inträffat och vilka åtgärder som vidtagits i förhållande till berörd incident.

Logginformation ska skyddas mot förvanskning samt obehörig åtkomst. Logginformation ska sparas och vara tillgänglig under 18 månader. Administration via konsol och fjärrstyrning ska spelas in och vara tillgänglig under 18 månader.

5.1 Loggintegration

Loggsystem ska kunna integreras med Ineras eget Security Information and Event Management (SIEM) system, minimum på syslog nivå.

6. Lagring

6.1 Lagringsformat

Data ska lagras i SAN-form, antingen som utrymme på filsystem eller utrymme i databas.

Lagringsutrymme ska kunna skalas upp, efter ökande behov utifrån lagringsbehov, svarstider och redundans. Kapacitetsökning när det gäller lagringsutrymme ska kunna ske utan påverkan på tillgängligheten.

Lagringsutrymme ska kunna skalas ner, efter minskande behov utifrån lagringsbehov, svarstider och redundans. Kapacitetsminskning när det gäller lagringsutrymme ska kunna ske utan påverkan på tillgängligheten.

6.2 Säkerhetskopiering

Det ska vara möjligt att säkerhetskopiera all lagrad data såsom systemkonfiguration, databaser, servrar, filer och filsystem oavsett format. Det ska finnas rutiner för Säkerhetskopiering.

Säkerhetskopiering ska använda ett format som möjliggör återställning av all lagrad data utan att förlora data.

Säkerhetskopiering ska kunna utföras utan att tillgänglighet och prestanda påverkas.

6.3 Lagring av säkerhetskopior

Säkerhetskopior ska lagras i separat datahall avskild från datahallarna som svarar för driften.

Lagringstiden för säkerhetskopior ska vara beslutad och dokumenterad med utgångspunkt från Ineras och kunders krav. Om det är reglerat i lagar och förordningar ska lagringstiden följa detta.

6.3.1 Kryptering av säkerhetskopior

Säkerhetskopior ska vid behov kunna krypteras.

Godkända kryptoalgoritmer står i paritet med vad som är godkänt dvs. grönmarkerade i Anvisning Trafikkryptering. Nyckellängd ska vara minst 128 bitar. Nyckellagret, där krypteringsnycklar lagras, ska i första hand krypteras med ett RSA nyckelpar med minst 2048 bitars nyckel och i andra hand med en symmetrisk krypteringsalgoritm med ett lösenord av minst 16 tecken och med en vedertagen lösenordskomplexitet.

Kryptering ska ske med en för Inera unik krypteringsnyckel, dvs för inte vara delad med andra kunder i de fall driften är utlagd hos en leverantör. Nycklar ska försvaras skyddade mot obehörig åtkomst och på ett sätt som säkerställer att nycklar inte går förlorade.

6.4 Arkivering

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

Arkiverad data och information ska förvaras i arkivbeständigt format som säkerställer tillgång över tid enligt gällande bestämmelser (minst 10 år i vissa fall).

Tillgängligheten till arkiverad data och information ska anpassas till behovet av åtkomst.

6.5 Återställande av data

Ett Tjänsteobjekt ska kunna återställas med stöd av säkerhetskopia.

Återställning av säkerhetskopia från det tre senaste veckorna ska kunna genomföras inom 24 timmar. Återställning av säkerhetskopia som är äldre än tre veckor ska kunna genomföras inom 48 timmar. Test av återställande utifrån säkerhetskopior ska ske kontinuerligt minst 2 ggr per år.

7. Datahallar

7.1 Flerhallslösning

Driftsmiljön ska vara fullständigt redundant och speglad i två separata datahallar till både funktionalitet, konfiguration och data. Båda datahallarna ska uppfylla samtliga krav i denna anvisning. Kapacitet och prestanda ska inte påverkas i det fall bara en av datahallarna är tillgänglig. Datahallarna ska vara fysiskt åtskilda och placerade med ett avstånd om minst 15 kilometer mätt fågelvägen.

I de fall Driftsmiljön blir utslagen ska en alternativ Driftsmiljö för produktionsmiljö vara tillgänglig inom 48 timmar.

7.2 Placering av datahallar

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

Som huvudregel ska all utlagd drift vara lokaliserad inom Sveriges gränser. Avsteg från denna huvudregel ska endast ske efter att risker analyserats och ett beslut fattats av Ineras ledning.

