Säkerhetsdeklaration version 1.1

1. Information om leverantören

Leverantörens namn: ITSL Solutions AB
Kontaktperson/uppgiftslämnare: Fredrik Jonasson
E-post: fredrik@itsl.se
Telefonnummer: 070-330 11 89

2. Systemöversikt

ITSL Hubs är en säker digital samarbetsplattform utvecklad av ITSL Solutions för att möta offentlig sektors krav på informationshantering. Plattformen erbjuder funktioner för säker kommunikation och samarbete (bl.a. filhantering, meddelanden och integration med nationella tjänster som SDK) i en helhetslösning som utgör ett svenskt alternativ till utländska molntjänster. Systemet drivs i Sverige på lokal molninfrastruktur (Secuvas driftmiljö i IP-Onlys datacenter i Stockholm) och bygger på en härdad open source-plattform, vilket ger hög säkerhet, transparens och full kontroll över data. Ni kan därigenom uppfylla lagkrav (t.ex. geografisk lagring inom Sverige, GDPR) med denna lösning.

En detaljerad översikt av systemets komponenter och IT-miljö återfinns i bilaga "Arkitekturbeskrivning".

3. Informationshantering

3.1 Informationstillgångar

Systemet hanterar främst elektronisk information som användaruppgifter (t.ex. namn, kontaktinfo, organisationstillhörighet), autentiseringsdata (inloggningsuppgifter och loggar), samt arbetsmaterial och meddelanden som användarna lagrar eller skickar.

Detta innefattar filer och dokument som kan innehålla personuppgifter eller känslig information, SDK-meddelanden (säker digital kommunikation mellan myndigheter) och metadata kring kommunikationen. Även systemloggar och konfigurationsdata räknas som viktiga informationstillgångar.

Utöver den affärsdata som kunderna lagrar är leveransen beroende av vissa underliggande informationstillgångar såsom kryptografiska nycklar/certifikat (för kryptering och signering), kontouppgifter för administratörer, samt information om infrastrukturen (t.ex. virtuella serveravbilder och nätverksinställningar) som krävs för driften. Alla dessa tillgångar identifieras och inventeras inom ramen för leveransen. ITSL Solutions upprätthåller en centraliserad krypterad databas över informationstillgångar i våra kundleveranser, där tillgångarna kategoriseras (t.ex. kunddata, autentiseringsdata, loggar) och värderas utifrån känslighet.

Förvaltning av informationstillgångarna sker genom att ansvariga är utsedda för respektive tillgång och att rutiner finns för att hålla inventeringen uppdaterad.

Kunderna behåller ägarskap över sin data i systemet och styr vilka som har åtkomst, medan leverantören ser till att skyddsmekanismer är på plats under hela livscykeln.

3.2 Artificiell intelligens

I dagsläget ingår ingen AI-funktionalitet i den erbjudna versionen av Hubs. Plattformen har visserligen stöd för vissa AI-baserade funktioner i grunden, men dessa är inte aktiverade i leveransen. Om ni framöver skulle identifiera ett behov av AI-stöd kan leverantören vid behov tillhandahålla mer information om hur sådana funktioner kan implementeras i systemet. Sammanfattningsvis är AI ej relevant för nuvarande systemdrift, vilket minimerar komplexitet och potentiella risker kopplade till AI.

4. Arkitektur

4.1 Datacenter

Tjänsten levereras från Secuvas datacenter i Stockholm, Sverige. Secuva utnyttjar två högmoderna datahallar i Stockholmsregionen (belägna i Hammarby och Sätra, ägda av IP-Only/GlobalConnect) för drift av molntjänsten.

Geografisk placering: Båda datahallarna är belägna inom Sverige (Stockholmsområdet) för att säkerställa datahållning inom landet. Primär drift sker i anläggningen i Hammarby, med möjlighet till redundans via hallen i Sätra.

Fysisk säkerhet: Datacentren är inrymda i skyddade byggnader med omfattande fysiskt skalskydd. Områdena övervakas med kamerabevakning dygnet runt och regelbundna säkerhetsronder av väktare. Flera lager av åtkomstkontroll finns; för att komma in krävs passage genom grindar och dörrar med behörigt passerkort samt biometrisk verifiering (t.ex. fingeravtryck). Endast auktoriserad personal har tillträde, och alla besök loggas. Byggnaderna är utrustade med inbrottslarm direkt kopplade till larmcentral, vilket gör att obehöriga försök att ta sig in omedelbart upptäcks och hanteras.

Zonindelning: Internt är datacentren indelade i separata säkerhetszoner och datahallar. Secuva har egna låsta utrymmen inom dessa datahallar som är isolerade från andra kunders utrustning. Dessa sektioner utgör särskilda säkerhetszoner där endast behöriga kommer in. Zonindelningen förhindrar att händelser i en zon påverkar andra – till exempel är olika kundmiljöer och infrastrukturelement logiskt segmenterade för extra säkerhet.

Åtkomst till datacenter: Endast driftpersonal med särskild behörighet (t.ex. datacenterleverantörens tekniker samt utsedda Secuva-tekniker) har fysisk åtkomst till servrarna. All inpassering styrs via elektroniskt passagesystem och registreras i loggar; utdrag ur passersystemet och kamerainspelningar kan tillhandahållas för revision vid behov. Personalens åtkomst är rollbaserad och minimerad efter behov, och kräver

multifaktor-autentisering (både passerkort och biometrisk verifiering). Regelbundna kontroller görs av åtkomsträttigheter till datacentret, och listor över godkända personer uppdateras vid personalförändringar.

Dimensionering för tillgänglighet: Datahallarna är konstruerade för hög tillgänglighet motsvarande Tier-3-standard. Det innebär att kritiska system är redundant uppsatta så att underhåll eller fel inte ska orsaka driftstopp. Det finns redundant kraftmatning med UPS-batterier och dieselgenerator som reservkraft (i N+1- eller 2N-konfiguration), så att anläggningen kan drivas oberoende av elnätet vid avbrott. Även kylsystemen är redundant utformade (N+1/2N) för att hålla rätt temperatur. Datacentren har avancerad branddetektering (luftprovtagning) och släcksystem med inert gas anpassad för serverhallar; brandlarm är direktkopplat till räddningstjänsten. Även fukt- och översvämningssensorer finns installerade. Sammantaget klarar anläggningarna av att leverera kontinuerlig drift dygnet runt. Driftcentralen (NOC) övervakar kritiska parametrar 24/7. Kombinationen av skalskydd, redundans och övervakning gör att tillgänglighetsmålen uppfylls med god marginal (99,9%+ upptid).

