

TA-01-B

Vedlegg B - Soneinndeling / Sikkerhet

Nytt fagsystem

GARANTIKASSEN FOR FISKERE

B.1. Formål	3
B.2. Soneinndeling	3
B.3. API-lag	3
B.4. Portal og dokumentinnsending	4
B.4.1 Rolle og avgrensning	4
B.4.2 Autentisering.....	4
B.4.3 Autorisasjon og representasjon	4
B.4.4 Opplasting og håndtering av vedlegg	5
B.4.5 Beskyttelse mot misbruk.....	5
B.5. Database	5
B.6. Datarevisjon og sporbarhet.....	6
B.7. Drift og administrativ tilgang	6
B.8. Informasjonssikkerhetskrav	6
B.8.1 Logging	7
B.8.2 Sårbarhetshåndtering	7
B.8.3 Hendelseshåndtering	7
B.9. Verifikasjon og akseptanse	7
B.10. Trusselmodell og sikkerhetsforutsetninger	8
B.10.1 Formål	8
B.10.2 Beskyttelsesverdier.....	8
B.10.3 Trusselaktører	8
B.10.4 Angrepsflater.....	8
B.10.5 Typiske angrepsscenarier	8
B.10.6 Sikkerhetsforutsetninger	10
B.11. Krav–Risiko–Kontroll-matrise	10
B.12. Diagram for soneinndeling	10
B.13. Bruk av AI i utvikling.....	11
B.13.1 Tillatt bruk	11
B.13.2 Leverandøransvar	11
B.13.3 Forståelighet og vedlikeholdbarhet	12
B.13.4 Beskyttelse av personopplysninger og annen beskyttelsesverdig informasjon	12

B.13.5 Styring av AI-verktøy og leverandørstyring	12
B.13.6 Immaterielle rettigheter og tredjepartskode	12
B.13.7 Kvalitetssikring og menneskelig kontroll	13
B.13.8 Sporbarhet i utviklingsprosessen	13
B.13.9 Sikker utviklingspraksis	13
B.13.10 Dokumentasjon ved forespørsel	13

B.1. Formål

Dette kapittelet beskriver formålet med sikkerhetsarkitekturen for løsningen, inkludert soneinndeling, API-lag og overordnede sikkerhetsmekanismer. Sikkerhetsarkitekturen skal sikre at sensitive data beskyttes, at tilganger er kontrollert, og at systemet er robust mot både feil og angrep.

Manglende eller svak implementering av disse prinsippene vil øke risikoen for datalekkasjer, uautorisert tilgang og svekket tillit til løsningen.

B.1.1 Løsningen skal sikre tydelig separasjon mellom ekstern og intern sone.

B.1.2 Løsningen skal etablere kontrollert integrasjon mellom portal og interne systemer.

B.1.3 Løsningen skal beskytte sensitive data mot uautorisert tilgang.

B.1.4 Løsningen skal sikre sporbarhet og revisjonsmulighet.

B.1.5 Løsningen skal redusere angrepsflate.

B.1.6 Løsningen skal tydeliggjøre ansvarsdeling mellom presentasjonslag og beslutningslag.

B.2. Soneinndeling

Overordnet arkitektur og komponentstruktur er beskrevet i TA-01-A og TA-01-C. Dette kapittelet beskriver sikkerhetsmessige krav knyttet til denne arkitekturen, med fokus på soneinndeling og kontroll av trafikk mellom soner.

Feil soneinndeling eller manglende kontroll mellom soner vil kunne gi direkte tilgang til interne systemer og data.

B.2.1 Løsningen skal bestå av en ekstern sone for portal og en intern sone for fagsystem og database.

B.2.2 Intern database skal ikke være direkte tilgjengelig fra ekstern sone.

B.2.3 All kommunikasjon mellom soner skal være eksplisitt definert og dokumentert.

B.2.4 All kommunikasjon mellom soner skal være kryptert.

