Juni 2022
**Bilaga 3**

# Säkerhetsbilaga IA-systemet

# Innehåll

# 1 Inledning

Afa Trygg tjänstepensionsaktiebolag org. nr. 516401–8615 (Leverantören) strävar efter att upprätthålla en god säkerhet för såväl kunders (Användarorganisationer) information som sin egen. För att uppnå det utförs allt arbete på ett strukturerat och dokumenterat sätt samt utvärderas regelbundet med syfte att ständigt förbättra säkerhet och kvalitén.

Denna säkerhetsbilaga redogör för hur Leverantören arbetar för att uppnå god säkerhet för sina användarorganisationers information som hanteras i systemet ”Informationssystem för Arbetsmiljö”, härefter kallat för IA-systemet.

Sist i dokumentet finns ett appendix som listar verktyg som används i säkerhetsarbetet.

Bilagan inkluderar även ett kapitel som avser krav om användarorganisationens ansvar i att bidra till säkerhetsarbetet.

Frågor gällande Leverantörens arbete för god informationssäkerhet kan ställas till IA-supporten på e-postadress: iasupport@afaforsakring.se.

# 2 Organisatoriska skyddsåtgärder

## 2.1 Ledarskap

Informations- och IT-säkerhet är fokusområden vid såväl utveckling, drift och förvaltning.

## 2.2 Organisation

Leverantören har en dedikerad organisation, IA-verksamheten” som ansvarar för samtliga aspekter (till exempel utveckling, drift, förvaltning, säkerhet och support) av IA-systemets applikationer och plattformar.

Drift och förvaltning av IA-systemet sker av Leverantören utan nyttjande av tredje part.

### 2.2.1 Säkerhetsfunktionen

Till sin hjälp har IA-verksamheten en central säkerhetsfunktion som bistår med kompetens, utvärderingar, och riktlinjer för informations- och IT-säkerhet. Säkerhetsfunktionen hanterar även frågor gällande fysisk säkerhet och personalsäkerhet.

### 2.2.2 Computer Emergency Response Team (CERT)

Utöver den centrala säkerhetsfunktionen sätts vid behov ett internt Computer Emergency Response Team (CERT) samman som under ledning av säkerhetschefen är till för att stoppa, analysera och leda återställningen av eventuell skada som skett vid en attack.

## 2.3 Personal

Leverantören använder sig av egen samt inhyrd personal för att leverera IA-systemet (i fortsättningen omnämnd som “samtlig personal”).

### 2.3.1 Tystnadsplikt

Samtlig personal skriver på avtal om tystnadsplikt innan åtkomst till IT-system i enlighet med Lag (2020:914) om tystnadsplikt vid utkontraktering av teknisk bearbetning eller lagring av uppgifter.

### 2.3.2 Bakgrundskontroll

Grundläggande bakgrundskontroll på ny personal, både anställda och konsulter, som ska arbeta med IA-systemet.

### 2.3.3 Utbildning

Samtlig personal som börjar arbetar med IA-systemet får utbildning om hur IA-systemet nyttjas, vilka restriktioner som finns samt en introduktion till relevanta styrande interna regler.

Utöver det får personalen säkerhetsutbildning specifik för sin yrkesroll, det kan vara saker som till exempel säker programutveckling, hotmodellering, användandet av säkerhetsverktyg.

Leverantören arbetar sedan löpande för att hålla personalen uppdaterad kring ovanstående samt kontinuerligt vidareutbilda personalen när det tillkommer relevanta områden.

### 2.3.4 Uppföljning

Regelbundna samtal med samtlig personal nyttjas för att säkerställa en god arbetsmiljö samt upptäcka och förebygga otillbörligt agerande.

## 2.4 Styrande Interna Regler

Via styrande interna regler (administrerade som dokument) säkerställer Leverantören att den operationella säkerheten upprätthålls inom organisationen. Det finns en intern process för framtagande/ändring av regler samt att gällande regler revideras minst en gång per år. De styrande interna reglerna står under kontroll av regelefterlevnadsansvarig och internrevision hos Leverantören.

## 2.5 Regelefterlevnad

Internrevisionen hos Leverantören arbetar enligt en årligen fastställd revisionsplan. Rapportering sker till styrelsen, revisionsutskott, och VD. Revisionsplanen upprättas genom en objektiv och oberoende granskning utifrån väsentlighet och risk för att ge en helhetsbedömning av verksamhetens interna styrning och kontroll.