Data och information som innehåller personuppgifter får oaktat ovan 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.

7.3 Utformning av datahall

- Datahall ska bevakas manuellt och/eller genom kameraövervakning och inbrottslarm.
- Datahall ska vara försedd med brandskydd.
- Brandskyddsöversyn av datahall ska årligen genomföras tillsammans med specialistföretag/räddningstjänst.
- Datahall ska ha redundant strömförsörjning till. UPS, reservkraft. Tester som visar att utrustningen bibehåller för uppgiften erforderlig prestanda och funktion ska genomföras kvartalsvis.
- Datahall ska ha kylanläggning och övervakning av temperatur.
- Datahall ska vara så placerad att risken för påverkan av extern händelse minimeras. Riskanalys avseende placering av datahall ska vara genomförd.
- Datahall ska ha separerade vägar in för exempelvis fiber och el.

- Den fysiska utrustning som är placerad i datahall ska inte vara åtkomlig för obehöriga personer. Inera godkänner inlåsning i egen säkerhetsklassad bur.

7.3.1 Behörighet till datahallar

Det ska finnas behörighetskontroll till datahallar (kontroll och loggning av in- och utpassering).

Det ska vara möjligt att följa upp vilka som har behörighet att ha tillträde till de utrymme o datahall där Ineras Tjänster utförs och hanteras.

8. Tillgänglighetskrav

Tjänster har olika krav på tillgänglighet som då kravställer driftmiljöns klassning och uppbyggnad. Finns krav på hög tillgänglig uppkommer krav på klustrade och redundanta driftmiljöer, se rubriken 9 Tillkommande krav för hög tillgänglighet.

8.1 Tillgänglighetsklasser av tjänst

Verksamhetens krav på tillgänglighet till tjänsten:

A: Tjänsten är Verksamhetskritiskt, ska vara tillgänglig 7/24 med högsta tillgänglighetskrav dvs. incidentåtgärd krävs dygnet runt med minsta fördröjning.

B: Tjänsten är Verksamhetskritiskt, ska vara tillgänglig 7/24 men har endast krav på incidentåtgärd mellan 06–22 alla dagar i veckan alt vardagar mellan 06–22 med åtgärdsstart inom 4 timmar.

C: Tjänsten ska vara tillgänglig 7/24 men har endast krav på incidentåtgärd under kontorstid dvs. mellan 8–17, åtgärdsstart inom 4 timmar.

D: Tjänsten har endast krav på tillgänglighet under kontorstid, krav på incidentåtgärd under kontorstid dvs. mellan 8–17, åtgärdsstart inom 8 timmar.

9. Tillkommande krav för hög tillgänglighet

I detta kapitlet, i den här första utgåvan av **Anvisning för säkerhet i Drift,** är inte alla krav fullständigt genomarbetade. Innehållet t.ex. gällande krav för att bygga klustrade miljöer ska ses som av informativ karaktär. Utförligare krav kommer att införas i kommande utgåva.

9.1 Hög tillgänglighet

Inera har målsättningen att, för vissa kritiska tjänster som Inera tillhandahåller, erbjuda en tillgänglighet som är i det närmaste 100%.

- Tjänster ska, helt eller delar av miljön, vara möjlig att uppgradera eller patcha utan påverkan på tillgänglighet.

- Applikationer ska alltid vara minst n-1 kompatibla på minor nivå dvs. en version 1.2 av en tjänst ska alltid vara minst bakåtkompatibel med den tidigare versionen 1.1
- Det är eftersträvansvärt att även ha n-1 kompatibilitet på major nivå dvs. en version 3.0 bör vara bakåtkompatibel med den tidigare versionen 2.8.

9.1.1 Microservices

Komponenter i en tjänst ska vara baserad på **Microservice**. I Microservices bryts en applikation upp i mindre, oberoende och utbytbara moduler som var för sig utför en specifik del av en önskad funktionalitet**.** Microservices kan jämföras med t.ex. Service Oriented Architecture, SOA som strukturerar en tjänst i löst kopplade deltjänster.

Microservices baserad arkitektur är möjliggörare för driftsättning med en s.k. “Continuous Delivery” process.