4.2 System och delsystem

Systemets arkitektur är modulärt uppbyggd och består av flera samverkande delkomponenter. En central webbaserad applikation (gränssnittet "Hubs") utgör portalen där användarna loggar in och får tillgång till tjänster som dokumenthantering, meddelanden m.m. Under ytan finns separata serverkomponenter för olika funktioner – exempelvis filhantering, databastjänst, autentiseringstjänst och integrationskomponenter.

Dessa komponenter körs som container-applikationer i Secuvas molninfrastruktur (IP-Onlys datacenter) och kommunicerar över interna API:er. Arkitekturen följer principen om lagerindelning: det finns ett presentationslager (webbgränssnitt/API), ett applikationslogiklager samt ett datalager (databaser och filstorage). Detta ger tydlig separation och förenklar både skalning och säkerhetskontroll (t.ex. kan databasservrar skyddas bakom extra brandväggar). Systemet är designat för att vara horisontellt skalbart, så att fler instanser av en komponent kan läggas till vid ökad belastning utan att störa befintlig drift.

Ingående programvaror och hårdvaror: Hubs-plattformen bygger på välbeprövade öppna källkodsprodukter som har anpassats för hög säkerhet. Kärnan i systemet bygger på teknologi från Nextcloud, en plattform för fil- och samarbetsfunktioner. Ovanpå koden för Nextcloud har ITSL utvecklat och integrerat ytterligare moduler för särskilda behov, såsom säker meddelandehantering (inklusive fullt stöd för SDK-standardens API:er), gruppbrevlådor, fax och identitetshantering. Varje ingående programvara (t.ex. Nextcloud och övriga open source-komponenter) är noggrant härdad, granskad och paketerad av ITSL Solutions för att möta offentlig sektors höga säkerhetskrav.

På hårdvarusidan körs plattformen på en fysisk infrastruktur med x86-baserade Dell-servrar i kluster, redundanta NetApp-lagringssystem och Juniper-nätverksutrustning.

Containers orkestrerar applikationerna, vilket gör att ingen specifik kundhårdvara behövs på plats – allt levereras som en molntjänst. Hårdvarukomponenter som CPU, minne, lagring och nätverkskort övervakas kontinuerligt och byts proaktivt ut vid tecken på fel, så att applikationen kan fungera utan avbrott.

Specifikt utvecklade säkerhetsmekanismer: Utöver de inbyggda säkerhetsfunktionerna i valda plattformar har systemet flera lager av extra skydd. All kommunikation internt mellan moduler och externt mot användare är krypterad (se avsnitt 4.5). Applikationen implementerar rollbaserad åtkomstkontroll för att säkerställa att användare endast kan se och göra det deras roll tillåter. Loggning sker av viktiga händelser (se avsnitt 4.8) för spårbarhet. Vidare är plattformen integrerad med svenska e-legitimationslösningar för stark autentisering – t.ex. kan användare logga in via BankID för hög identitetsäkerhet. Systemet har också stöd för multifaktorautentisering (t.ex. via autentiseringsapp eller SMS) som komplement för att höja säkerhetsnivån. Andra säkerhetsmekanismer inkluderar intrångsskydd i applikationen (skydd mot vanliga attacker som XSS, CSRF etc. genom ramverkets säkerhetsfunktioner), samt kryptering av lagrade filer och databaser (beskrivs mer i avsnitt 4.6). Varje komponent i arkitekturen hålls uppdaterad med senaste säkerhetspatchar och genomgår regelbundet sårbarhetstester, så att eventuella nyupptäckta säkerhetshål åtgärdas.

4.3 Miljötyper – Hubs

För att säkerställa kvalitet och säkerhet arbetar vi med separata miljöer för olika ändamål. Vi har fyra typer av driftmiljöer: **produktions-, QA-, demo- och utvecklingsmiljöer**, med tydlig åtskillnad mellan dem.

- **Produktionsmiljöer** – Detta är de skarpa miljöerna som hanterar kundens verkliga data och användare. Produktionsmiljöerna är hårt säkrade och har fullständig backup. Endast behörig driftpersonal har åtkomst i produktion; utvecklare eller andra obehöriga har inte möjlighet att göra ändringar direkt i produktionsmiljön. På så vis upprätthålls en hög säkerhetsnivå och risken för mänskliga misstag i drift minimeras.

- **QA-miljöer** – Dessa miljöer används för integrationstester och kvalitetssäkring tillsammans med kunden, innan förändringar eller nya funktioner tas i drift. QA-miljöerna speglar i stor utsträckning produktionskonfigurationen. Backup tas, men mer begränsat än i produktion. ITSL/Secuva-personal har administrativ åtkomst i QA-miljöer för att kunna felsöka och stödja kundens tester. Kunder kan ges tillgång till sin QA-miljö för att verifiera integrationer och funktionalitet i förväg.

- **Demomiljöer** – I dessa miljöer kan vi demonstrera plattformens funktioner för kunden eller låta kunden prova Hubs under en avgränsad period innan de får en egen QA- eller produktionsmiljö. Demomiljöer innehåller ingen skarp kunddata och betraktas som temporära; de kan snabbt sättas upp och avvecklas efter behov. De

har normalt ingen regelbunden backup (då de är kortlivade) och åtkomst ges endast till berörda parter under demon.

- **Utvecklingsmiljöer** – Interna miljöer där ITSLs utvecklare bygger och testar ny funktionalitet initialt. Dessa miljöer är helt avskilda och kunder har aldrig tillgång till dem. Ingen backup tas på utvecklingsmiljöer, då de främst innehåller testdata och kan återskapas vid behov. Utvecklarna har full åtkomst här för att kunna iterera snabbt, men miljöerna har ingen koppling till produktionsdata eller externa tjänster.

