CyberResilient

SÄKERHETSÖVERSIKT

# Säkerhet i CyberResilient

Hur plattformen är byggd, var era uppgifter finns och hur vi arbetar med informationssäkerhet som bolag.

CyberResilient AB (556702-0200) · Version 1.2 · 15 september 2026 · Klassning: Öppen

I CyberResilient samlar ni bedömningssvar, underlag, handlingsplan och riskregister. Tillsammans blir det en detaljerad bild av var er organisation är sårbar. Det här dokumentet beskriver hur vi skyddar den bilden.

Vi beskriver bara det som är på plats i dag. Mer om oss, och dokument ni kan begära, finns på cyberresilient.se/sv/trust.

## 1 Vilka uppgifter hanterar plattformen?

**Ni matar in tre sorters uppgifter.** Uppgifter om organisationen när ni kommer igång, som namn, organisationsnummer, sektor och storlek. Svar på bedömningens frågor, med de anteckningar ni skriver till dem. Och underlag, alltså dokument ni laddar upp för att styrka ett svar.

**Plattformen räknar och skriver.** Svaren poängsätts mot det ramverk ni valt, och en rapport tas fram med observationer och rekommendationer. Rekommendationerna blir mål och åtgärder i handlingsplanen, och riskregistret pekar tillbaka på samma åtgärder.

**Uppgifter lämnar plattformen främst i tre flöden.** Text ur underlag, svar och anteckningar, och en begränsad del av organisationsprofilen, går till vår AI-leverantör (avsnitt 4). Mejl från plattformen skickas via vår e-postleverantör. Faktureringsuppgifter går till vår betalningsleverantör. Vi säljer inte era uppgifter.

## 2 Var finns era uppgifter?

Plattformen drivs hos Hetzner i Falkenstein, Tyskland. Produktionsservern kör applikationen, databasen och bakgrundsjobben. Uppladdade underlag lagras i Hetzner Object Storage i samma region. Plattformens drift, lagring och AI-bearbetning sker inom EU. Leverantörerna för e-post och betalningar kan överföra uppgifter utanför EU, se integritetspolicyn.

| VAD | VAR |
|---|---|
| **Plattform och databas** | Hetzner, Falkenstein, Tyskland |
| **Uppladdade underlag** | Hetzner Object Storage, samma region |
| **AI-bearbetning** | Berget AI, Sverige |

**Exponering.** Produktionsservern har bara port 80 och 443 öppna mot internet. Databasen och cachen publicerar inga portar och går inte att nå utifrån. All trafik till plattformen går över HTTPS.

**Vår egen åtkomst.** Ingen server har publik SSH. Driftåtkomst går över ett krypterat nätverk, med personliga konton och tvåfaktor, och styrs av nätverkets behörighetsregler. All vår personal använder tvåfaktorsinloggning i samtliga interna system.

**Uppbyggnad och säkerhetskopiering.** Servrar, nätverk och brandväggar är beskrivna i kod med Terraform, vilket gör miljön granskningsbar och återskapbar. Alla servrar säkerhetskopieras automatiskt varje dag. Produktion och test körs på egna servrar med egna databaser.

En fullständig lista över underbiträden lämnas på begäran.

## 3 Hur skyddas åtkomsten?

### Inloggning

- Lösenord ska vara minst tolv tecken och klara en styrkekontroll som avvisar vanliga och gissningsbara lösenord. De lagras som Argon2id-hash (64 MiB minne, tre iterationer, fyra trådar).
- Tvåfaktorsinloggning med engångskoder (TOTP, RFC 6238) och tio reservkoder. Hemligheten lagras krypterad, reservkoderna hashas och krypteras.
- Inloggning, registrering, engångskoder, lösenordsåterställning och tvåfaktorssteget är frekvensbegränsade. Efter tio misslyckade försök låses kontot och alla sessioner avslutas.
- Inloggning och registrering svarar likadant oavsett om en adress finns, så att ingen kan ta reda på vilka konton som existerar.
- Varje session har en slumpad nyckel på 256 bitar som bara lagras som hash. Sessioner avslutas efter inaktivitet och efter en längsta livstid, och kan avslutas manuellt.

### Separation mellan organisationer

Vilken organisation ett anrop gäller avgörs mot databasen varje gång, och kräver både aktivt medlemskap och en aktiv roll. Kakan som bär valet är signerad och räknas bara som ett förslag.

När en partner arbetar i er organisation krävs tre saker samtidigt: aktivt medlemskap hos partnern, en aktiv roll där, och att er organisation är kopplad till just den partnern. Partnerns behörighet kan aldrig överstiga dess roll. Att radera organisationen kräver direkt ägarskap och en ny tvåfaktorskontroll, och är helt spärrat för partner.