## 2.6 Arbetsmetodiker, principer och kvalitetskontroller

Leverantören arbetar utifrån livscykelsfaserna:

- Utveckling
- Drift
- Förvaltning

Nedan redovisas de ur ett säkerhetsperspektiv relevanta arbetsmetodikerna, principerna och kvalitetskontrollerna.

### 2.6.1 Utveckling och förvaltning

#### 2.6.1.1 Arbetsmetodiker

Viktiga arbetsmetodiker är:

- Security & Privacy by Design
- Hotmodellering

- Behavior-driven development (BDD)
- Continuous Testing
    - Funktionellt
    - Icke-funktionellt
    - Kodkvalitet
    - Software Composition Analysis
- Referentgranskningar
    - Lösningsförslag
    - Kodkvalitet
- Retrospektiv
- Infrastructure as Code (IaC)

#### 2.6.1.2 Principer vid val av teknologier

Övergripande principer är:

- För att få maximal upplevelse, säkerhet och förvaltningsbarhet väljs de mest lämpliga teknologierna utifrån de egenskaper IA-systemet ska leverera, vilket i praktiken innebär att IA-systemet är ett heterogent system med många olika teknologier, både open source och proprietär teknologi
- För att bedriva en kostnadseffektiv verksamhet väljs teknologier utifrån "Consume – Buy – Build" och med det menas att Leverantören först och främst nyttjar open source, därefter proprietär teknologi och som sista utväg byggs egna lösningar
- För att ha en stabil och förutsägbar leverans väljs etablerade teknologier som har visat sig fungera
- För att underlätta för alla inblandade parter och bedriva en kostnadseffektiv verksamhet väljs de facto-standarder när sådana finns
- För att inte riskera att fastna så väljs i första hand teknologier som har ett stort och aktivt community, oavsett om det är open source eller proprietär teknologi
- För att kunna utveckla fort och säkert väljs i första hand teknologier med inbyggda kontrollmekanismer till exempel typsäkra programmeringsspråk

#### 2.6.1.3 Kvalitetskontroller

All egenutvecklad kod kontrolleras vid varje incheckning med Static Application Security Testing (SAST) och det finns en hård gateway som hindrar kod från att komma ut i produktion om den inte uppfyller alla

kvalitets och säkerhetskrav.

All kod från open source projekt kontrolleras vid varje incheckning med Software Composition Analysis (SCA).

### 2.6.2 Drift

#### 2.6.2.1 Arbetsmetodiker

- Least privilage
- Site Reliability Engineering (SRE)
- Continuous Security Scanning
    - Software Composition Analysis (SCA)
    - Dynamic application security testing (DAST)
- Continuous Testing in Production
    - Syntetisk monitorering rullar varje minut, dygnet runt för att säkerställa att IA-systemet är tillgängligt och kvalitativt
- Continuous Patching
    - Applikationer använder alltid supporterade versioner av t.ex. ramverk
    - Normalt beteende är att åtgärda identifierade sårbarheter snarast möjligt med undantag för sårbarheter som vi bedömer som väldigt små och inte äventyrar säkerheten.

#### 2.6.2.2 Kvalitetskontroller

Alla applikationer övervakas dygnet runt med hjälp av automatiserad syntetisk monitorering.

Alla miljöer (se nedan) kontrolleras veckovis med Dynamic Application Security Testing (DAST).

### 2.6.3 Incidenthantering

Incident Commander leder det operativa arbetet med hanteringen av allvarliga IT-incidenter, vilket innebär kommunikation, utredning och rapportering.

Incident Commander analyserar IT-incidenterna för att säkerställa att tillräckliga åtgärder har vidtagits för att hantera incidenten samt för att verksamheten ska kunna utnyttja erfarenheterna av dessa i den operativa riskhanteringen.

Det är i första hand Leverantörens team för Site Reliability Engineering (SRE) som utför det operativa arbetet men Incident Commander har möjlighet att kalla in all tillgänglig personal vid behov.

I det fall Leverantören utsätts för en cyberattack aktiveras Leverantörens egen CERT.

Beroende på omfattningens allvarlighetsgrad av incidenten kan Leverantörens krisledningsorganisation aktiveras.

Hantering av personuppgiftsrelaterade incidenter hanteras i enlighet med Personuppgiftsbiträdesavtalet.