Alla icke-produktionsmiljöer är strikt avskilda från produktionsmiljön. De körs på separata instanser och nät, utan någon koppling till produktionsdata eller -tjänster. Produktionsdata blandas **aldrig** in i test-, demo- eller QA-miljöer. Eftersom vi använder principen *Infrastructure as Code* byggs test- och QA-miljöerna ofta upp från grunden och rensas bort när de inte behövs, snarare än att drivas som permanenta instanser. Detta innebär att testmiljöer alltid kan spegla aktuell produktionskonfiguration och att oönskade förändringar inte "smyger sig in" över tid. Det säkerställer också att vi kan återskapa hela miljöer vid behov – en metodik som stärker katastrofberedskapen (se avsnitt 7.3).

4.4 Integrationer

Systemet erbjuder stora möjligheter till integration med andra system och tjänster i kundens IT-miljö. Hubs är byggt för att fungera som en central hub för dokument och meddelanden, och kan via öppna API:er och standardprotokoll kopplas samman med exempelvis kommunens ärendehanteringssystem, diarieföring, e-arkiv eller identitetshanteringssystem.

Externa system kan anropa Hubs API för att ladda upp, hämta eller uppdatera dokument och metadata, eller för att skicka och ta emot meddelanden via den inbyggda SDK-funktionaliteten. Hubs har stöd för SFTP/FTPS och andra säkra överföringsmetoder för integrationer som kräver filutbyte. Plattformen kan också integreras med Single Sign-On (t.ex. SAML2/OIDC) för att fungera sömlöst i användarens befintliga systemmiljö. Vi erbjuder färdiga plug-in-moduler för vissa vanliga system (t.ex. integration med Microsoft AD för katalogsynkronisering, eID-tjänster för autentisering) och ett flexibelt API som möjliggör anpassade integrationer.

Genom att Hubs är modulärt kan vi utöka integrationsmöjligheterna vid behov; nya API-endpoints eller webbtjänster kan utvecklas för att möta unika krav. Fokus ligger på att underlätta datautbyte på ett säkert sätt – all integrationskommunikation kan krypteras och autentiseras, och vi stödjer principen om minsta möjliga åtkomst även för systemintegrationer (d.v.s. externa system får endast åtkomst till de resurser i Hubs som de behöver). Varje integrerad lösning dokumenteras och testas noggrant för att säkerställa att den uppfyller både funktionella krav och säkerhetskrav.

4.5 Nätverk och kommunikation

Säkerhet för data under transport är ett fundamentalt krav i systemet. All klientkommunikation med Hubs över internet sker genom starkt krypterade kanaler. Webbgränssnittet och API:erna nås endast via HTTPS med TLS (endast moderna protokoll TLS 1.2 eller högre stöds). På så sätt skyddas information (som inloggningsuppgifter, meddelanden, filer) mot avlyssning och manipulation under överföring. Även intern kommunikation mellan olika serverkomponenter i Hubs-miljön sker antingen över interna nätverk som är isolerade från internet eller över krypterade förbindelser, vilket förhindrar att data kan snappas upp även om någon skulle komma åt det interna nätverket.

Systemets nätverk är uppdelat så att olika delar är logiskt separerade. Till exempel isoleras den publika webbtrafiken i en DMZ-zon, medan databasservern ligger på ett internt nät skyddat av brandvägg – endast applikationsservern får prata med databasen. Externa portar och protokoll är strikt begränsade till vad som behövs; brandväggsregler (inklusive säkerhetsgrupper i virtualiseringslagret) blockerar all onödig trafik.

Driftmiljön har inbyggda skydd mot DDoS-attacker och övervakar trafikmönster kontinuerligt. Nätverksutrustning (switchar, routrar, virtuella brandväggar) uppdateras regelbundet med säkerhetspatchar för att eliminera kända sårbarheter. Kombinationen av kryptering, segmentering och aktiv övervakning borgar för att data under transport förblir skyddad och att kommunikationskanalerna inte kan utnyttjas av obehöriga.

4.6 Datahantering och lagring

Systemet är uppdelat i logiska zoner för olika funktioner. Olika servrar/instanser (webb, applikation, databas, fillagring) körs separat och får bara kommunicera via bestämda gränssnitt. Om en komponent skulle komprometteras ger detta inte automatisk åtkomst till andra delar utan korrekt autentisering.

Virtuella servrar är grupperade i olika säkerhetsgrupper baserat på roll: front-end (exponeras utåt för webbtrafik via HTTPS), back-end (endast åtkomlig från front-end-lagret) och databas (endast åtkomlig från applikationslagret). Denna segmentering gör att även om en front-end-server skulle drabbas av en sårbarhet kan inte angriparen nå databasen direkt. Strikt brandväggs- och nätverkssegmentering tillämpas således mellan lagren.

Hubs är uteslutande en single-tenant-plattform, vilket innebär att inga kunder delar applikation; varje kunds instans är separat i både applikations- och databasskiktet. Varje kund har en dedikerad instans, vilket är vår standardleverans. Varje kunds data krypteras dessutom med kundunika nycklar, vilket gör att även om data skulle hamna utanför systemet kan ingen obehörig läsa den utan rätt nyckelmaterial.

Systemet har också innehållskontroller för att öka säkerheten. Alla filer som laddas upp skannas automatiskt av antivirusprogram (ClamAV) så att skadlig kod upptäcks och blockeras. Administratörer kan ange vilka filtyper som får laddas upp eller skickas, för att förhindra att otillåtna eller riskabla filer sprids. Om en användare försöker ladda upp en

filtyp som inte är tillåten nekas filen och händelsen loggas för uppföljning. På så vis förhindras att kända malware-filer eller osäkra format sprids inom plattformen.

All lagring är säkrad med flera mekanismer. Alla underliggande lagringsvolymer är krypterade – om någon skulle få tag i en fysisk disk är datan oläslig utan dekrypteringsnycklar. Säkerhetskopior av data är också krypterade och lagras åtskilt (se 7.3). Ingen slutanvändare har direkt filsystemåtkomst; all åtkomst sker via applikationens behörighetskontroller och filsystemets rättigheter, vilket förhindrar obehörig insyn även internt.

