Retur Kvalitetshåndbok

Kravspesifikasjon ved anskaffelse av IT-systemer

Formål og omfang

- Sørge for at felles IT-systemer blir innført på bakgrunn av kvalifiserte behovsvurderinger, og at innføringen blir forankret hos sentrale aktører (se Omfang).
- Danne grunnlag for felles forståelse mellom leverandører og RegionData om sikkerhetskravene til IT-systemet, leveransen og tilhørende tjenester.
- Forebygge sikkerhetshendelser og -brudd i implementerings- og driftsfasen.
- Utgangspunkt for etablering/endring av eksisterende sikkerhetsdokumentasjon.
- Grunnlag for senere sikkerhetsevaluering av IT-systemet og leverandøren og for gjennomføring av sikkerhetsrevisjoner knyttet til systemet.

Omfang

Kravspesifikasjonen gjelder for daglig leder, behandlingsansvarige og den respektive fagansvarlige, RegionDatas styre, regional IT-gruppe, RegionDatas databehandler og systembrukere. Kravspesifikasjonen gjelder ikke ved utvikling av programvare, men kan omfatte enkelte tilpasninger, f.eks. valg mellom standardopsjoner.

Kravspesifikasjonen omfatter nedenstående faser og behandler ansvar, rollefordeling og retningslinjer som gjelder for hver fase, herunder tiltak og kontrollpunkter som skal sikre aktiviteter, kvalitet, testrutiner, leveranser og dokumentasjon:

1. Identifisering og behovsvurdering
2. Prosjektetablering
3. Sikkerhetsvurdering
4. Sikkerhetskrav
5. Sikkerhetstiltak
6. Sikkerhetstesting og kontroll
7. Risikovurdering
8. Metodeutvikling

NB: Spesifikasjonen behandler, i tillegg til identifisering og vurdering av behov, ***kun*** sikkerhetsaspektet ved anskaffelse, implementering og bruk av felles IT-systemer i RegionData. Spesifisering av IT-systemets funksjonalitet og omfang (maskiner, tilleggsutstyr, programmer, komponenter, osv.) og evaluering og valg av system og leverandør omfattes ikke, men ligger til grunn for denne kravspesifikasjonen.

Hver fase er beskrevet på følgende måte:

1. Formål: Beskrivelse av hvorfor fasen blir benyttet i modellen.
2. Deltakere og roller: Funksjoner (interne og eksterne) som bør medvirke, deres ansvar og roller og evt. hvilken kompetanse som er påkrevet.
3. Forutsetninger: Fasens input.
   - Beslutningsgrunnlag: Ønsker, krav, behov, mål, planer, budsjetter, osv.
   - Henvisning til og evt. beskrivelse av hvilket regelverk og hvilke rammebetingelser som ligger til grunn og som vil være bestemmende for framgangsmåter og for konklusjonene/beslutningene: Relevante lover/forskrifter, rammebetingelser for RegionData (krav/mål, retningslinjer, forpliktelser til kommunene) og individuelle forutsetninger i kommunene.
4. Forventede resultater: Fasens output (en del av neste fases input).
5. Aktiviteter: Beskrivelse av alle aktivitetene.

Fase 1: Identifisering og behovsvurdering

1. Formål:

- Identifisere behov for å innføre/oppgradere fagsystemer i de enkelte kommunene.
- Identifisere behov for å etablere felles IT-systemer for eierkommunene i RegionData med enten separate eller felles tjenester for to eller flere av kommunene.
- Forankre beslutninger om å innføre/oppgradere fagsystemet hos eierkommunenes behandlingsansvarlige og den respektive fagansvarlige, RegionDatas styre, regional IT-gruppe, RegionDatas ledelse, databehandler i RegionData og brukere.

2. Deltakere og roller:

- Daglig leder RegionData:
  - Initiere oppgradering/innføring av felles IT-systemer for eierkommunene.
  - Sørge for at styret har tilstrekkelig grunnlag til å kunne foreta beslutninger.
- Prosjektleder (daglig leder): Utarbeidelse av prosjektbeskrivelse, mål og plan.
- Behandlingsansvarlige i kommunene/RegionDatas styre: Beslutningsmyndighet.
- Fagansvarlig i eierkommunene: Rådgivende funksjon.