# 3 Tekniska skyddsåtgärder

## 3.1 Inledning

### 3.1.1 Tekniska lager

**Applikationer**

- De applikationer som IA-användarna direkt eller indirekt nyttjar
- IA-systemets applikationer kategoriseras i tre typer:
  - Mobilapplikationer
  - Webbapplikationer
  - API:er

**Plattformar**

- De plattformar som behövs för att kunna utveckla och drifta ovanstående applikationer t.ex. Container-kluster, applikations- och databasservar
- Plattformar som sätts ihop till miljöer för applikationer att driftsättas på t.ex. produktionsmiljö, acceptanstestmiljö och utvecklingsmiljö

**Infrastruktur**

- Den underliggande infrastrukturen som behövs för att kunna utveckla och drifta ovanstående plattformar så som datacenter och virtualisering av dess resurser

## 3.2 Konfidentialitet

### 3.2.1 Åtkomstkontroll

#### 3.2.1.1 Generellt

Med hänsyn till att känsliga personuppgifter kan hanteras i IA-systemet, klassificeras data som konfidentiell. Leverantören arbetar aktivt med behovsstyrd behörighetstilldelning via attributbaserad åtkomstkontroll innehållandes bl.a. roller.

#### 3.2.1.2 För Leverantören

Leverantörens supportpersonal för IA-systemet kan för att ge korrekta svar gällande inkomna supportfrågor, behöva koppla upp sig mot användarorganisationen och därigenom ta del av organisationens data. Detta görs enbart efter skriftligt godkännande från användarorganisationen. Alla läsningar av data i IA-systemet loggas för varje enskilt ärende. Dessa loggar finns tillgängliga i IA-systemet för behörig personal hos användarorganisationen.

Endast ett mycket begränsat antal administratörer (namngivna) har fulla rättigheter till lagring, säkerhetskopior och katalogtjänster. Alla inloggningar i IA-systemet görs via personliga konton och loggas.

#### 3.2.1.3 För användarorganisationer

Leverantören upprättar och tilldelar endast behörigheter för ett första administrativt konto hos användarorganisationen. Användarorganisationen är därefter själva ansvariga för att administrera användare av IA-systemet inom sin organisation. Behörigheter styrs via roller, vilka tilldelas användare via administratörerna. Användarorganisationens användare, administratörer såväl som övriga användare, har möjlighet att ange en tidsbegränsad ersättare för sin behörighet.

Användarorganisationen ansvarar själv för inloggningsmetod.

### 3.2.2 Kryptering

All kommunikation använder encryption in transit med krypringsalgoritm i enlighet med 188 Scheme Crypto Policy (Swedish Certification Body for IT Security), vanligast förekommande är kryptering med Transport Layer Security (TLS) version 1.2.

Persistering (till exempel. databas) av känsliga uppgifter använder alltid encryption at rest med krypringsalgoritm i enlighet med 188 Scheme Crypto Policy (Swedish Certification Body for IT Security), vanligast förekommande är The Advanced Encryption Standard (AES), 128 bits.

Dokumenterade rutiner för hantering och uppdatering av kryptografiskt material såsom nycklar för certifikat är etablerade.

### 3.2.3 Separation

IA-systemet har helt dedikerade plattformar. Dessa är separerade från övriga system och applikationer hos Leverantören genom nätsegmentering (brandväggsregler).

IA-systemets produktionsmiljöer (produktion, utbildning och referens) är helt separerade från övriga miljöer så som t.ex. acceptanstestmiljöer genom nätsegmentering (brandväggsregler).

IA-systemet är ett så kallat multi-tenant system vilket innebär att alla

användarorganisationers data lagras i samma databas i respektive miljö och skiljs åt via logisk separation.

### 3.2.4 Skalskydd, härdning och underhåll

Alla miljöer skyddas av redundanta brandväggar.

Servrar som används för IA-systemet har Antivirus, Anti-spyware och Anti-ransomware installerat och aktiverat.

All utrustning och programvara i IA-systemet underhålls kontinuerligt och till stora delar automatiserat gällande patchning av applikationer och plattformar.

## 3.3 Riktighet

IA-systemets tid hämtas från systemets servrar, samt bakomliggande tjänster. Loggade tider presenteras i användarbrowserns tidszon och formatet hämtas från användarens språkinställning.