9.2 Arkitektur för hög tillgänglighet (High Availability, HA)

För att Inera ska kunna erbjuda en hög tillgänglighet för vissa kritiska tjänster på i det närmaste 100% behöver en tjänst och dess tillhörande komponenter kunna byggas med hög tillgänglighet, antingen med extern lastbalansering eller i en egen klustrad miljö.

I en HA miljö strävar vi efter att skapa redundans mellan ingående komponenter som kan ta över vid ett driftavbrott i en utrustning och att eliminera Single Point of Failure. För vissa kritiska tjänster med krav på hög tillgänglighet ska förlust av sessionsinformation minimeras.

En HA miljö kan, beroende på tillgänglighetskrav, byggas som:

- Aktiv – Aktiv, alla ingående noder bidrar till att automatiskt lastdela aktiviteter i en tjänst. Alla ingående noder bör också ha sessionssynkronisering aktiverat mellan varandra så att kvarvarande nod/noder kan ta över en icke fullgjord uppgift från ett driftavbrott i en nod. Utan sessionssynkronisering kommer en icke fullgjord uppgift att förloras om en nod fallerar under pågående arbete.
- Aktiv – Passiv, hot standby. Endast en nod är aktiv men en eller flera noder kan automatiskt ta över om den aktiva noden fallerar. En vanlig aktiv-passiv teknik är VRRP. Alla ingående noder bör, som i fallet ovan, ha sessionssynkronisering aktiverat mellan varandra, så att kvarvarande nod kan ta över en icke fullgjord uppgift från en fallerad nod.
- Aktiv – Passiv, cold standby. Endast en nod är aktiv och i drift. Vid ett ev. driftavbrott i en komponent måste en drifttekniker aktivt ta den redundanta noden i drift eller så kan en aktiv watchdog process aktivera en vilande nod. I aktiv-passiv cold standby kommer alla sessioner och icke slutförda uppgifter att förloras.

9.2.1 Lastbalansering

Lastbalansering kan antingen byggas mha extern lastbalanserare från tex. F5 (BIG-IP LTM) eller Citrix (NetScaler) eller att man bygger in lastbalansering och lastbalanseringsprotokoll i tjänsten.

En extern lastbalanserare ska supportera s.k. Sticky session dvs. att den externa lastbalanseraren kan bibehålla en upprättad session till en specifik nod.

9.2.2 Krav för att bygga klustrade miljöer

I en klustrad miljö måste alla komponenter (noder/medlemmar) kunna leva autonomt och stödja flera parallella sekvenser. En sessions tillstånd och status, i en komponent, ska också kunna synkroniseras mellan noder för att en s.k. fail-over till en annan nod/medlem i klustret utan informationsförlust ska kunna ske vid ett ev. driftavbrott i en nod.

I de fall då en tjänst har krav på hög tillgänglighet men man kan acceptera att en användare får logga in igen vid en ev. fail-over till en annan nod i klustret, behöver noder och komponenter inte supportera sessionssynkronisering dvs. tjänsten ska ha så hög tillgänglighet som möjligt men man accepterar ev. förlust av sessionsinformation för en upprättad användarsession.

10. Kontinuitetskrav

Det ska finnas en tillgänglighetsplan med SLA-nivåer i enlighet med verksamhetens krav

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

11. Följsamhet till Ineras ITIL processer

Driftmiljöer ska följa Ineras Incident-, Problem-, Ändrings- och Driftsättningsprocesser samt Ineras kommande Konfigurationsprocess.

- Ineras Incidentansvarig ansvarar för att Incident- och Problemprocessen följs.
- Ineras Ändringsansvarig ansvarar för att Ändrings- och Driftsättningsprocessen följs.
- Ineras Konfigurationsansvarig ansvarar för att kommande Konfigurationsprocess följs.

12. Tillkommande krav för Containerbaserad exekveringsplattform

Inera har som målsättning att införa Containerbaserad exekveringsplattform t.ex. baserad på Docker. Docker eller annan kommande plattform kommer att ha en påverkan på denna Anvisning och eventuella referenser till andra Anvisningar som berör Containerbaserad exekveringsplattform när det införs.

Innehållet och kommande krav för att bygga Containerbaserad exekveringsplattform ska i denna utgåva ses som av informativ karaktär. Utförligare information kommer att införas i kommande utgåva.