3. Forutsetninger

Oppgradering eller innføring av felles IT-systemer med separate eller felles tjenester skal være begrunnet i eierkommunenes behov for å:

- Eliminere årsaker til eventuelle sikkerhetshendelser, -brudd og svakheter i eksisterende systemer ***og/eller***
- forbedre tjenestetilbudet, redusere kostnadene, forbedre kontroll og informasjonssikkerheten og/eller effektivisere ressursbruken.

Beslutningsgrunnlaget overfor styret bør være begrunnet i konkrete mål/krav. Følgende forbedringsområder bør vurderes i denne sammenhengen:

- Ytelse: Forholdet mellom arbeidsinnsats og responstid på tjenestene.
- Informasjon: Informasjonstilbudet overfor kommunens innbyggere.
- Økonomi: Kostnadene og kostnadskontrollen.
- Kontroll: Kontrollen og informasjonssikkerheten.
- Effektivitet: Utnyttelsen av menneskelige og teknologiske ressurser og prosesser.
- Service: Servicetilbudet overfor kommunens innbyggere.

Regelverk og rammebetingelser:

- Kommuneloven. Se også Sentrale lover og forskrifter.
- Samarbeidsavtalen mellom RegionData og eierkommunene.
- RegionDatas retningslinjer for Sikkerhetshendelser, -brudd og -svakheter.

4. Forventede resultater – fasens output:

- Identifiserte behov.
- Beslutningsgrunnlag overfor styret og styrevedtak.

5. Aktiviteter:

- Identifisering av behov i kommunene basert på kunnskap om kommunene, dialog med sentrale aktører og muligheter til å kunne innfri forbedringspotensialet.
- Utarbeide og underbygge beslutningsgrunnlag.
- Styremøte: Avslag, utsettelse eller godkjennelse med budsjettramme.
- Informere sentrale aktører om vedtak og rammevilkår.

Fase 2: Prosjektetablering

1. Formål:

- Initiere prosjektet og etablere og klarlegge prosjektvilkårene.
- Etablere en prosjektorganisasjon bestående av kompetent personell.
- Skape forståelse og aksept for prosjektets mål og planer i prosjektorganisasjonen.

2. Deltakere og roller:

- Prosjektleder (daglig leder): Utarbeidelse av prosjektbeskrivelse, mål og plan.
- Styringsgruppe: Beslutningsmyndighet.
- Prosjektdeltakere, herunder også RegionDatas databehandler og fagleverandør: Oppgaver og ansvar i henhold til tildelte roller.

3. Forutsetninger:

- Rammevilkår fra fase 1.
- RegionDatas retningslinjer for organisering av prosjekter: Prosjektorganisasjon.

4. Forventede resultater – fasens output

I løpet av denne fasen skal prosjektet være initiert og det skal være etablert:

- Prosjektorganisasjon.
- Prosjektbeskrivelse, mål, plan og budsjettramme.

5. Aktiviteter:

- Etablering av styringsgruppe og initiering av prosjekt.
- Utarbeide prosjektskisse innenfor rammene gitt av styret.
- Etablering av prosjektorganisasjon med ansvar og roller.
- Godkjennelse av prosjektbeskrivelse, mål, plan og budsjettramme.
- Informere prosjektdeltakere om prosjektbeskrivelse, arbeidsmodell, individuelle oppgaver og ansvar.

NB: Aktiviteter og beslutninger vedrørende valg av system og leverandør er ikke en del av, men ligger til grunn for kravspesifikasjon for sikkerhet.

Fase 3: Sikkerhetsvurdering

1. Formål:

- Identifisere og beskrive faktorer som vil være avgjørende for sikkerhetsvurderingen ved oppgradering eller innføring av felles IT-systemer for kommunene.
- Foreta en sikkerhetsvurdering basert på disse faktorene.
- Skape aksept og forståelse for sikkerhetsvurderingen i prosjektorganisasjonen.
- Grunnlag for etablering av sikkerhetskrav.