Vid specifik beställning från kunden då detta är kostnadsdrivande har vi även möjlighet att aktivera sk. *Confidential Computing* om en kund skulle kräva att även data under bearbetning hålls skyddad i säkra exekveringsmiljöer. ITSL har utvärderat hur en *zero knowledge*-arkitektur kan implementeras genom att använda betrodda exekveringsmiljöer (TEE), och kan erbjuda sådana lösningar för kunder med extrema säkerhetskrav.

4.7 Fysisk säkerhet i kontor

Utöver det fysiska skydd som beskrivits för datacentret (skalskydd, lås, larm, bevakning) vidtas även andra fysiska säkerhetsåtgärder kring systemdriften. ITSL Solutions egna kontor i Sundsvall och övriga driftplatser har adekvata säkerhetsarrangemang – lokalerna är låsta med passer- och larmsystem. Inga servrar med kunddata finns dock i dessa kontor; all produktion ligger i våra datacenter, så den fysiska säkerheten för själva driftmiljön hanteras primärt av Secuva och dess datacenterpartner. Leverantörens personal som hanterar känsliga uppgifter (t.ex. konfigurationsbackup, krypteringsnycklar) följer interna policys för fysisk förvaring av media: t.ex. förvaras eventuella utskrifter eller bärbara lagringsmedia i värdeskåp. Därigenom minimeras risken att information på papper eller externa medier hamnar i orätta händer.

4.8 Loggning och övervakning

Systemet genomför loggning av händelser för att möjliggöra spårbarhet och upptäckt av incidenter. Alla inloggningsförsök (både lyckade och misslyckade) loggas med användar-ID, tidpunkt och IP-adress. Även viktiga användaraktiviteter – såsom skapande, åtkomst eller radering av filer, skickade meddelanden via SDK, ändringar i inställningar – genererar logghändelser. Administrativa åtgärder loggas också. Loggarna lagras centralt på en loggserver inom plattformen, separerad från själva applikationsservern, för att förhindra att en angripare kan manipulera loggarna obemärkt. Endast behörig driftpersonal har åtkomst till råa loggfiler, och åtkomsten till loggarna i sig är skyddad med stark autentisering. Logginformationen är strukturerad och tidssynkroniserad (NTP används på alla servrar) för att underlätta analys vid behov.

Loggarna övervakas både automatiskt och manuellt. Vi har implementerat varningar för vissa typer av logghändelser – exempelvis triggas larm om ett konto får många misslyckade inloggningar på kort tid (möjligt brute-force-försök), eller om en ovanligt stor datamängd

laddas ner utanför kontorstid. Sådana larm skickas i realtid till driftansvariga, som kan reagera omedelbart. Övervakningsverktyg spårar dessutom systemprestanda och resursutnyttjande; om loggar indikerar avvikande beteende (t.ex. en process som använder ovanligt mycket minne) kan driftteamet undersöka detta närmare.

Under Q1 2026 kommer en extern Security Operations Center (SOC) att anslutas till tjänsten (via leverantören Syndis) för att ytterligare höja säkerheten. SOC:en kommer att i realtid analysera logg- och larmdata från Hubs-miljön för att identifiera potentiella intrång eller misstänkt beteende som kan indikera en attack. Detta ger en extra nivå av övervakning dygnet runt och säkerställer att vi snabbt fångar upp även sofistikerade angreppsförsök.

5. Åtkomsthantering

5.1 Autentisering och auktorisation

Systemet stödjer federerad autentisering såväl som lokala konton. Användare inom kommunen kan logga in via kommunens eget AD/SSO för Single Sign-On, eller med separata Hubs-konton för externa användare. All inloggning sker över krypterade förbindelser och kräver giltiga användaruppgifter.

Behörighetsstyrningen är rollbaserad (RBAC). Varje användare tilldelas en eller flera roller som styr vilka funktioner och data som är åtkomliga. Principen om minsta behörighet tillämpas – ingen användare har mer rättigheter än nödvändigt för sina arbetsuppgifter. En vanlig användare kan exempelvis bara komma åt sina egna dokument och skicka meddelanden, medan en administratör har utökade rättigheter att hantera användare och inställningar. Det finns särskilda administratörsroller definierade: en systemadministratör (hos Secuva) med full behörighet att underhålla plattformen, samt en eller flera kundadministratörer (hos kommunen) som kan hantera den egna organisationens konton och inställningar. Kundadministratörer kan inte se eller påverka andra kunders information. Alla administratörsrättigheter tilldelas restriktivt och dokumenteras.

För lokala konton gäller strikta lösenordspolicyer med krav på komplexitet (minst 12 tecken, blandade bokstäver, siffror, specialtecken). Lösenord lagras aldrig i klartext utan hash:as med saltad algoritm (t.ex. bcrypt/SHA). Vid AD-integration gäller kommunens befintliga lösenordspolicy automatiskt. Konto-låsningsmekanismer finns – efter upprepade felaktiga inloggningar spärras kontot temporärt eller tills administratör verifierat användaren, för att motverka brute force-attacker.

Systemet har stöd för multifaktorautentisering (MFA) för att höja säkerheten. Exempelvis kan BankID eller engångskoder via SMS/autentiseringsapp användas som extra inloggningssteg, beroende på vad som bestäms vid införandet hos kunden. Administratören kan kräva tvåfaktor för alla användare eller för vissa känsligare roller. Med MFA måste användaren ange både lösenord och en engångskod vid inloggning, vilket kraftigt försvårar obehörig åtkomst även om ett lösenord skulle läcka.

5.2 Autentisering och auktorisation – höga behörigheter

Åtkomst till administrationskonton med hög privilegienivå i produktion är strikt kontrollerad. Endast ett fåtal utsedda ITSL-medarbetare (systemadministratörer) har sådana behörigheter. Dessa personer har genomgått bakgrundskontroller och lyder under stränga sekretessavtal. Alla inloggningar till administratörskonton är föremål för extra övervakning och loggas separat för granskning. Vid användning av administratörskonton krävs alltid multifaktorautentisering. Alla ändringar som görs via dessa konton dokumenteras i ändringshistorik.

