IT- och informationssäkerhetspolicy för BLOOM Institution for social transformation AB

2026-06-11 Version 1

Syfte och omfattning

BLOOM hanterar i förekommande fall komplexa data för att stödja våra kunder och samarbetspartners. Denna policy säkerställer att vi skyddar den information kunden anförtror oss, särskilt i ljuset av EU AI Act och NIS2. Policyn gäller för alla anställda, konsulter och tredje parter som hanterar BLOOMs informationstillgångar. Ansvarig för dess efterlevnad är Robert Nyqvist, tekniskt ansvarig.

Dataskydd och Integritet (GDPR+)

- **Inbyggt dataskydd:** Vid utveckling av digitala verktyg tillämpar vi "Privacy by Design".
- **Känslig data:** Vi hanterar personuppgifter och känslig information med högsta säkerhetsnivå, inklusive kryptering och strikt behörighetskontroll.
- **Datahantering och lagring:** All information ska klassificeras baserat på känslighet. Data ska endast lagras på godkända system och lagringsplatser.
- **Datareducering och radering:** Vi tillämpar en policy för dataminimering och har fastställda rutiner för säker radering av personuppgifter och känslig information när de inte längre är nödvändiga för uppdraget eller lagliga ändamål.
- **Riskhantering och kontinuitet (NIS2):** Vi genomför regelbundna riskbedömningar av kritiska system och processer. Åtgärder för att säkerställa verksamhetskontinuitet, inklusive reservlösningar och återställningsplaner (katastrofåterställning), ska dokumenteras och testas årligen.
- **Leverantörssäkerhet:** Särskild uppmärksamhet ska riktas mot säkerheten hos våra leverantörer av digitala tjänster (molntjänster, analysverktyg). Avtal ska inkludera krav på informationssäkerhet och incidentrapportering i linje med denna policy och NIS2.
- **Incidentrapportering:** Rutinerna för incidenthantering inkluderar en tidsram för rapportering till relevanta myndigheter (t.ex. CSIRT/CERT) vid allvarliga incidenter, i enlighet med NIS2-kraven.

Säker användning av AI och teknik

- **Ansvarsfull AI:** Då vi integrerar AI för datadrivet beslutsfattande ska alla modeller vara transparenta, rättvisa och fria från bias som kan missgynna utsatta grupper.
- **Verifiering:** Vi genomför regelbundna kontroller av våra analysverktyg för att säkerställa att tekniken stödjer, snarare än ersätter, mänsklig expertis.
- **Dokumentation och spårbarhet (EU AI Act):** För alla AI-modeller som används för datadrivet beslutsfattande ska fullständig dokumentation av datasätt, designval och prestandatester upprätthållas. Detta inkluderar loggning av beslut för att säkerställa fullständig spårbarhet och förklarlighet.

- **Övervakning och revision:** AI-system ska övervakas kontinuerligt för att upptäcka prestandaförsämring och driftavvikelser (drifting) som kan leda till orättvisa eller felaktiga resultat.

Operativ säkerhet

- **Behörighet:** Vi tillämpar principen om "minsta möjliga behörighet". Endast de som behöver data för att utföra sitt uppdrag har tillgång till den.
- **Incidenthantering:** Vi har fastställda rutiner för att snabbt identifiera, rapportera och åtgärda eventuella informationssäkerhetsincidenter.
- **Säkerhetsutbildning:** Alla medarbetare ska genomgå obligatorisk och regelbunden utbildning i informationssäkerhet, dataskydd och ansvarsfull AI-användning.
- **Lösenordspolicy:** Starka och unika lösenord är obligatoriska. Multi-faktorautentisering (MFA) ska användas för åtkomst till kritiska system.

Fysisk och nätverkssäkerhet

- **Fysisk säkerhet:** Åtkomst till servrar, nätverksutrustning och andra fysiska informationsbärande enheter ska begränsas till auktoriserad personal.
- **Nätverkssegmentering och skydd:** Nätverk ska segmenteras för att isolera känsliga tillgångar. Brandväggar och intrångsdetekteringssystem ska användas för att skydda mot obehörig åtkomst och skadlig programvara.
- **Patch- och sårbarhetshantering:** Vi har rutiner för regelbunden uppdatering av all mjukvara och hårdvara för att åtgärda kända sårbarheter.