2. Deltakere og roller:

- Prosjektleder: Oppgaver og ansvar i henhold til prosjektorganisasjonen.
- Prosjektgruppe: Godkjenne arbeidsgruppens sikkerhetsvurdering.
- Arbeidsgruppe: Identifisering av faktorer og foreta en sikkerhetsvurdering.

3. Forutsetninger:

Fasens input:

- Prosjektbeskrivelse med mål, planer og budsjettramme.
- IT-systemets omfang (maskiner, tilleggsutstyr og -funksjonaliteter, programmer, komponenter).

Faktorer som vil være avgjørende for sikkerhetsvurderingen og som vil danne grunnlag for sikkerhetskravene (faktorene skal beskrives nærmere av arbeidsgruppa):

1. IT-systemets virkeområde (sikkerhetsløsninger, infrastruktur, fagsystemer, eller annet) og formålet med anskaffelsen.
2. IT-systemets omfang.
3. Systemmiljøet i RegionDatas serverpark.
4. Klassifisering av informasjonen som skal behandles i fagsystemet:
   - Offentlig tilgjengelig
   - Personsensitiv
   - Fortrolig
   - Evt. behov for sikkerhetsgradering i henhold til sikkerhetsloven
5. Fagsystem og dets anvendelsesområde, herunder bruk av:
   - Stasjonære tjenester.
   - Mobile tjenester.
   - Elektronisk meldingsutveksling.
   - Elektroniske signaturer.
6. Organisering av tjenestene i fellessystemet:
   - Separate tjenester.
   - Fellestjenester mellom et utvalg av eierkommunene.
7. Eksterne forbindelser og fjerntilgang til systemet.
8. Kommunenes sårbarhet for driftsforstyrrelser og -stans i IT-systemet.

4. Forventede resultater – fasens output:

- Dokumentert grunnlag for etablering av sikkerhetskrav.

5. Aktiviteter:

- Etablering av arbeidsgruppe med ansvar og roller.
- Identifisere, beskrive og prioritere faktorer som er avgjørende for sikkerhetsvurderingen og utarbeide en sikkerhetsvurdering på bakgrunn av dette.
- Underbygge eller eventuelt endre målene fra fase 1.

Fase 4: Sikkerhetskrav

1. Formål:

- Etablere sikkerhetskravene i forbindelse med anskaffelse, implementering og bruk av felles IT-systemer med utgangspunkt i sikkerhetsvurderingen.
- Grunnlag for etablering av sikkerhetstiltak overfor fag-/systemleverandør i forbindelse med implementering av systemet i RegionData.

2. Deltakere og roller:

- Prosjektleder: Oppgaver og ansvar i henhold til prosjektorganisasjonen.
- Prosjektgruppe: Godkjenne arbeidsgruppens sikkerhetskrav.
- Arbeidsgruppe: Utarbeide sikkerhetskrav basert på sikkerhetsvurderingen.

3. Forutsetninger:

Fasens input:

- Sikkerhetsvurdering.
- IT-systemets omfang.

Regelverk og rammebetingelser:

- Sentrale lover og forskrifter som gjelder for RegionData, og som vil være retningsgivende for sikkerhetskravene til den informasjonen som skal behandles i systemet.

Med bakgrunn i sikkerhetsvurderingen, skal arbeidsgruppen vurdere sikkerhetskrav i forbindelse med anskaffelse, implementering og bruk. Dette gjelder innenfor:

1. Kontraktsvilkår
2. Dokumentasjonskrav til leveransen
3. Systemtekniske sikkerhetskrav
4. Interne sikkerhetsforhold

1. Kontraktsvilkår:

- Sikkerhetskrav i kontrakter (se Krav til Samarbeidspartnere og leverandører).
- Leverandørens ansvar og rolle i prosjektet.
- Spesifisering av eventuelle tilleggsytelser (bistand ved innkjøring av system, konvertering av data fra tidligere systemer, osv.).
- Support og fastsettelse av tjenestenivå, f.eks. telefonveiledning, feilretting via nett, service på brukersted, tilkallingstid, tilgjengelighet (døgntider og ukedager).
- Programservicens omfang: Feilretting, oppgraderinger til nye versjoner (forbedringer og nye funksjonaliteter), tilpasninger til nye generelle krav i lovverk.
- Leverandøren skal gjøres kjent med RegionDatas rutiner for tildeling av rettigheter ved oppgraderinger, endringer eller feilretting.

