Säkerhetsdeklaration för

Detta dokument utgör en övergripande beskrivning av vilka säkerhetsåtgärder som ingår i leveransen. Svara på frågorna under respektive rubrik. Östhammars kommun använder denna säkerhetsdeklaration för att vid upphandling bedöma om anbudet kan anses uppfylla ska-kraven på informationssäkerhet. Säkerhetsdeklarationen ska vara tydlig så att den kan användas för utvärdering utan hänvisning till annan dokumentation annat än där det uttryckligen efterfrågas. Uppgifterna som redovisas nedan kan komma att kontrolleras och behöva uppdateras under avtalsperioden av båda parter.

1. Information om leverantören

Leverantörens namn:

Kontaktuppgifter/uppgiftslämnare:

E-post:

Telefonnummer:

2. Underleverantörer

2.1 Hur många underleverantörer använder ni er av?

2.2 Görs periodiska kontroller avseende informationssäkerhet på underleverantörer ni använder er av?

3. Informationshantering

3.1 Informationstillgångar

Beskriv vilka informationstillgångar leveransen är beroende av för att säkerställa en lyckad och effektiv leverans. Informationstillgångar kan vara av fysisk eller logisk karaktär, eller bådadera.

3.2 Artificiell intelligens

Om leveransen inkluderar någon form av artificiell intelligens, beskriv i så fall vilken data som används och hur denna data behandlas.

4. Arkitektur

4.1 Datacenter

Är datacenter geografiskt inom EU/EES?

4.2 Utvecklings – och testmiljö

Hur separeras produktionsdata och testdata?

4.3 Integrationer

Beskriv systemets integrationer och/eller beroenden till andra system.

4.4 Nätverk och kommunikation

Hur skyddas all kommunikation till och från systemet mot obehörig åtkomst och förvanskning?

4.5 Datahantering och lagring

Hur separeras olika kunders miljöer?

4.6 Fysisk säkerhet

Vilken skyddsnivå uppfyller era datahallar? (”datahall” enligt MSB ”Vägledning för fysisk informationssäkerhet i it-utrymmen)

4.7 Loggning och spårbarhet

Beskriv hur loggning genomförs och hur logginnehåll övervakas.

5. Åtkomsthantering

5.1 Åtkomstkontroll

Beskriv kortfattat vilka dokumenterade regler och rutiner som finns för fysisk respektive logisk åtkomst till informationstillgångar.

Redogör för hur åtkomsträttigheter granskas, inklusive hur ofta granskning sker och vem som ansvarar för den.

5.2 Autentisering och behörigheter

Beskriv principer för autentisering och behörigheter av användare.

Beskriv principer för lösenord.

Beskriv stöd för flerfaktorsautentisering/MFA

5.3 Tredjeparts åtkomst

Beskriv hur behov av åtkomst från tredje part (underleverantör) hanteras.

6. Systemutvecklingsprocess

6.1 Utvecklingsprocess

Beskriv hur informationssäkerheten hanteras under utvecklingsprocessen.

6.2 Ändringshantering

Beskriv processen för ändringshantering.

Beskriv hur ändringar riskbedöms och beslutas samt dokumenteras.

7. Drift av systemet

7.1 Drift

Beskriv rutiner för uppdateringar.

Beskriv vilka tekniska och organisatoriska åtgärder som finns för att skydda informationstillgångarna mot elavbrott och störningar.

7.2 Incidenthantering

Hur många säkerhetsrelaterade incidenter har rapporterats de senaste 2 åren?

Hur ser er kommunikationsprocess ut för incidenter som påverkar/riskerar att påverka informationssäkerheten?

7.3 Katastrofhantering och återställning

Hur ofta tas backup?

Hur förvaras backup och är åtskild från produktionsmiljön?

8. Regelefterlevnad och systematik

8.1 Ledningssystem och riskhantering

Beskriv hur ni arbetar systematiskt och riskbaserat med informationssäkerhet. Vilka standarder jobbar ni enligt?

Bifoga certifikat på ISO27001 om sådant finns.

Hur ofta genomför ni riskutvärderingar avseende säkerhet?

Vilken rapportering och uppföljning genomför ni till er själva avseende informationssäkerhet?

8.2 Granskningar

Har ni gjort någon extern revision på informationssäkerheten senaste 2 åren?

Har ni gjort någon granskning av teknisk efterlevnad (t.ex. penetrationstester och sårbarhetsgranskningar) senaste 2 åren? Om Ja, vilken?