

TEKNISKA OCH ORGANISATORISKA SÄKERHETSÅTGÄRDER

1 GENERELLT

- 1.1 Hogia försäkrar att det finns erforderligt säkerhetsskydd för att leveranser som utförs av Hogia skall uppfylla de bestämmelser som anges i detta dokument samt i aktuellt produktavtal.
- 1.2 Hogia strävar efter att uppfylla MSBs (Myndigheten för samhällsskydd och beredskap) ramverk för etablering och användande av ledningssystem för informationssäkerhet (LIS) baserat på internationella standarder i ISO 27000-serien. Hogia har en informationssäkerhetspolicy som beskriver Hogias uppfyllande av angivna standarder m m.
- 1.3 Samtliga Hogias anställda omfattas av sekretessåtaganden.
- 1.4 Hogias åtaganden avseende säkerhetsskyddsåtgärder inkluderar, men är inte begränsat, till följande:
 - (a) Hogia säkerställer att säkerhetssystem och administrativa verktyg endast används på avsett sätt;
 - (b) Hogia säkerställer att anställda och konsulter inom Hogia har fått relevant utbildning i säkerhetsfrågor.
- 1.5 Säkerhetsincidentshantering. Vid en säkerhetsincident som påverkar eller kan påverka en kund rapporterar Hogia omgående till Kundens kontaktperson.
- 1.6 Hogia har i sin organisation en befattning som är ansvarig för att sköta kontakten med kunder i frågor gällande säkerhet. I det fall kund önskar, förser Hogia denne med uppgifter om den Hogia-medarbetare som innehar nämnd befattning. Se nedan kontaktuppgifter för nämnd befattning:
Befattning: CISO (Chief Information Security Officer)

Epost: ciso@hogia.se
- 1.7 Krisplan. Hogia har en dokumenterad och implementerad krisplan som regelbundet övas och revideras. I krisplaneringsarbetet ingår olika former av riskhantering.

2 GRUNDLÄGGANDE SÄKERHET

Denna del behandlar Hogias grundläggande löpande säkerhetsarbete.

2.1 Hogias IT-miljö

- 2.1.1 Hantering av tillgångar. Tillgångar förknippade med information och informationshantering definieras, registreras och uppdateras i ett centralt register som underhålls av Hogia.
- 2.1.2 Förändringshantering. Förändringar i infrastruktur, servers, driftade system och tjänster genomförs och godkänns i enlighet med Hogias förändringsprocess. Förändringsrutinerna säkerställer kontroll över alla säkerhetsrelaterade förändringar.
- 2.1.3 Backup. Backup utförs regelbundet och lagras geografiskt avskilt från den ordinarie driftsmiljön.
- 2.1.4 Skydd mot skadliga program. Kontroller för att förebygga och upptäcka skadliga program genomförs för att löpande säkerställa kapaciteten i Hogias IT-miljö att upptäcka, ta bort och skydda, så långt som möjligt är, mot alla kända typer av skadlig programvara.