2. Dokumentasjonskrav til leveransen:

- Komponentspesifikasjon: Klar og entydig definering av alle komponenter.
- Avvik mellom spesifikasjon og tilbud: Leverandøren skal klargjøre på hvilke punkter RegionDatas sikkerhetskrav, kravspesifikasjoner til funksjonalitet og/ eller formålsbeskrivelse ikke blir dekket av den løsningen som leverandøren kan tilby og som partene har blitt enige om.

- Installasjon av programvare: Leverandøren skal kunne vise til dokumenterte prosedyrer for å kontrollere installasjon av programvare i serverparken, herunder prosedyrer for testing og beskyttelse av data for systemtesting (se fase 6 Sikkerhetstesting og kontroll).
- Endringsstyring: Leverandøren skal kunne vise til dokumenterte prosedyrer for endringsstyring slik at alle planlagte systemendringer blir kontrollert på en måte som vil sikre at de ikke svekker sikkerheten til det aktuelle systemet eller driftsmiljøet.
- Prosjektrapportering: Leverandøren kan avvike fra RegionDatas rapporteringsrutiner dersom han kan vise til egne rutiner som kan godkjennes av RegionData.

3. Systemtekniske sikkerhetskrav

- "Helpdesk" for rapportering og oppfølging av sikkerhetshendelser, -brudd og -svakheter.
- Sikkerhetskrav til løsninger for kryptert datakommunikasjon og elektroniske signaturer:
  - Dokumentasjon av sertifikatpolicy.
  - Leverandøren skal dokumentere at nøkkeladministrasjon er basert på et avtalt sett med standarder, prosedyrer og sikre metoder.
  - Leverandøren skal klarlegge hvilke kryptografiske teknikker som anvendes:
    - Passord
    - Asymmetrisk (elektroniske signaturer)
    - Symmetrisk
  - Leverandøren skal oppgi nøkkellengden for ulike kryptografiske systemer og forskjellige applikasjoner som omfattes av leveransen. Ved generering av kvalifiserte elektroniske sertifikater til offentlig sektor, skal det benyttes en nøkkellengde på minst 1024 bit.
  - Leverandøren (utvikleren) skal, hvis mulig, forelegge en erklæring om i hvilken grad alle nøkkelmulighetene som ligger i de genererte nøkkellengdene blir utnyttet for hver nøkkel.
  - Tekniske spesifikasjoner og integrasjon mot andre systemer:
    - I henhold til Kravspesifikasjon for PKI i offentlig sektor.
  - Leverandøren skal dokumentere at elektroniske signaturer blir generert i henhold til kravene i Kravspesifikasjon for PKI i offentlig sektor, og at de er kvalifiserte i henhold til e-signaturloven med forskrift.
  - Funksjoner for logging av aktiviteter.

4. Interne sikkerhetskrav

I forbindelse med implementering og bruk av systemet, bør arbeidsgruppen, med utgangspunkt i sikkerhetsvurderingen, klarlegge følgende sikkerhetskrav:

- Bruk av felles tjenester: Det skal foreligge kommunale avtaler som regulerer forholdene mellom kommunene og tilgang til de ulike databasene ved innføring av felles fagsystemer med felles tjenester.
- Soneplassering (sikret eller intern).
- Autorisering av personell for tilgangsrettigheter.
- Aktivitetslogging og krav til registrering og oppbevaring av logger.
- Oppbevaring av sikkerhetskopier.
- Bruk av e-post.
- Krav om meldeplikt (gjelder eierkommunene).
- Avhending av utstyr.

Regelverk og rammebetingelser for vurdering av interne sikkerhetskrav:

- Lovhenvisning: Se Sentrale lover og forskrifter som gjelder for RegionData.
- Nettverks- og IT-sikkerhetsarkitektur.
- Autorisasjon og tilgangsrettigheter.
- Aktivitetslogg.
- Oppbevaring av kopier.
- Bruk av elektronisk e-post.
- Krav om meldeplikt (angår kommunene).
- Avhending av brukt og kassert utstyr.