B.2.5 Kun definerte API-endepunkter skal være tilgjengelige mellom soner.

B.2.6 Det skal dokumenteres hvilke komponenter som har nettverkstilgang til hverandre.

B.2.7 All annen trafikk enn eksplisitt tillatt kommunikasjon mellom soner skal blokkeres.

B.3. API-lag

Dette kapittelet beskriver API-lagets rolle som kontrollpunkt mellom ekstern og intern sone. API-laget er en kritisk sikkerhetsbarriere og skal håndheve autentisering, autorisasjon og validering.

Feil i API-laget vil kunne gi uautorisert tilgang til interne systemer eller feil behandling av data.

- B.3.1 API-laget skal separere presentasjonslag fra forretningslogikk.
- B.3.2 All kommunikasjon mellom portal og intern API skal være kryptert.
- B.3.3 System-til-system kommunikasjon skal autentiseres med sterk tjenesteautentisering.
- B.3.4 Intern API skal validere systemidentitet og brukeridentitet for alle forespørsler.
- B.3.5 Portalen skal kun ha begrensede rettigheter til innsending og vedlegg.
- B.3.6 Portalen skal ikke ha generell lesetilgang til interne saksdata.
- B.3.7 Alle API-kall skal logges med identitet og korrelasjonsinformasjon.
- B.3.8 Integrasjon mot arkivsystem skal være kontrollert og dokumentert.

B.4. Portal og dokumentinnsending

Dette kapittelet beskriver portalens rolle som innsamlingskanal og hvordan dokumenter håndteres. Portalen er eksponert mot eksterne brukere og utgjør en viktig angrepsflate. Feil håndtering av input eller vedlegg kan føre til kompromittering av systemet eller feil i datagrunnlaget.

B.4.1 Rolle og avgrensning

Portalen skal kun samle inn data og skal ikke inneholde forretningslogikk. All validering av regler skal skje i fagsystemet.

- B.4.1.1 Portalen skal fungere som presentasjons- og innsamlingslag.
- B.4.1.2 Portalen skal ikke inneholde beslutningslogikk.
- B.4.1.3 All forretningsvalidering skal utføres i fagsystemet.

B.4.2 Autentisering

Feil autentisering kan gi uautorisert tilgang til systemet.

- B.4.2.1 Løsningen skal støtte autentisering via nasjonal identitetsinfrastruktur.
- B.4.2.2 Token skal valideres med hensyn til signatur, gyldighet og opprinnelse.
- B.4.2.3 Ugyldig token skal avvises.
- B.4.2.4 Brukeridentitet skal lagres som metadata.

B.4.3 Autorisasjon og representasjon

Feil autorisasjon kan gi tilgang til feil data eller funksjoner.

- B.4.3.1 Representasjonsrett skal verifiseres.
- B.4.3.2 Portalen skal ikke implementere kvalifikasjonsregler.
- B.4.3.3 Berettigelsesvurdering skal utføres i fagsystemet.
- B.4.3.4 Avvisning basert på regler skal skje i fagsystemet.

B.4.4 Opplasting og håndtering av vedlegg

Vedlegg er en kjent angrepsflate og må behandles strengt.

B.4.4.1 Filtype skal valideres.

B.4.4.2 Ikke tillatte filer skal avvises.

B.4.4.3 Filstørrelse skal være konfigurert.

B.4.4.4 Antall vedlegg skal være konfigurert.

B.4.4.5 Vedlegg skal skadevarekannet før videre behandling.

B.4.4.6 Vedlegg som feiler kontroll skal avvises og logges.

B.4.4.7 Vedlegg skal lagres sikkert.

B.4.4.8 Tilgang til vedlegg skal logges.

B.4.5 Beskyttelse mot misbruk

Dette kapittelet beskriver tiltak for å beskytte løsningen mot misbruk og angrep.

B.4.5.1 Løsningen skal implementere rate limiting.

