

Vedlegg A

Kravspesifikasjon:

Implementering av ISO 27001 for Bioforsk, del 2

Beskrivelse av leveransen:

Prosjekt lederstøtte for gjennomføring og implementering av ISMS med utgangspunkt i ISO 27001:2005 og i henhold til utarbeidet GAP analyse og Business case.

Som et ledd i Bioforsk sitt sikkerhetsarbeid ønsker Bioforsk med prosjektlederstøtte å få implementert en ISMS med utgangspunkt i standard ISO/IEC-27001:2005 «Information Security Management System - Requirements» og utarbeidet GAP-analys og SOA som ble utarbeidet av konsulenter høsten 2011 som var del 1 i denne prosessen.

Prosjektlederstøtten kan bistå ved en eventuell full sertifisering av Bioforsk etter nevnte standard.

Implementering av styringssystemet er en prosess som vil måtte strekke seg over en lengre tidsperiode. Det skal gjennomføres risikovurderinger og etableres planer for risikohåndtering innenfor alle områder som er omfattet av styringssystemet. Dette krever ofte kompetansehevende tiltak og bistand ved første gjennomføring. Når styringssystemet er etablert skal det fungere som en kontinuerlig prosess, noe som krever at sentrale nøkkelroller følger opp etterlevelsen.

Bioforsk har både internasjonale og nasjonale forskingsprosjekter samt at vi er lokalisert i 14 bygg på 13 lokaliteter i landet, hvorav 220 av 470 er lokalisert på Ås.

Bioforsk har også flere laboratorier der 2 av disse er ISO 9000 sertifisert. Et lokalisert på Ås og et lokalisert på Svanhovd i Pasvik.

IKT infrastruktur og servere driftes av Itas Eierdrift som Bioforsk er medeier i og som Bioforsk har et nært og godt samarbeid med. Itas Eierdrift er lokalisert på Ås.

Det skal utarbeides globale dokumenter som skal dekke de viktigste områder når det gjelder Bioforsk sin informasjonssikkerhet, men det skal ikke være uttømmende. Alle dokumenter skal være skrevet på norsk og følge formkrav i ISO/IEC-27001:2005.

Utarbeidet GAP-analysen har avdekket at Bioforsk vil ha en ISMS som inneholder 122 kontroller av ISO 27001 vedlegg A sine 133 kontroller. Det er virksomhetens egne behov som skal danne grunnlag for hvilke kontroller som er hensiktsmessig å ta med.

Arbeidet skal gjøres i nært samarbeid med Bioforsk sine ansatte og spesielt Bioforsk sin IKT- og sikkerhetsleder og Informasjons og kommunikasjonsdirektøren som er prosjekteier.

Bioforsk ser for seg arbeidsfordelingen etter følgende forslag til prosjektorganisering, og hvilke ressurser som bør bistå i prosjektgjennomføringen. Omfanget av den enkelte ressurs sitt bidrag må avstemmes opp mot besluttet tidsplan for prosjektgjennomføringen og konkretiseringen av innholdet i de identifiserte aktivitetene. Bioforsk er åpen for andre forslag til ressursbruk, men må beslutte prosjektorganiseringen ved prosjektetablering.

Prosjekteier	Administrerende direktør	ISMS etableres for at virksomheten ved adm.dir. skal få bedre styring og kontroll med informasjonssikkerheten. Dette er han pålagt gjennom tildelingsbrev, i tillegg til at det er stilt som krav personopplysningsloven og økonomireglementet.
Prosjektleder	Sikkerhetsleder	ISMS er sikkerhetsleder sitt viktigste verktøy for å kunne stille sikkerhetskrav inn i virksomheten og for å kunne følge opp (kontrollere) sikkerhetstilstanden. Vedkommende er essensiell for at ISMS skal fungere i en ellers hektisk hverdag.
Prosjektlederstøtte	Intern eller ekstern ressurs	Ettersom sikkerhetsleder ikke selv har kapasitet til å drive prosjektet på fulltid vil det være fornuftig å benytte prosjektlederstøtte/ eventuelt leie inn en ekstern prosjektleder. I sum bør prosjektleder + prosjektlederstøtte tilsvare en stilling på 80 - 100 %.
Prosjektdeltaker	Representant for operative prosessledere	Bioforsk må vurdere sikkerhetsbehovet for all informasjon som samles, produseres, behandles, utveksles og slettes.
Prosjektdeltaker	Representant fra IT	IKT er vesentlig for brorparten av all informasjonsbehandling i Bioforsk. Prosjektet bør bemannes med en representant for de IKT-tjenester som Bioforsk selv håndterer.
Prosjektdeltaker	Representant fra HR	HR spiller en viktig rolle før,

		under og ved avslutning av ansettelse. I tillegg vil vedkommende trolig være involvert i opplæring og bevisstgjøring.
Prosjektdeltaker	Representant fra fysisk sikring av kontormasse	Her inngår alt fra adgangskontroll og soneinndeling til sikring av serverrom. Kanskje også internpost, håndtering av avfall (makulering, etc), og bruk av brannskap, etc.
Prosjektdeltaker	Eventuelt representant fra enhet for virksomhetsstyring	Styringssystemet bør innkorporeres i allerede eksisterende system for virksomhetsstyring.
Prosjektdeltaker	Eventuelt representant fra juridisk enhet	Prosjektet bør ha tilgang til juridisk kompetanse ved behov.

Utgangspunktet er at Bioforsk ønsker å ha en ISMS på plass innen medio 2013 og en eventuell full sertifisering i henhold til standard innen utgangen av 2013.

Oppstart av arbeidet kan skje i løpe av første tertial 2012.

Det stilles krav til at tilbyder stiller med kvalifisert personell med sertifiseringene ISO 27001 Lead Implementer og ISO 27001 Lead Auditor. Samt at personell som tilbys behersker både muntlig og skriftlig godt norsk siden arbeidsspråket i prosessen vil bli på norsk.

Mot underskriving av vedlegg B "konfidensialitetserklæring" og innsending av denne til arkiv@bioforsk.no vil oppdragssøker motta SOA og GAP analysen for Bioforsk som er utarbeidet i prosjektets del1 inne 2 arbeidsdager. Fristen for å be om denne er satt til 13. mars.

Tilbudet skal være basert på oppdragsforståelse og hvordan tilbyder ser for seg prosjektet løst med en fremdriftsplan med antatt timeforbruk, timepris og ressurser tilbyder kan tilby. (Se for øvrig pkt 3.1 Tilbudets struktur og innhold i konkurransegrunnlaget)

Tilbudet skal ende opp i en ISMS for Bioforsk som kan danne grunnlag og være utfyllende nok for sertifisering av Bioforsk etter standard ISO 27001:2005.

Vedlegg B:

Konfidensialetserklæring for tilsending av SOA og GAP