Overordnede sikkerhetskrav

i Arbeids- og velferdsetaten

«Dette dokumentet inneholder overordnede sikkerhetskrav innenfor områdene personvern, informasjonssikkerhet og beredskap for Arbeids- og velferdsetaten»

Godkjent 16.02.2018

ENDRINGSLOGG

Ver.	Dato	Kap.	Endring	Produsent	Godkjent av
1.0	28.04.2010	Alle	Endelig standard-dokument godkjent	IT-sikkerhetsansvarlig	IT-direktør
1.01	05.07.2012	Alle	Periodisk revisjon, endret navn		
1.02	24.08.2012	Alle	Gjennomgått i PIB, for høring		
1.03	12.10.2012	Alle	Innarbeidelse av høringssvar	Seksjon PIB	Til behandling i d-møte
1.03	30.10.2012	Alle	Ingen	Seksjon PIB	Behandlet og godkjent i d-møte 30.10.12
1.07	Nov. 2014	Alle	Oppdatert iht. ISO 27001:2013 og organisasjons-endringer	Sikkerhetsseksjonen	
1.1	17.02.2015	Alle	Ingen	Sikkerhetsseksjonen	Godkjent i D-møte 17.02.15
1.16	12.06.2017	Alle	Gjennomgått for høring	Sikkerhetsseksjonen	
1.18	27.06.2017	Alle	Sendt på høring i avdelingene	Sikkerhetsseksjonen	
1.19	01.09.2017	Alle	Innarbeidelse av høringssvar	Sikkerhetsseksjonen	
1.2	16.02.2018	Alle	Gjeldende fram til mai 2018	Sikkerhetsseksjonen	Geir Axelsen

INNHOLDSFORTEGNELSE

0. INNLEDNING

0.1 Hvordan oppnå tilfredsstillende sikkerhet i Arbeids- og velferdsetaten

Begrepet *sikkerhet* i denne sammenhengen favner både personvern-, informasjonssikkerhets-, og beredskapsområdet. Tilfredsstillende sikkerhet baserer seg på gode holdninger og bevissthet hos ledere og medarbeidere, robuste systemer og etterlevelse av etatens mål, strategier og sikkerhetskrav. Gode kontrollmekanismer, klare ansvarsforhold, kompetente medarbeidere, samt klare og oppdaterte sikkerhetskrav og operative retningslinjer vil sammen danne grunnlag for en god sikkerhetskultur i Arbeids- og velferdsetaten.

0.2 Formål og innhold

Dokumentet beskriver etatens sikkerhetskrav samlet sett og er underordnet «Styringsdokument for personvern, informasjonssikkerhet og beredskap i NAV». Kravene er delt inn i 15 fokusområder, med beskrivelse av mål og nødvendige sikkerhetskrav for å sikre måloppnåelsen. Det er tatt utgangspunkt i «Norsk Standard NS-ISO/IEC 27001:2013 Administrasjon av informasjonssikkerhet» ved utforming av dette dokumentet. Personvern er tatt med som eget fokusområde. Beredskap er tatt med som en utvidelse av fokusområde «Kontinuitet» som blir til «Kontinuitet og beredskap».

Sikkerhetskravene er avstemt mot lovpålagte krav og håndteres i henhold til ovennevnte ISO-standard. Ansvaret for å følge opp kravene fremgår av styringsdokumentet/1/. Praktisk gjennomføring av kravene er beskrevet i operative retningslinjer.

Økonomi- og styringsdirektøren har regimeansvaret for sikkerhet og er eier av dokumentet. Kunnskapsavdelingen har regimeansvaret for personvern og gir føringer innenfor dette området. Dokumentet skal gjennomgås årlig for å sikre at det er oppdatert i forhold til regler og trusselbilde. Ved vesentlige endringer forankres dokumentet gjennom høring i avdelingene i direktoratet og behandling i direktørmøtet.

Dokumentet har følgende vedlegg:

- Vedlegg A: Relevante lover, forskrifter og regelverk
- Vedlegg B: Oversikt over operative sikkerhetskrav
- Vedlegg C: Definisjoner
- Vedlegg D: Interessenter til sikkerhetsarbeidet

0.3 Fokusområder

De 15 fokusområdene som sikkerhetskravene deles inn i er gjengitt i figur 1 og danner grunnlag for disposisjonen av kravene i dette dokumentet:

1. Personvern	**2. Styring av sikkerhet**	**3. Organisering av sikkerhet**	**4. Personellsikkerhet**	**5. Administrasjon av informasjonsressurser**
6. Tilgangskontroll	**7. Kryptografi**	**8. Fysisk og miljømessig sikkerhet**	**9. Driftssikkerhet**	**10. Sikker kommunikasjon**
11. Sikker anskaffelse og utvikling av IT-systemer	**12. Leverandørstyring**	**13. Sikkerhetshendelser og avvik**	**14. Kontinuitet og beredskap**	**15. Etterlevelse**

Figur 1: *Sikkerhet i NAV er inndelt i 15 fokusområder*

1. PERSONVERN

Det er under utarbeidelse et eget styringssystem for personvern. Dette vil bli vedtatt i løpet av våren 2018. Kravene i det nye styringssystemet vil være gjeldende på personvernområdet.