B.4.5.2 Løsningen skal kunne blokkere unormal trafikk.

B.4.5.3 All input skal valideres.

B.4.5.4 Feilmeldinger skal ikke eksponere interne detaljer.

B.5. Database

Dette kapittelet beskriver sikker håndtering av databasen. Databasen inneholder sensitive data og er et kritisk mål for angrep.

Feil tilgangskontroll eller manglende sikring vil kunne føre til datalekkasjer eller datamanipulasjon.

B.5.1 Databasetilgang skal være rollebasert og begrenset.

B.5.2 Applikasjonen skal ikke bruke administratorrettigheter.

B.5.3 Sensitive data skal beskyttes gjennom tilgangskontroll, kryptering og logging.

B.5.4 Testmiljø skal ikke inneholde reelle data uten særskilt sikring.

B.5.5 Backup skal sikres.

B.5.6 Gjenoppretting fra backup skal testes minimum én gang per år og etter vesentlige endringer i backup eller gjenopprettingsløsningen. Testen skal verifisere at backupen kan gjenopprettes til en fungerende løsning, og at gjenopprettede data kan benyttes som forutsatt. Testen skal dokumenteres og eventuelle avvik skal følges opp.

B.5.7 Direkte manuell endring av forretningsdata i produksjonsdatabasen skal som hovedregel ikke benyttes.

B.5.8 Dersom direkte endring av produksjonsdata er nødvendig som del av kontrollert feilretting eller annen særskilt operasjon, skal endringen være autorisert, dokumentert og fullt sporbar.

B.5.9 Direkte endringer i produksjonsdata skal omfattes av kravene til audit i TA-01-D, herunder identitet på aktør, tidspunkt, berørte data og verdier før og etter endringen.

B.6. Datarevisjon og sporbarhet

Dette kapittelet beskriver krav til logging av endringer.

Uten Datarevisjon vil det ikke være mulig å etterprøve hva som har skjedd i systemet eller avdekke feil og misbruk.

B.6.1 Alle endringer skal logges.

B.6.2 Logger skal beskyttes mot uautorisert tilgang og endring.

B.6.3 Endring av logging skal logges.

B.6.4 Konfigurasjonsendringer skal være sporbare.

B.7. Drift og administrativ tilgang

Dette kapittelet beskriver hvordan administrativ tilgang skal håndteres.

Feil håndtering av administratorrettigheter er en av de største sikkerhetsrisikoene i systemet.

B.7.1 Administrativ tilgang skal være personlig.

B.7.2 Administrativ tilgang skal kreve flerfaktorausentisering.

B.7.3 Break-glass tilgang skal kontrolleres og logges.

B.7.4 Fjernadministrasjon skal være sikker.

B.7.5 Privilegerte tilganger skal begrenses til personer og systemidentiteter med dokumentert behov og skal kunne identifiseres og etterprøves.

B.7.6 Tildeling, endring og opphør av privilegerte tilganger skal være sporbar.

B.8. Informasjonssikkerhetskrav

Dette kapittelet samler overordnede sikkerhetskrav knyttet til drift og vedlikehold av løsningen.

Manglende etterlevelse vil kunne føre til kjente sårbarheter, dårlig hendelseshåndtering og økt risiko for sikkerhetsbrudd.

B.8.1 Logging

Dette delkapittelet beskriver krav til sikkerhetslogging og overvåkning. Formålet er å sikre at relevante sikkerhetshendelser kan oppdages, analyseres og følges opp på en kontrollert måte.

B.8.1.1 Sikkerhetslogger skal dekke kritiske hendelser.

B.8.1.2 Logger skal ikke inneholde sensitiv informasjon.

B.8.1.3 Logger skal beskyttes.

B.8.1.4 Løsningen skal støtte sentral logganalyse og kunne integreres med eksterne løsninger for sikkerhetsanalyse gjennom standardiserte mekanismer for overføring av logger og sikkerhetshendelser.