Behandling av sikkerhetsgradert informasjon:

- Henvisning til egne veiledninger fra Nasjonal Sikkerhetsmyndighet: (www.nsm.stat.no).

4. Forventede resultater – fasens output

- Sikkerhetskrav i forbindelse med anskaffelse, implementering og bruk av felles IT-systemer i RegionDatas serverpark.
- Grunnlag for sikkerhetstiltak i fase 5.
- Eventuelle endringer i omfang eller presisering av mål.

5. Aktiviteter:

- Etablering av arbeidsgruppe med ansvar og roller.
- Fastsettelse av sikkerhetsmessige kontraktsvilkår.
- Utarbeidelse av dokumentasjon av sikkerhet ved leveransen.
- Fastsettelse av systemtekniske sikkerhetskrav.
- Fastsettelse av interne sikkerhetsforhold.
- Godkjenning av sikkerhetskravene.
- Klarlegging og godkjenning av eventuelle endringer i omfang eller mål.

Fase 5: Sikkerhetstiltak

1. Formål:

- Beskrivelse av hvordan sikkerhetskravene skal gjennomføres i kontraktgjennomgåelsen med leverandør og i implementeringen av systemet i RegionData.
- Klarlegge behovet for og omfanget av sikkerhetstesting og kontroll (se fase 6).
- Sørge for å etablere eller oppdatere/endre sikkerhetsdokumentasjon som følge av sikkerhetskravene:
  - Sikkerhetssystemet eller sikkerhetsprosedyrer.
  - Registreringer: Kontrakter og sikkerhetsavtaler, autorisasjon og rettigheter, passordoversikter, nettverks- og sikkerhetsarkitektur, utstyr og komponentoversikt, etc.

2. Deltakere og roller:

- Prosjektleder: Oppgaver og ansvar i henhold til prosjektorganisasjonen.
- Prosjektgruppe: Godkjenne arbeidsgruppens sikkerhetstiltak.
- Arbeidsgruppe: Utarbeide sikkerhetstiltak basert på sikkerhetskravene.
- Eksterne ressurser: Fagleverandør, RegionDatas databehandler.

3. Forutsetninger:

Fasens input:

- IT-systemets omfang.
- Sikkerhetskrav fra fase 4.
- Leverandørens prosedyrer for testing (se fase 6).

Regelverk og rammebetingelser:

- Sentrale lover og forskrifter som gjelder for RegionData.
- Sikkerhetshåndbok.
- Endringsstyring.

4. Forventede resultater – fasens output:

- Oppdaterte registreringer i sikkerhetssystemet.
- Eventuelle endringer i sikkerhetshåndbok.
- Grunnlag for gjennomgåelse av sikkerhetskravene i kontrakten med leverandør.

5. Aktiviteter:

- Etablering av arbeidsgruppe med ansvar og roller.
- Klarlegge eksterne ressursers roller som bidragsyter til arbeidsgruppen.
- Utarbeidelse av sikkerhetstiltak basert på sikkerhetskravene i fase 4.
- Godkjenning av sikkerhetstiltakene.

Fase 6: sikkerhetstesting og kontroll

1. Formål:

- Testing av implementerte sikkerhetstiltak ved behov.

2. Deltakere og roller:

- Prosjektleder: Oppgaver og ansvar i henhold til prosjektorganisasjonen.
- Prosjektgruppe: Godkjenne systemgruppens testresultater.
- Systemgruppe: Testing og evaluering av fagsystem og sikkerhetstiltak.
- Eksterne ressurser: Fagleverandør, RegionDatas databehandler.

3. Forutsetninger:

Fasens input:

- IT-systemets omfang.
- Sikkerhetstiltak fra fase 5.