5.3 Avslut av behörigheter

När en anställd hos ITSL slutar eller byter roll finns rutiner för att snabbt ta bort eller justera dennes åtkomst. Inför sista anställningsdagen inaktiveras eller raderas personens konton i alla relevanta system (administratörskonton i Hubs, utvecklingssystem etc.). Detta sker i direkt anslutning till avslutad anställning. Vid interna rollförändringar ses medarbetarens behörigheter över så att onödiga rättigheter avlägsnas och eventuellt nya läggs till utifrån den nya rollen, efter godkännande.

Regelbundna revisioner av användarregister genomförs för att säkerställa att inga aktiva konton finns kvar för personer som slutat. Eftersom inga privata eller generiska konton används för driftåtkomst är det enkelt att stänga av en användare som slutat. Eventuella arbetsrelaterade data från den anställdes konton hanteras enligt rutin (t.ex. överlämnas eller arkiveras), och känsliga nycklar eller lösenord som personen haft kännedom om byts ut. Dessa åtgärder minimerar risken att före detta personal behåller obehörig åtkomst.

5.4 Löpande hantering av åtkomst

Behörigheter och konton administreras aktivt under hela driften. KISA (Kvalitet- och InformationsSäkerhetsAnsvarig) utför årsvisa genomgångar av samtliga användarkonton och deras rättigheter för att verifiera att de är korrekta och aktuella.

Vid nyanställningar eller ändrade arbetsuppgifter följs en formell process: den nya användarens chef eller kundens systemansvarige begär specifika åtkomsträttigheter, någon med behörighet (t.ex. systemägare eller säkerhetsansvarig) godkänner, och sedan implementeras ändringen av systemadministratören. Allt dokumenteras, så att det i efterhand går att se vem som begärt och godkänt en viss behörighetsändring och när den utfördes.

5.5 Tredjeparts åtkomst

Som standard ges inga externa parter tillgång till kunddata eller systemet utan uttryckligt tillstånd. ITSL anlitar inte underleverantörer för drift av Hubs; all känslig drift hanteras av ITSLs egen personal (inklusive Secuvas driftteam för infrastruktur) enligt avtal. Vid behov av specialiststöd (t.ex. vid säkerhetsgranskningar eller akut expertis) säkerställer vi att strikta avtal (NDA, personuppgiftsbiträdesavtal m.m.) finns på plats och att dessa tredjeparter inte

får direktåtkomst till systemet, utan arbetar på utdragna data eller i kontrollerade sessioner under uppsikt av ITSL.

6. Systemutvecklingsprocess

6.1 Utvecklingsprocess

Informationssäkerhet beaktas i samtliga steg av utvecklingen av Hubs.

Systemutvecklarna har hög kompetens kring säker kodning och är medvetna om vanliga sårbarheter (som XSS, SQL-injektion) som ska undvikas. Vi använder säkra ramverk och pålitliga tredjartsbibliotek för funktioner som kryptering i stället för att uppfinna egna lösningar.

Årligen genomförs också penetrationstester, antingen automatiserat eller manuellt, för att upptäcka eventuella säkerhetsluckor. Vi anlitar leverantören Syndis för dessa oberoende penetrationstester. De utförs vanligtvis i början på året, men kan vid behov genomföras oftare. Efter varje penetrationstest går vi igenom resultatet noggrant och åtgärdar eventuella funna sårbarheter skyndsamt.

De öppna komponenter som plattformen bygger på (t.ex. Nextcloud) är dessutom kontinuerligt säkerhetsgranskade av sina respektive communities och utvalda just för att de underhålls aktivt och har en transparent utvecklingsprocess. Eventuella säkerhetsproblem i dessa komponenter fångas upp och patchas ofta mycket snabbt av communityn, vilket vi drar nytta av genom att hålla våra system uppdaterade.

All källkod dokumenteras i versionshanterings- och ärendehanteringssystem (GitLab), vilket ger spårbarhet från krav till leverans. Varje ändring kopplas till ett ärende, kodgranskas av minst två utvecklare och testas innan den levereras. Historik och diffar finns bevarade för alla förändringar, vilket underlättar felsökning och revisionsspårning.

6.2 Ändringshantering

Vi följer en formell ändringshanteringsprocess för alla förändringar i systemet, särskilt i produktionsmiljön. Varje föreslagen ändring initieras med ett ändringsärende (Change Request) där ändringen beskrivs, motiveras och analyseras. Vi använder GitLab som verktyg för att hantera förändringsärenden och releases.

Både programvaruändringar (nya releaser, patchar) och större konfigurationsändringar omfattas av processen. Alla kundpåverkande ändringar (t.ex. ny funktionalitet eller planerade driftavbrott) kommuniceras i förväg med kunden enligt avtalat SLA.

Efter godkännande planeras och genomförs ändringen, oftast först i test-/QA-miljö för verifiering innan produktionssättning. Varje steg – beslut, tester, godkännande och utförande – dokumenteras i ändringsärendet med tidsstämplar och ansvariga. Inga oplanerade direktändringar görs i produktion; allt är spårbart och genomgånget enligt rutin.

Vi har en central konfigurationsdatabas över samtliga komponenter i drift. I detta register noteras aktuell version (t.ex. vilken version av Hubs, databashanterare, operativsystem som körs), installationsdatum och senaste uppdatering. När en komponent uppdateras genom en ändring uppdateras även dokumentationen. Detta kan delvis ske automatiskt via skript, men verifieras manuellt.

Alla förändringar i underliggande infrastruktur (t.ex. hypervisor, lagringssystem) loggas och dokumenteras. Denna dokumentation gör att vi snabbt kan svara på frågor om vilken version som körs var, och det underlättar felsökning (t.ex. om ett problem uppstod direkt efter en viss uppdatering).

6.3 Säkerhetsbedömningar

Vi har ett löpande arbete för att proaktivt identifiera svagheter. Detta inkluderar automatiska skanningar av systemets nätverksytor (öppna portar/tjänster) samt kontroller av servrar och applikationer mot kända sårbarheter (CVE-databasen m.m.). Vi bevakar nyupptäckta säkerhetshål i de teknologier vi använder – t.ex. prenumererar vi på säkerhetsbulletiner från leverantörer och relevant community (som Nextcloud) – så att vi snabbt får reda på om något behöver åtgärdas.