B.8.2 Sårbarhetshåndtering

Dette delkapittelet beskriver krav til identifisering og håndtering av sikkerhetssårbarheter. Formålet er å redusere risikoen for at kjente sårbarheter kan utnyttes og sikre at nødvendige sikkerhetsoppdateringer gjennomføres kontrollert.

B.8.2.1 Programvare skal holdes oppdatert.

B.8.2.2 Sårbarhetsskanning skal gjennomføres regelmessig.

B.8.2.3 Kritiske sårbarheter skal håndteres innen definerte tidsfrister.

B.8.3 Hendelseshåndtering

Dette delkapittelet beskriver krav til håndtering av sikkerhetshendelser. Formålet er å sikre at hendelser kan identifiseres, registreres, rapporteres og følges opp på en strukturert og sporbar måte.

B.8.3.1 Prosess for hendelseshåndtering skal etableres.

B.8.3.2 Hendelser skal kunne identifiseres, logges og rapporteres.

B.9. Verifikasjon og akseptanse

Dette kapittelet beskriver hvordan kravene skal verifiseres.

Uten verifikasjon er kravene ikke etterprøvbare.

B.9.1 Som del av kontraktsgjennomføringen skal leverandøren etablere og vedlikeholde dokumentasjon som viser hvordan relevante sikkerhetskrav i dette vedlegget er ivarettatt i løsningen.

B.9.2 GFF skal kunne gjennomføre tester og revisjoner.

B.9.3 Manglende oppfyllelse anses som vesentlig avvik.

B.10. Trusselmodell og sikkerhetsforutsetninger

Dette kapittelet beskriver trusselbildet og hvilke forutsetninger som ligger til grunn.

Dette gir kontekst for sikkerhetskravene og hvorfor de er nødvendige.

B.10.1 Formål

Dette vedlegget beskriver antatte trusselaktører, beskyttelsesverdier, angrepsflater og typiske angrepsscenarioer, samt sikkerhetsforutsetninger lagt til grunn i spesifikasjonen.

B.10.2 Beskyttelsesverdier

- Personopplysninger (inkludert fødselsnummer)
- Kontonummer og betalingsinformasjon
- Vedtak og saksbehandlingsdata
- Søknadsvedlegg
- Tilgangsrettigheter og rolleinformasjon
- Systemlogger
- Integritet i tilskudds- og refusjonsordninger

B.10.3 Trusselaktører

Følgende trusselaktører legges til grunn:

- Ekstern angriper: økonomisk motivert angrep, identitetstyveri, tjenestenekt
- Intern bruker med for høye rettigheter: uaktsomhet eller misbruk
- Kompromittert ekstern komponent: utnyttelse av sårbarhet i portal eller skadevare via vedlegg
- Leverandørrelatert risiko: feilkonfigurasjon, utilstrekkelig sikkerhetsoppfølging

B.10.4 Angrepsflater

- Ekstern portal (skjema, autentisering, vedlegg)
- API mellom soner
- Autentiseringstoken og sesjonshåndtering
- Database og datatilgang
- Administrative grensesnitt og driftstilganger
- Logging og sikkerhetskopier

B.10.5 Typiske angrepsscenarioer

Scenario 1 – Manipulert innsending

Angriper forsøker å sende manipulert søknad via portalen (for eksempel endret payload eller ugyldige felt).

Kontroller:

- Input-validering
- Autorisasjon i fagsystem
- Sikkerhetslogging og korrelasjon

Scenario 2 – Ondsinnet vedlegg

Angriper laster opp skadelig vedlegg (for eksempel PDF eller arkivfil) for å kompromittere interne arbeidsstasjoner eller systemer.

Kontroller:

- Filtypekontroll (MIME-type + filsignatur)
- Skadevareskanning før intern tilgjengelighet
- Isolert lagring og logg av nedlastinger/visninger

Scenario 3 – Misbruk av systemidentitet

Kompromittert portal eller integrasjonskomponent forsøker å kalle interne API-er utover tillatte operasjoner.