- 2.1.5 Teknisk sårbarhet i system och tjänster övervakas och hanteras löpande.
- 2.1.6 Systematiska penetrationstester görs löpande på system och tjänster, exponerade mot Internet eller internt inom Hogia. Kund äger ej rätt att genomföra egna penetrationstester mot sina system om dessa finns hos Hogia, utan att först ha erhållit Hogias skriftliga godkännande.
- 2.1.7 Säkerhetsskydd av system och tjänster i nätverk. Endast godkända enheter kan kopplas till Hogias nätverk. Tillgång till system och tjänster som är kopplade till Hogias nätverk kräver auktoriserad åtkomst.
- 2.1.8 Hogia använder säkra processer vid utveckling av program och tjänster.
- 2.1.9 Hogia arbetar kontinuerligt med dataskyddsfrågor (t ex GDPR-efterlevnad) avseende våra program, tjänster, processer m m.
- 2.1.10 Åtkomstkontroll. Rutiner för åtkomstkontroll är tillämplig för all åtkomst till Hogias nätverk, program och tjänster oavsett om åtkomst initieras av kund, Hogia eller underleverantör till Hogia. Åtkomstkontroll inkluderar, men är inte begränsat till:
 - (a) Administrativa konton som används av Hogia för Hogias system och tjänster är definierade, dokumenterade och underhålls endast av personal som behöver använda dem för att utöva sitt uppdrag;
 - (b) Administrativa konton och behörigheter knyts till ett användarkonto som skiljer sig från de som används för löpande verksamhet;
 - (c) Användande av individuella användaridentiteter är ett krav oavsett om dessa används för löpande verksamhet eller för administrativa ändamål;
 - (d) Administrativa behörighetsrättigheter granskas och dokumenteras kvartalsvis;
 - (e) Ansökningar för nya administrativa konton och åtkomsträttigheter till system och tjänster dokumenteras formellt och godkänns av lämplig organisation;
 - (f) Samtliga åtkomsträttigheter för anställd avaktiveras i samband med anställningens avslutande;
 - (g) Användande av högkvalitativa lösenord upprätthålls (t ex krav på minsta längd och komplexitet); och
 - (h) Lösenord lagras och överförs på ett säkert sätt för att undvika att de äventyras.

2.2 Installation och igångkörning – Kundens IT-miljö

- 2.2.1 Åtkomstkontroll.
 - (a) Standard lösenord, tillfälliga lösenord och kryptografiska nycklar ändras i systemen och tjänsterna till unika värden innan användning;
 - (b) Alla behörighetsrättigheter för Hogia skall avaktiveras eller raderas vid överlämnande till kund;
 - (c) Information skall ges till kunden hur högkvalitativa lösenord i form av längd och komplexitet upprätthålls.
- 2.2.2 Hogia ändrar inte säkerhetslösning som har beställts och implementerats av en kund utan att först ha erhållit kundens skriftliga godkännande.

3 ÖVRIG SÄKERHET

3.1 Fjärrsupport

- 3.1.1 Fjärrsupport. Hogia följer kundens valda metod för åtkomst till kundens data på distans. Åtkomst till kunden innebär att Hogia kan komma att ta del av all data inklusive personliga data och information som genereras under fjärrsupporten. Detta som ett led av att kunden och/eller en av kundens utsedda företrädare ger Hogia den åtkomsten. Om ingen sådan metod finns kommer Hogia att rekommendera en metod baserad på säker kommunikation och flerstegsautentisering.
- 3.1.2 Hantering av kundens data. Information som sänds till Hogia för felsökning, eller av annat skäl, kommer att klassas och behandlas som konfidentiell information.

3.2 Fysisk säkerhet – Hogias datacenter

- 3.2.1 Säkra områden skyddas av lämpliga tillträdeskontroller för att säkerställa att endast auktoriserad personal får tillträde.
- 3.2.2 Våra datacenter har redundant kylnings-, elförsörjnings- och kommunikationsinfrastruktur. Det primära datacentret är klassat som ett högtillgänglighetsrum med skyddsklass R 60 D per EN 1047-2:2009 + A1:2013 och ECB-S C10.
- 3.2.3 Tillträdeslistor till säkra områden går igenom och dokumenteras var sjätte månad.
- 3.2.4 Begäran om tillträde till säkra områden dokumenteras formellt och godkänns av lämplig organisation.
- 3.2.5 Fysiskt skydd mot naturkatastrofer, skadliga attacker och olyckor har utarbetats och används.
- 3.2.6 Databärande kraft- och kommunikationsledningar skyddas från avlyssning, störning och skada.
- 3.2.7 Utrustning underhålls korrekt för att säkerställa dess löpande tillgänglighet och integritet.
- 3.2.8 Utrustning som finns på annan plats skyddas utifrån vilka risker det innebär att hantera denna utrustning utanför Hogias lokaler.
- 3.2.9 Utrustning och delar av utrustning som innehåller lagringsmedia verifieras för att säkerställa att all känslig data och licensierad mjukvara har raderats eller skrivits över på ett säkert sätt innan utrustningen kasseras eller återanvänds.