Det går inte att manipulera loggarna inifrån IA-systemet. Loggarna sparas i befintligt skick.

### 3.3.1 Spårbarhet

Central logghantering nyttjas för IA-systemet samt för relaterad nätverkskommunikation. Utsedd personal arbetar aktivt med att upptäcka riskfyllda händelser via regelbaserade alarm samt verktyg för avvikelseanalys. Vid behov kan relevanta delar av loggarna göras tillgänglig för användarorganisationen.

Data skyddas via behörigheter som kontrolleras på alla nivåer i IA-systemet. Hantering av data loggas, såväl läsning, editering samt inloggning. Även misslyckade inloggningsförsök loggas.

Systemet loggar ändring och läsning av händelsedata. Loggning av inloggningar görs för så väl lyckade som misslyckade försök. Behörighetsförändringar loggas också.

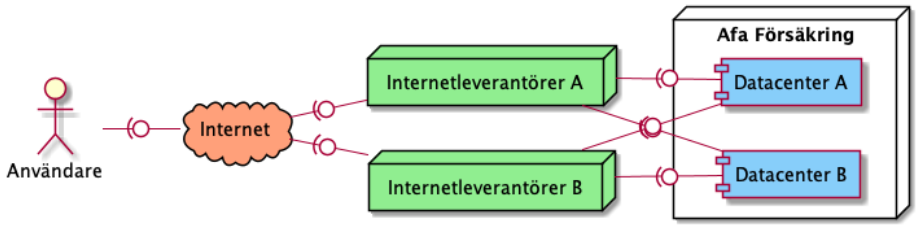
Tillgång till loggar är alltid behörighetsstyrt.

## 3.4 Tillgänglighet

### 3.4.1 Redundans

#### 3.4.1.1 Internetuppkoppling

Två oberoende, externa leverantörer nyttjas för att säkerställa redundant uppkoppling till internet.




#### 3.4.1.2 Datacenter

Båda datacentren är systemmässigt identiska och är speglade i realtid, det för att kunna erbjuda en hög tillgänglighet utan behov av nedtider.

Avseende sabotageförsök genom så kallade ’denial of service’ skyddas miljöerna genom inbyggd teknologi i brandvägg samt genom internetoperatörens försorg.

##### 3.4.1.2.1 Datacenter A

- Lokaliserat i Stockholmsområdet
- Privat datacenter
- Datacentret nyttjas av Leverantörens försäkringsrörelse, kapitalförvaltning, den förebyggande verksamheten och stödfunktioner
- Intern värdering till skyddsnivå 2 (MSB)

##### 3.4.1.2.2 Datacenter B

- Lokaliserat i Stockholmsområdet
- Samlokaliseringscenter
- Leverantören har egen utrustning, placerade i låsta rack, i en dedikerad och åtkomstkontrollerad bur
- Datacentret nyttjas av Leverantörens försäkringsrörelse, kapitalförvaltning, den förebyggande verksamheten och stödfunktioner
- Övriga kunder som nyttjar samlokaliseringscentret är okända
- Intern värdering till skyddsnivå 3 (MSB)

##### 3.4.1.2.3 Säkerhet specifikt kopplat till datacentren

Den fysiska säkerheten i våra datorhallar består av inbrottslarm, brandskydd, inpasseringssystem samt kameraövervakning.

Inbrottslarmet är kopplat till ett bevakningsföretag som inställer sig på larm dygnet runt. Driftsmiljön patrulleras av väktare, detta sker med oregelbundna intervall och minst två gånger per dygn.

Brandskyddet består av såväl rökdetektorer vilka är kopplade till räddningstjänsten som automatisk släckutrustning.

System för skydd mot strömavbrott finns.

Endast behörig personal har fysisk åtkomst till datorhallarna, access till datorhallarna är behörighetsstyrd. Inpasseringssystemet loggar såväl lyckade som misslyckade försök till fysisk åtkomst.

Data på digitala medier som utrangeras raderas, därefter destrueras de digitala medierna. Detta sker på en sekretessanläggning av säkerhetsgodkänd personal.

### 3.4.2 Säkerhetskopiering och återställning

Databaser såväl som transaktionsloggar säkerhetskopieras regelbundet, och återläsning av säkerhetskopior testas regelbundet. Systemet är anpassat för en maximal dataförlust på 1 timma, men backup sker på transaktionslogg var 15:e minut 24/7/365.