Kontroller:

- Gjensidig autentisering (mTLS) og unik tjenesteidentitet
- Minste privilegium på API-tilganger
- Logging av systemidentitet og avvik

Scenario 4 – Intern misbruk

Intern bruker forsøker å endre vedtak eller data uten autorisasjon.

Kontroller:

- Rollebasert tilgangsstyring
- To-rolle-prinsipp for kritiske handlinger der aktuelt
- Datarevisjon-logg for endringer

Scenario 5 – Tjenestenekt (DoS)

Automatisert trafikk eller store opplaster forsøker å gjøre portalen utilgjengelig.

Kontroller:

- Rate limiting
- Ressursbegrensning per bruker/IP
- Trafikkfiltrering og overvåking

B.10.6 Sikkerhetsforutsetninger

- Autentisering via nasjonal identitetsinfrastruktur anses som pålitelig når token-validering er korrekt implementert.
- Intern sone er ikke direkte eksponert mot internett.
- Database og logglagring driftes i kontrollert miljø med tilgangsstyring.
- Sikkerhetskrav i dette vedlegget oppfylles og dokumenteres av leverandør.

B.11 Krav–Risiko–Kontroll-matrise

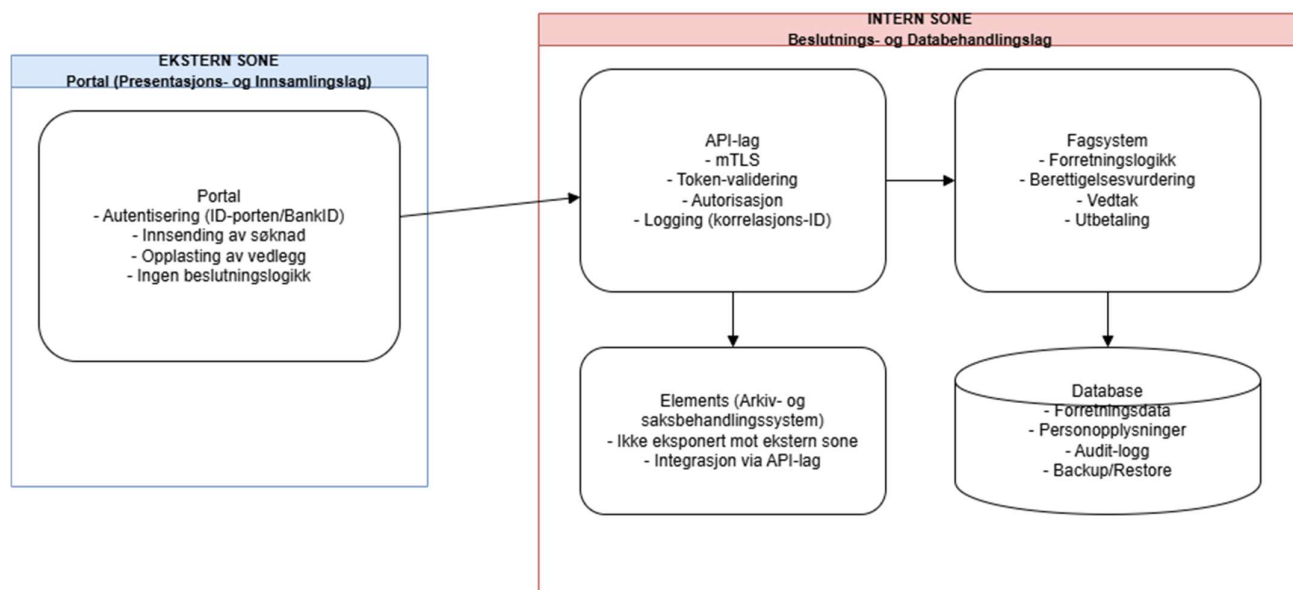
Dette kapittelet kobler risikoer til konkrete kontroller. Det gir oversikt og gjør det mulig å etterprøve at kravene dekker relevante trusler.