### Kryptering och underlag

Utöver krypteringen i överföring krypteras känsliga fält i applikationen med AES-256-GCM och versionerade nycklar, så att äldre uppgifter går att läsa även efter ett nyckelbyte. Det gäller tvåfaktorshemligheter och reservkoder, IP-adresser och webbläsaruppgifter i sessioner, säkerhetsloggar, e-posttokens och de bearbetade resultat som rapporten byggs av.

Uppladdade underlag serveras aldrig direkt. Varje åtkomst går genom en kontrollpunkt som prövar behörigheten, loggar åtkomsten och utfärdar en signerad länk som gäller i fem minuter. Filer kontrolleras vid uppladdning: filtyp, storlek och att innehållet är det filen utger sig för att vara.

### Spårbarhet

Varje ändring i riskregistret sparas som en egen händelse med vem, vad och när, i en logg som applikationen aldrig ändrar eller tar bort ur. Åtkomst till underlag loggas, liksom ändringar i en avslutad bedömning, med värdet före och efter.

## 4 Hur använder vi AI?

Plattformen använder språkmodeller för att läsa uppladdade underlag, koppla dem till rätt fråga och formulera rapportens observationer och rekommendationer. Rekommendationerna är vägledande. Plattformen fattar inga automatiserade beslut om enskilda personer.

**En leverantör, i Sverige.** Vi använder en enda AI-leverantör, Berget AI. Alla modeller vi kör har öppna vikter: *Mistral-Small-3.2-24B-Instruct-2506* för analys och rapporter, med *gemma-4-31B-it* som reserv, *multilingual-e5-large* för inbäddningar och *bge-reranker-v2-m3* för att rangordna träffar. Gemma är utvecklad

av Google, men körs som alla våra modeller hos Berget. Inga anrop går till Google eller någon annan amerikansk modelleverantör.

**Vad som skickas.** Text ur era underlag, era svar och era anteckningar till frågorna. Ur organisationsprofilen skickas tre fält: sektor, storleksintervall och den verksamhetsbeskrivning ni själva skrivit. Organisationsnummer och omsättning skickas aldrig.

**Ingen träning.** Vi tränar eller finjusterar inga modeller på kunddata. Prompter och svar med kunddata, och inbäddningar, klassas som konfidentiell information, på samma nivå som kunddata och källkod.

## 5 Hur bygger vi plattformen?

**Granskning.** Vår riktlinje för säker utveckling kräver att en annan utvecklare granskar varje ändring innan den läggs samman, och att OWASP Top 10 följs som lägsta nivå för webb och API.

**Automatiska tester.** Varje ändring körs genom kodstandard, typkontroll, formatkontroll och hela testsviten mot en riktig databas och cache. Testtäckningen mäts mot en satt tröskel.

**Utrullning.** Utrullning sker automatiserat från versionshanteringen, aldrig för hand på en server. En utrullning räknas som lyckad först när applikationen faktiskt svarar.

## 6 Hur styr vi säkerhet som bolag?

Sedan den 20 juli 2026 har vi ett dokumenterat ledningssystem för informationssäkerhet, beslutat av vd. Det består av en policy, tre riktlinjer, två anvisningar, två rutiner och mallar för riskanalys, tillämplighetsförklaring och uppföljning. Strukturen följer ISO/IEC 27001 Annex A, och riskarbetet en metod inspirerad av ISO/IEC 27005.

**Certifiering är målet.** Vi har inte satt något datum och påstår inte att vi är certifierade.

**Klassning och sekretess.** Kunddata, källkod, hemligheter och loggar är konfidentiella som utgångspunkt. Personal och konsulter omfattas av sekretessavtal.

**Vad ledningssystemet förpliktar oss till:**

| OMRÅDE | ÅTAGANDE |
|---|---|
| **Incidenter** | Första åtgärd inom 1 timme för de allvarligaste, inom 4 och 24 timmar för nästa nivåer |
| **Kundavisering** | Enligt avtal, och där avtal saknas inom 24 timmar från bekräftad påverkan |
| **Personuppgiftsincidenter** | Bedömning av anmälan till Integritetsskyddsmyndigheten inom 72 timmar |
| **Leverantörer** | Klassas efter kritikalitet. AI-leverantörer räknas alltid som kritiska och följs upp minst årligen |
| **Uppföljning** | Ledningens genomgång och intern revision av ledningssystemet varje år |

**Incidenthantering.** Roller är utpekade för incidentledning, teknisk hantering och kundkommunikation, med beslutsstöd per incidenttyp. Det gäller också ett särskilt förlopp för om data läcker via en AI-tjänst.

---

**Frågor?** Styrande dokument, säkerhetsformulär eller annat: security@cyberresilient.se · cyberresilient.se/sv/trust
**Hittat en sårbarhet?** Skicka vad ni hittat och hur det går att återskapa till security@cyberresilient.se, som också anges i vår security.txt. Testa inte mot andra kunders uppgifter.