- RPO (Recovery Point Objective/Data loss) på 1 timme
- RTO (Recovery Time Objective/Down time) på 8 timmar

Säkerhetskopior tas på servrar i båda datorhallarna och sparas på en plats skild från originalet, i 60 dagar.

### 3.4.3 Monitorering

Alla applikationer, plattformar och infrastruktur övervakas dygnet runt med hjälp av automatiserad monitorering. Avvikelser larmas till behörig personal.

### 3.4.4 Export av data

Händelsedata från IA-systemet kan hämtas som Excel-filer eller PDF:er. Data om riskhanteringar hämtas som protokoll till PDF.

### 3.4.5 Avveckling

Efter avtalets upphörande och, i enlighet med de allmänna villkoren, kommer personuppgifter raderas på inrapporterade arbetsskaderisker och arbetsskador.

Användarorganisationen kan ta ut sitt data ur systemet. Data om inrapporterade händelser hämtas ut till Excel, data om inrapporterade riskhanteringar hämtas som protokoll till PDF.

# 4 Användarorganisationens egna ansvar

## 4.1 Webbapplikationen

### 4.1.1 Uppdaterade webbläsare

IA levereras som en SaaS-tjänst som används via webbgränssnitt. Webbapplikationen är anpassat för xhtml-kompatibla webbläsare och optimerat för chromiumbaserade webbläsare. Webbläsare ska hållas uppdaterade.

### 4.1.2 Val av inloggningsmetod

IA-systemet erbjuder inloggning via användarnamn/lösenord och/eller Single sign-on (SSO) via SAML 2.0.

Inloggning med hjälp av SSO ökar säkerheten vid användning av IA-systemet. Användarorganisationen kan själv konfigurera så att bara inloggning via SSO accepteras, på så sätt säkerställs att användare av IA-systemet har autentiserat sig innan inloggning sker i IA-systemet. SSO medför dock att anonym rapportering av ärenden i IA-systemet inte är möjligt.

Nivån för autentisering sätts av användarorganisationen vid konfiguration av SSO i användarorganisationens miljö.

Logg över SSO-inloggningar finns tillgänglig för behöriga användare i systemet. I loggen framgår eventuella inloggningsproblem för enskilda användare.

### 4.1.3 Hantering av positionsdata/koordinater

IA-systemet använder Google Maps för kartfunktion.

Användning av Google Maps innebär godkännande av Googles användarvillkor: https://maps.google.com/help/terms_maps/ och Privacy policy https://www.google.com/policies/privacy/ . När kartan öppnas förs inga uppgifter över till Google från IA-systemet.

Om användarorganisationen inte önskar använda Google Maps funktionen kan den stängas av under Generella inställningar på sidan Admin/Organisation i systemet.

## 4.2 Mobilapp

Till systemet finns en mobilapp för inrapportering, som det är valfritt att använda. Mobilappen är utvecklad för iOS och Android och finns publicerad på Appstore och Google play för nedladdning.

Det är viktigt att hålla appen uppdaterat till senast publicerade version.

Appen använder telefonens inbyggda kamera och kartfunktion vilket ger möjlighet att skicka med bilder och/eller positionsuppgifter. Det går att

stänga av dessa båda funktioner via systemets administrationsfunktion.

Kommunikation mellan mobilapp och systemets backend sker krypterat via https. Uppgifter skickas i första hand från appen till backend, endast ärendets status returneras till appen.

Inloggning i appen sker via gruppkonto via användarnamn och lösenord.

## 4.3 Api:er

IA-systemet har api:er för automatiserad administration av organisation och användare samt tjänster för att hämta data.

Api:erna är versionshanterade. Information om nya versioner av api:erna når användarorganisationen via systemets nyhetsbrev. Gamla api:er tas bort ca 6 månader efter att de nya publicerats.

Logg över importer framgår i systemet för behöriga användare. Eventuella felposter framgår i loggen.

# Appendix 1 – Verktyg

| Verktyg | Användningsområde |
|---|---|
| **Sonarcloud** | Static Application Security Testing – SAST<br>Statisk kodanalys |
| **Whitesource** | Software Compositional Analysis - SCA<br>Automatiserad analys och beskrivning av mjukvara med öppen källkod |
| **Holm Security** | Dynamic Application Security Testing – DAST<br>Programtester i drifttillstånd för att hitta säkerhetsproblem |