Matrisen kobler trusler og risikoer til kontroller og kravreferanser i dette dokumentet.

Risiko	Konsekvens	Kontroll
Uautorisert tilgang via portal	Datainnbrudd / datalekkasjer	Sterk autentisering og token-validering
Token-misbruk (feil issuer/audience)	Tilgang til feil system	Validering av issuer/audience/signatur/utløp
Skadelig vedlegg	Kompromittering av interne brukere/systemer	Filtypekontroll + skadevareskanning + isolert lagring
Misbruk av systemidentitet	Uautorisert tilgang til intern API	mTLS og minste privilegium
For høye rettigheter internt	Uautorisert endring/vedtak	Rollebasert tilgang og logging
Datamanipulasjon	Feil utbetaling / feil vedtak	Datarevisjon-logg for endringer
Loggmanipulasjon	Manglende sporbarhet	Beskyttet logglagring og tilgangskontroll
Tjenestenekt	Utilgjengelig portal	Rate limiting og trafikktiltak
Administrator-misbruk	Datatap eller endringsforfalskning	Break-glass-kontroll + MFA
Manglende patching	Kjente sårbarheter utnyttet	Sårbarhetshåndtering og oppdateringsrutiner
Manglende hendelseshåndtering	Sen oppdagelse og større skade	Dokumentert hendelseshåndtering

B.12 Diagram for soneinndeling

Dette kapittelet skal visualisere soneinndelingen og støtte forståelse av arkitekturen.



B.13 Bruk av AI i utvikling

Leverandøren kan benytte AI-baserte verktøy som støtte i utviklingsarbeidet. Bruk av slike verktøy skal skje på en kontrollert måte og skal ikke redusere kravene til kvalitet, sikkerhet, personvern, sporbarhet, rettigheter eller vedlikeholdbarhet i den leverte løsningen.

B.13.1 Tillatt bruk

Leverandøren kan benytte AI-baserte verktøy i utviklingsprosessen, herunder til støtte for programmering, testing, dokumentasjon, analyse og kvalitetssikring.

Bruk av AI-baserte verktøy fritar ikke leverandøren fra noen av kravene eller forpliktelsene som følger av konkurransegrunnlaget, kontrakten eller gjeldende regelverk.

B.13.2 Leverandøransvar

Leverandøren skal ha fullt ansvar for all kode, dokumentasjon, konfigurasjon og øvrige leveranser, uavhengig av om hele eller deler av innholdet er produsert eller foreslått ved bruk av AI-baserte verktøy.

AI-generert eller AI-assistert innhold skal være underlagt samme krav til kvalitetssikring, testing, sikkerhetskontroll og godkjenning som øvrig utviklet innhold.

B.13.3 Forståelighet og vedlikeholdbarhet

Leverert kode, konfigurasjon og dokumentasjon skal være forståelig, dokumentert og vedlikeholdbar uten avhengighet av det AI-verktøyet som er benyttet under utviklingen.

Det skal ikke være nødvendig å ha tilgang til leverandørens AI-verktøy, tidligere AI-samtaler eller prompt-historikk for å kunne forstå, drifte, vedlikeholde eller videreutvikle løsningen.

B.13.4 Beskyttelse av personopplysninger og annen beskyttelsesverdig informasjon

Leverandøren skal sikre at personopplysninger, taushetsbelagte opplysninger, autentiseringsopplysninger, sikkerhetsinformasjon, produksjonsdata, kildekode med særskilt beskyttelsesbehov eller annen beskyttelsesverdig informasjon ikke overføres til AI-baserte tjenester uten at slik behandling er uttrykkelig godkjent av oppdragsgiver og gjennomført i samsvar med gjeldende regelverk og avtalte sikkerhetskrav.