Utöver verktygsbaserade skanningar gör vi med jämna mellanrum manuella genomgångar av systemets säkerhetsarkitektur och hotbild, för att beakta nya risker i takt med att systemet eller omvärlden förändras.

Minst en gång om året låter vi en extern säkerhetsexpert (Syndis) genomföra ett djupgående penetrationstest av Hubs (antingen direkt mot produktionsmiljön under kontrollerade former, eller mot en identisk staging-miljö). Testaren försöker då hitta och utnyttja eventuella sårbarheter i allt från nätverket (t.ex. öppna portar eller felkonfigurerade tjänster) till applikationen (t.ex. XSS, SQL-injektion, brister i affärslogik eller åtkomstkontroller). Resultatet av dessa tester dokumenteras och ligger till grund för förbättringsåtgärder som prioriteras in i utvecklingsprocessen.

6.4 Kapacitetsplanering

Vi planerar kapacitet för nätverk, lagring, databaser och applikation proaktivt för att upprätthålla god prestanda. Systemet övervakas kontinuerligt avseende belastning: vi följer CPU-, minnes- och diskutnyttjande, databassvarstider och nätverkstrafik. Om trender visar att vi närmar oss kapacitetstak (t.ex. att lagringsutrymmet börjar bli fullt vid ~80% av tilldelad kapacitet) utökar vi resurserna i god tid innan det blir kritiskt.

I Secuvas molninfrastruktur kan vi snabbt skala upp resurser (öka CPU/RAM, utöka diskvolymer), och systemarkitekturen medger att fler applikationsinstanser kan läggas till bakom lastbalansering vid behov. Nätverket är dimensionerat med hög bandbredd och redundanta förbindelser, och övervakas kontinuerligt för att undvika flaskhalsar.

Denna skalbarhet och övervakning innebär att vi kan möta ökad efterfrågan utan att tumma på prestanda. Skulle en kund exempelvis öka antalet användare markant eller lagra ovanligt stora datamängder kan vi snabbt tilldela mer CPU, minne eller lagring så att användarupplevelsen förblir god.

7. Drift av systemet

7.1 Drift

Systemet övervakas dygnet runt för att säkerställa hög upptid och snabb respons vid driftstörningar. Övervakningsverktyg larmar automatiskt om en kritisk tjänst blir otillgänglig eller om resurser överstiger givna tröskelvärden (t.ex. om CPU- eller minnesanvändning blir för hög, eller om en diskenhet håller på att fyllas).

Larmen går direkt ut till ITSLs jourtekniker via flera kanaler (SMS, e-post m.m.) så att åtgärder kan initieras omedelbart, oavsett tid på dygnet.

Tack vare denna övervakning kan vi ofta upptäcka och åtgärda potentiella problem innan de påverkar slutanvändarna (t.ex. utöka lagringsutrymme innan det blir fullt, eller återstarta en tjänst som börjar uppvisa felbeteende). Driftpersonalen följer etablerade felsökningsrutiner när larm utlöses och eskalerar ärenden enligt incidenthanteringsplanen (se 7.2) om problemet inte snabbt kan avhjälpas. Utöver realtidsövervakningen genomförs dagliga kontroller, såsom att verifiera att nattens säkerhetskopiering lyckades och att inga oväntade felmeddelanden dykt upp i loggarna.

Vi genomför regelbundet uppdateringar för att hålla systemet stabilt och säkert. Mindre förbättringar och buggfixar samlas normalt till planerade underhållsfönster (t.ex. månadsvis eller kvartalsvis beroende på avtal med kunden). Innan uppdateringar installeras i produktion testas de alltid först i en QA- eller testmiljö för att säkerställa att de inte orsakar regressioner. Kritiska säkerhetsuppdateringar prioriteras alltid: om en allvarlig sårbarhet upptäcks i någon komponent (operativsystem, databas, applikation) applicerar vi patchar skyndsamt, ibland utanför ordinarie schema – ofta inom 24 timmar från att en patch släppts, i dialog med kunden. Mindre brådskande patchar kan inkluderas i nästa ordinarie release.

Vi ser också till att underliggande system är uppdaterade; operativsystem och plattformstjänster får regelbundna patchar (t.ex. veckovisa automatiserade uppdateringar av säkerhetsfixar) så länge de inte stör tjänsten. Under uppdateringsarbetet följer vi definierade rutiner: vi tar backup före större ändringar, installerar uppdateringar kontrollerat (ibland en nod i taget om möjligt för att undvika nertid) och övervakar sedan systemen noggrant.

Ändringshantering i driftmiljön följer de formella rutinerna (se 6.2). Även mindre justeringar bedöms och testas i förväg om de kan påverka kunder. Inga hastiga ingrepp görs utan riskanalys, vilket ger en stabil drift.

Vi arbetar också löpande med att identifiera och hantera sårbarheter under drift. Tack vare omvärldsbevakning (se 7.2) är vi medvetna om nya hot, och vi genomför regelbundna sårbarhetsskanningar även på produktionsmiljön. Om en ny sårbarhet upptäcks i någon komponent vi använder analyserar vi om Hubs är påverkad och tillämpar i så fall uppdateringar eller skyddsåtgärder snarast möjligt.

Vi planerar även för att införa intrångsdetektering via en extern SOC-tjänst (som nämnts i avsnitt 4.8) under Q1 2026, vilket ytterligare kommer förbättra möjligheten att upptäcka avancerade attacker mot driftmiljön i realtid.

7.2 Incidenthantering

Omvärldsbevakning: Vi bedriver aktiv omvärldsbevakning av säkerhetshot och sårbarheter för att förebygga incidenter. Via CERT-SE, MSB, CVE-databaser och andra säkerhetskällor håller vi oss uppdaterade om nya sårbarheter, attacker och skadlig kod som kan vara relevanta. Secuva bevakar också hot mot infrastrukturen och förser oss med information om relevanta händelser (t.ex. varningar om DDoS-attacker eller kritiska sårbarheter i datacentermiljön). Vi deltar dessutom i branschnätverk och forum (t.ex. Cybernoden, Dataföreningens säkerhetsnätverk) för att utbyta erfarenheter och lära av andras säkerhetshändelser.