Rammebetingelser:

1. Testbeskrivelsen bør inneholde følgende punkter:
   - Bakgrunn for testen.
   - Formål: Hva man ønsker å finne ut av.
   - Omfang: Hva som skal testes og varighet på testen.
   - Prosessopplysninger: Opplysninger om prosessen som er viktig for testen.
   - Evaluering: Tilpasset formålet med testen.
2. Beskyttelse av data for systemtesting: NS-ISO/IEC 17799:2006:
   - Testing av databaser som inneholder persondata eller annen sensitiv informasjon bør unngås. Dersom persondata eller annen sensitiv informasjon brukes i testing, bør alle sensitive opplysninger og alt sensitivt innhold fjernes eller gjøres ugjenkjennelig før bruk. Følgende retningslinjer bør brukes for å beskytte produksjonsdata når de skal brukes i testing:
     - Prosedyrene for aksesskontroll som gjelder for fagsystemene, bør også gjelde for testsystemene.
     - Det bør kreves separat autorisasjon hver gang produksjonsinformasjon kopieres til et testsystem.
     - Produksjonsdata bør slettes fra testsystemet umiddelbart etter at testingen er avsluttet.
     - Kopiering og bruk av produksjonsinformasjon bør logges for å sikre revisjonsspor.

4. Forventede resultater – fasens output:

Evaluerte sikkerhetstiltak med angivelse av eventuelle avvik.

5. Aktiviteter:

- Testing av sikkerhetstiltak.
- Godkjenning av sikkerhetstiltakene basert på testresultatene.

Fase 7: Risikovurdering

1. Formål:

Formålet med risikovurderingen er:

- Håndtere eventuelle avvik som ble registrert i foregående faser.
- Beskrive og vurdere de sikkerhetsmessige konsekvensene av hvert avvik.
- Beskrive kompenserende tiltak inntil den gjenværende risikoen er akseptabel.

2. Deltakere og roller:

- Styringsgruppen (behandlingsansvarlige i kommunene) og daglig leder i Region-Data: Fastsette akseptabel risiko.
- Prosjektleder: Oppgaver og ansvar i henhold til prosjektorganisasjonen.
- Prosjektgruppe: Godkjenne risikovurderingen.
- Arbeidsgruppe (person(er), internt evt. ekstern person): Risikovurdering.
- Fagansvarlig i eierkommunene: Rådgivende funksjon.
- Eksterne ressurser: Fagleverandør, RegionDatas databehandler.

3. Forutsetninger:

Fasens input:

- Registrerte avvik fra fase 6 og tidligere faser.
- Se også prosedyre for Risikovurderinger.

4. Forventede resultater:

- Godkjenning av anskaffelse og implementering.

5. Aktiviteter:

- Gjennomføring av risikovurdering på bakgrunn av registrerte avvik.
- Fastsettelse av akseptabel risiko.
- Eventuell korrigering av avvik.

Referanser

Sikkerhetsrevisjoner og risikovurderinger.

Fase 8: Metodeutvikling

1. Formål:

- Evaluere metodikken i forhold til formålet.
- Holde metoden ved like og utvikle den slik at den til enhver tid er oppdatert og hensiktsmessig i forhold til praktisk bruk, lovmessige, kontraktsmessige og forretningsmessige forutsetninger.

2. Deltakere og roller:

- Daglig leder: Evaluering av metode og ansvarlig funksjon.
- Leder av prosjektgruppe: Evaluering av metode.
- Utvalg av prosjektdeltakere: Evaluering av metode.
- Intern sikkerhetsrevisor: Revisjon av metode.

3. Forutsetninger:

At metoden har blitt benyttet og evaluert etter hvert prosjekt i forhold formålet med fase 7.

Grunnlaget for evaluering av metoden vil være:

- Erfaringer fra bruk av metoden i prosjekter.
- Resultater fra sikkerhetsrevisjoner og risikovurderinger.
- Endringer i offentlige rammevilkår (lover, forskrifter, normer).

4. Forventede resultater – fasens output:

- Eventuelle endringer i metode.
- Utfylling av punkter som er retningsgivende for de respektive fasene.

5. Aktiviteter:

- Valg av én eller flere person(er) fra prosjektet.
- Gjennomgang og evaluering av metode i forhold til formål og oppnådde resultater.

Referanser

Endringsstyring.