Produksjonsdata skal ikke benyttes som input til AI-baserte utviklingsverktøy med mindre dette er særskilt avtalt med oppdragsgiver.

B.13.5 Styring av AI-verktøy og leverandørstyring

Leverandøren skal ha kontroll med hvilke AI-baserte verktøy som benyttes i utviklingsarbeidet.

Bruk av AI-baserte utviklingsverktøy skal inngå i leverandørens dokumenterte sikkerhets- og personvernstyring. Dokumentasjonen skal kunne fremlegges for GFF under kontraktgjennomføringen.

Der tredjeparts AI-tjenester behandler informasjon på vegne av leverandøren, skal leverandøren sikre nødvendig kontroll med tjenesteleverandører og eventuelle underleverandører.

B.13.6 Immaterielle rettigheter og tredjepartskode

Leverandøren skal sikre at kode, dokumentasjon og annet materiale som er generert eller bearbeidet ved bruk av AI-baserte verktøy, kan benyttes av oppdragsgiver i samsvar med kontrakten.

Leverandøren skal kontrollere AI-generert eller AI-assistert innhold for mulig brudd på tredjeparts immaterielle rettigheter, lisensvilkår eller andre bruksbegrensninger.

Bruk av AI-baserte verktøy skal ikke medføre at oppdragsgiver får svakere rettigheter til den leverte løsningen enn det som følger av kontrakten.

B.13.7 Kvalitetssikring og menneskelig kontroll

AI-generert eller AI-assistert kode skal kvalitetssikres av kvalifisert personell før den inngår i løsningen.

Leverandøren skal sikre at kritisk funksjonalitet, herunder funksjoner knyttet til tilgangsstyring, behandling av personopplysninger, vedtak, beregning, økonomiske disposisjoner og integrasjoner, er gjenstand for ordinær faglig gjennomgang, testing og sikkerhetskontroll.

AI-generert innhold skal ikke aksepteres som korrekt utelukkende fordi det er produsert av et AI-verktøy.

B.13.8 Sporbarhet i utviklingsprosessen

Bruk av AI-baserte utviklingsverktøy skal ikke redusere sporbarheten i utviklingsprosessen.

Kode og andre relevante endringer skal håndteres gjennom leverandørens ordinære mekanismer for versjonskontroll, kodegjennomgang, testing, godkjenning og releasehåndtering.

Oppdragsgiver skal ikke være avhengig av tilgang til AI-verktøyets prompt- eller samtalehistorikk for å kunne etterprøve hvordan en endring er utviklet, kontrollert og godkjent.

B.13.9 Sikker utviklingspraksis

Bruk av AI-baserte verktøy skal inngå i leverandørens etablerte prosesser for sikker programvareutvikling.

Leverandøren skal sikre at AI-generert eller AI-assistert kode vurderes for sikkerhetssvakheter, feil, uønskede avhengigheter og andre forhold som kan påvirke løsningens kvalitet eller sikkerhet.

Bruk av AI-baserte utviklingsverktøy skal ikke redusere kravene til sikkerhetsgjennomgang, testing eller sårbarhetshåndtering som gjelder for løsningen for øvrig.

B.13.10 Dokumentasjon ved forespørsel

GFF skal under kontraktsgjennomføringen kunne be om dokumentasjon av leverandørens overordnede prinsipper og kontrollmekanismer for bruk av AI-baserte verktøy i utviklingsprosessen, herunder hvordan leverandøren ivaretar informasjonssikkerhet, personvern, kvalitetssikring og immaterielle rettigheter.

Kravet innebærer ikke at leverandøren skal utlevere individuelle AI-prompter, samtalehistorikk eller annen utviklerintern arbeidsinformasjon, med mindre dette følger av særskilt avtale eller er nødvendig for å undersøke et konkret sikkerhets- eller kontraktsavvik.