Tekniska incidenter: När en teknisk incident upptäcks (via larm eller felanmälan) kategoriserar vi den genast utifrån allvarlighetsgrad och påverkan på verksamheten. Drifttekniker felsöker omedelbart genom att granska loggar, kontrollera kända felbilder och försöka återställa funktionen. Under hela förloppet förs en incidentlogg. Kommunikation med kunden sköts enligt överenskomna SLA: vid större avbrott skickas omgående information om problemet och uppdateringar följer löpande tills det är löst. Om problemet relaterar till underliggande infrastruktur kontaktar vi datacenterleverantören för stöd (t.ex. om det gäller nätverksstörningar eller hårdvarufel i datahallen). När problemet är åtgärdat (t.ex. genom omstart av en tjänst eller en snabbfix i konfigurationen) övervakar vi systemet extra noga en tid för att försäkra att allt fungerar normalt. Sedan avslutas incidenten och vi utför en rotfelsanalys: vi identifierar grundorsaken och vidtar permanenta åtgärder för att undvika att samma typ av incident händer igen.

Säkerhets- och personuppgiftsincidenter: Misstänkta eller konstaterade säkerhetsincidenter – som intrångsförsök, malware-utbrott eller oavsiktlig exponering av känsliga personuppgifter – behandlas skyndsamt och konfidentiellt. Om något sådant inträffar larmas omedelbart KISA (Kvalitets- och Informationssäkerhetsansvarig). Första steget är att begränsa skadan: vi isolerar drabbade system eller konton (t.ex. stänger av komprometterade användare, tar en server offline, kopplar bort drabbade nätverkssegment) för att stoppa pågående angrepp och säkra bevismaterial. Vi kartlägger därefter vad som hänt genom logganalyser och forensiska verktyg – identifierar intrångsväg, omfattning och vilka data eller användare som påverkats. Vi kommer också att kontakta vår SOC för fördjupad incidentanalys om det behövs expertis i realtid.

Parallellt informeras kunden tidigt. Er utsedda kontaktperson hos kommunen får besked om att en incident skett, vilka initiala fakta vi har och vilka åtgärder som vidtas. Beroende på incidentens natur involverar vi även nödvändiga externa parter:

- Vid personuppgiftsincidenter kontaktas kommunens dataskyddsombud omedelbart (om de inte redan är involverade). Vi bistår kommunen med underlag för en eventuell anmälan till Integritetsskyddsmyndigheten (IMY) inom 72 timmar enligt GDPR, om så krävs. Det innebär att vi snabbt tar fram information om vilka personuppgifter och individer som kan vara drabbade, hur incidenten skedde och vilka konsekvenser det kan få, så att kommunen kan fullgöra sin anmälningsplikt och informera berörda.

- Vid misstänkt brottslig aktivitet (t.ex. ransomware-angrepp med krav på lösensumma) råder vi kommunen att polisanmäla, och vi säkrar då all evidens (loggar, infekterade filer) för utredning. Vi kan även kontakta MSB eller CERT-SE för rådgivning om incidenten verkar ingå i en större hotbild mot offentlig sektor.

Secuva informeras om incidenten rör datacentret eller infrastrukturen (t.ex. om ett intrång skett via virtualiseringslagret eller om datacentrets nätverk utnyttjats). De hjälper då till med fördjupad teknisk analys och åtgärder på den nivån. Under incidentens gång hanteras extern kommunikation i samråd med kunden – normalt är det kommunen som vid behov informerar allmänhet eller media, medan vi förser dem med tekniska fakta och stöd. När incidenten är under kontroll och åtgärdad (angriparen utkastad, skadlig kod borttagen, system återställt till säkert läge) gör teamet en grundlig genomgång av händelsen. En incidentrapport upprättas med tidslinje, påverkan och lärdomar, vilken delas med kunden. Avslutningsvis ser vi över om några ytterligare åtgärder krävs (t.ex. förbättrade kontroller eller utbildningsinsatser) för att förhindra liknande incidenter i framtiden.

7.3 Katastrofhantering och återställning

Backup och återställning: Alla kritiska data i Hubs säkerhetskopieras regelbundet för att kunna återställas vid en allvarlig incident. Vi tar täta snapshots och säkerhetskopior: timvisa snapshots av systemet, dagliga inkrementella backuper och veckovisa fullständiga backuper av bl.a. databasen, filområdet (användarfiler, bilagor) och viktiga konfigurationer. Detta ger ett värsta-fall RPO (Recovery Point Objective) på ca 1 timme – maximalt en timmes arbete kan gå förlorat vid en totalförlust, ofta mindre. Säkerhetskopiorna inkluderar alla väsentliga komponenter så att hela systemet kan rekonstrueras (användardata, loggar, systeminställningar m.m.).

Flera generationer av backup sparas (t.ex. dagliga för senaste veckan samt ytterligare veckobackuper över längre tid), vilket möjliggör återställning till olika tidpunkter om ett fel upptäcks för sent. Backupfilerna överförs via separata kanaler till Secuvas backupsystem som är fysiskt och logiskt skilt från produktionsmiljön. Dessa backuper är också krypterade för att skydda innehållet – om någon obehörig skulle komma över en backupfil går det inte att utläsa några uppgifter utan nycklar.

Åtkomsten till backupmiljön är strikt begränsad; endast utvalda systemadministratörer kan initiera en återläsning och produktionssystemet självt har normalt endast rätt att skriva nya backupfiler, inte att radera tidigare. Därmed påverkas inte backuphistoriken ens om produktionssystemet kompromitteras, exempelvis av ransomware.

Regelbundna tester av backup-återläsning genomförs för att säkerställa att säkerhetskopiorna verkligen går att använda och att återläsningsrutinerna är väl dokumenterade.

Återställning vid katastrof: Vi har en katastrofåterställningsplan för scenarier där primär driftmiljö blir otillgänglig, t.ex. vid brand, översvämning, omfattande strömavbrott eller större cyberangrepp mot datacentret. Planen innehåller flera nivåer av återställning beroende på skadans omfattning. Om endast applikationslagret påverkas (t.ex. en kritisk bugg i en ny version) kan vi snabbt rulla tillbaka till föregående stabila version eller flytta över tjänster till redundanta servrar inom det primära datacentret.

Om hela det primära datacentret skulle slås ut har vi en sekundär anläggning (den andra datahallen i Stockholm) dit vi kan flytta driften. Tack vare realtidsreplikering av data och automatiserade infrastrukturskript kan vi inom några timmar etablera miljön på den alternativa anläggningen och dirigera om användartrafiken dit. Dessutom finns en separat geografisk katastrofåterhämtningsplats i ett skyddat bergrum i Sverige, där uppdaterade kopior av systemet förvaras. Detta ger ytterligare redundans i händelse av en regional katastrof. RTO (Recovery Time Objective) för en total katastrof är satt till mellan några minuter och några timmar, beroende på incidentens natur och omfattning. Under en sådan återställning hålls kunden informerad kontinuerligt om förväntad nertid och eventuella temporära begränsningar i tjänsten.

Systemet är konstruerat med hög redundans även för mindre fel – t.ex. om en enskild server går sönder tar en redundant nod över automatiskt, och datacenter-nätverken har redundanta länkar – vilket gör att många avbrott inte märks alls för användarna eller endast orsakar en kort störning.

Test av återställningsförmåga: Då vi arbetar efter principen *Infrastructure as Code* är återställning och ombyggnad av miljöer en naturlig del av vårt arbetssätt. Vi bygger regelbundet upp våra test- och utvecklingsmiljöer från grunden med hjälp av kod och automatisk provisioning, vilket i princip simulerar en återställning av miljön. Genom att denna rutin ingår i vardagen är vi ständigt redo för en total återställning även av produktionsmiljön om det skulle krävas. Vi genomför dessutom planerade katastroftester där vi övar på att sätta upp en kopia av produktionsmiljön från backup i en separat miljö, för att verifiera att vår dokumentation och procedur klarar tidspressen vid en verklig katastrof. Eventuella brister i processen åtgärdas löpande, så att planen för katastrofåterställning förblir robust och uppdaterad.

8. Regelefterlevnad och systematik

8.1 Ledningssystem och riskhantering

ITSL arbetar i enlighet med de internationella standarderna ISO/IEC 27001 och ISO/IEC 27701 för informationssäkerhet och dataskydd, men är inte certifierade enligt dessa standarder.

Genom att följa dessa standarder har företaget upprättat ett integrerat ledningssystem (VLS) som effektivt samordnar arbetet med säkerhet och regelefterlevnad. Detta ledningssystem är riskbaserat och bygger på regelbundna riskbedömningar och informationsklassificering. Det innebär att ITSL systematiskt identifierar och analyserar potentiella säkerhetsrisker, samt klassificerar information och system utifrån känslighet och skyddsvärde. Baserat på riskanalysen införs sedan lämpliga säkerhetsåtgärder för att skydda data och system enligt både interna krav och kundens specifika skyddsbehov.

Ledningssystemet (VLS) integrerar krav och processer från flera områden – inte bara informationssäkerhet utan även dataskydd och andra relevanta regelverk. Genom ett strukturerat angreppssätt säkerställs att regelefterlevnad sker konsekvent i hela organisationen. Ledningen är aktivt engagerad i detta arbete och ser till att resurser avsätts för att upprätthålla och förbättra säkerhetsnivån. VLS inkluderar policyer, rutiner och kontrollmekanismer som kontinuerligt utvärderas och förbättras enligt principen om ständiga förbättringar (PDCA-cykeln: Plan, Do, Check, Act). Den integrerade ansatsen minskar dubbelarbete, då samtliga säkerhets- och regelefterlevnadsprocesser samlas under ett gemensamt system. På så vis kan ITSL snabbt anpassa sitt säkerhetsarbete när hotbilden förändras eller när nya krav från kunder och myndigheter tillkommer.

8.2 Granskningar

Interna revisioner sker årligen inom VLS, externa revisioner vid behov. Dessa omfattar regelefterlevnad, informationssäkerhet och teknisk kontroll av rutiner och efterlevnad.

Vi anlitar IT-Säkerhetsbolaget för att externt granska vårt informationssäkerhetsarbete. Resultatet av en sådan revision (i form av intyg/rapport) är bifogat i denna upphandling, alternativt kan det erhållas på begäran. Genom att låta tredje part granska oss säkerställer vi en objektiv kontroll av att våra processer och system håller måttet gentemot kravbilden.

Efter varje revision – intern som extern – följer vi upp eventuella avvikelser eller förbättringsförslag i en åtgärdsplan. Ledningen involveras i att prioritera och säkerställa att åtgärderna genomförs. Detta ger en kontinuerlig förbättringscykel där vi lär av granskningar och höjer vår säkerhetsnivå steg för steg.

8.3 Säkerhetsmedvetenhet

Inform**ationssäkerhet ingår i vårt DNA på ITSL. (Faktum är att förkortningen ITSL internt står för "IT som är Laglig och Lämplig".) Vi verkar på en marknad där hög säk**erhet och

efterlevnad är avgörande för vårt varumärke och vår trovärdighet, vilket präglar hela företagskulturen.

Varje anställd och konsult hos oss har insikten att information är en av våra viktigaste tillgångar och att skyddet av denna information är allas ansvar. Denna medvetenhet genomsyrar organisationen från ledning till nyanställda. I takt med att bolaget växer arbetar vi aktivt för att förstärka säkerhetskulturen genom kontinuerligt lärande och utbildning. Alla nyanställda genomgår introduktion i våra säkerhetspolicyer och rutiner. Vi genomför regelbundna utbildningar och påminnelser om säkerhetsfrågor, anpassade efter roll (t.ex. utvecklare får extra utbildning i säker kodning, supportpersonal i hantering av känslig information, etc.).

Genom att analysera och dela lärdomar från incidenter undviker vi att liknande händelser sker igen och höjer den samlade kompetensen. Varje säkerhets- eller integritetsincident följs upp med ett *lessons learned*-möte där vi diskuterar vad som hände och hur det kunde förebyggas. Även resultat från revisioner och förändringar i interna policyer kommuniceras tydligt ut i organisationen för att öka kunskapen och efterlevnaden. Sammantaget skapar dessa insatser en stark säkerhetskultur där medvetenheten är hög och där varje anställd känner till sitt ansvar för att skydda information samt upprätthålla företagets regelefterlevnad.