Personvern vil si å sørge for forsvarlig og sikker behandling av personopplysninger for å bidra til korrekte avveininger og avgjørelser. Arbeidet med personvern og herunder overholdelse av taushetsplikt skal bidra til ivaretakelse av rettssikkerhet og konfidensialitet. Et godt personvern skal sikre at forvaltningens brukere og samfunnet for øvrig, har tillit til NAVs behandling av personopplysninger.

1.1 Overordnede prinsipper for personvern

I arbeidsprosesser, organisasjonsutvikling, systemutviklingsprosesser og anskaffelser skal etaten ivareta personvernet. Vurdering av personvernkonsekvenser skal alltid gjennomføres og dokumenteres. Prinsippet om *innebygd personvern* skal følges ved etatens systemutvikling. Det betyr at det skal tas hensyn til personvern i alle utviklingsfaser av et system.

Generell informasjon om NAVs behandling av personopplysninger skal være lett tilgjengelig i form av en personvernerklæring på nav.no

Skriftlige avtaler med tredjeparter, samhandlere og leverandører skal inneholde alle relevante krav til personvern, taushetsplikt, informasjonssikkerhet og beredskap.

1.2 NAVs plikter som behandlingsansvarlig

Behandlingsansvar innebærer å ha det daglige ansvaret (fagansvar) for behandling av personopplysninger i arbeids- og velferdsetaten. Dette ansvaret skal være fastsatt og dokumentert.

Det skal være en samlet oversikt over etatens behandling av personopplysninger inndelt i behandlingslingsområder, som tar utgangspunkt i faglige områder som logisk hører sammen.

Det skal foreligge rettslig grunnlag for all behandling av personopplysninger i NAV. Formål med bruk av personopplysningene skal defineres, være saklig begrunnet ut fra NAVs virksomhet, og skal dokumenteres.

All behandling av personopplysninger skal tilfredsstille grunnleggende krav til kvalitet. Personopplysningene skal ved bruk være fullstendige, relevante, korrekte og oppdaterte ut fra det formål de skal brukes til.

Personopplysninger skal ikke lagres lengre enn det som er nødvendig. Det skal settes krav til lagring , lagringstid og sletting av personopplysninger.

Det skal være åpenhet ovenfor alle om hvordan NAV behandler personopplysninger og hva denne behandlingen går ut på. Det skal tilrettelegges for en generell innsynsrett. Enhver har rett til å få vite om NAV har registrert opplysninger om vedkommende, og kan kreve individuelt innsyn i personopplysningene.

NAV har i utgangspunktet en plikt til å gi informasjon eller varsle bruker når personopplysninger samles inn enten det er direkte fra bruker selv eller når opplysningene innhentes fra andre. Det gjelder ikke hvis innsamlingen er uttrykkelig fastsatt i lov.
All behandling av personopplysninger skal meldes til, eller det skal søkes konsesjon hos Datatilsynet. Meldingene skal fornyes hvert tredje år. Melding eller konsesjon skal foreligge før behandling av personopplysninger påbegynnes.

Det skal bare overføres personopplysninger til mottakere og leverandører i utlandet som sikrer forsvarlig behandling av personopplysninger. Ved bruk av databehandlere i tredjeland skal EU-standardkontrakt for overføring av personopplysninger til utlandet brukes.

1.3 Brukers rettigheter

NAV skal behandle personopplysninger innenfor definerte formål og rettslig grunnlag. Opplysningene som blir brukt skal ha nødvendig kvalitet og bli behandlet sikkert. NAV skal ivareta brukers rettigheter etter personopplysningsloven

- ved krav om informasjon om behandling av personopplysninger
- ved krav om innsyn
- ved krav om retting eller sletting av personopplysninger

Bruker skal involveres og informeres om hvilke personopplysninger NAV behandler om vedkommende for å kunne ivareta brukers personverninteresser og samtidig sikre en aktiv og god brukermedvirkning.

For automatiserte avgjørelser har bruker rett til å få informasjon om regelinnholdet som ligger til grunn.

1.4 Ansattes rettigheter

NAV som arbeidsgiver skal sikre at de ansatte er vernet mot inngripende kontroll gjennom å følge personopplysningsloven og arbeidsmiljølovens bestemmelser. Kontrolltiltak skal være saklig og ikke uforholdsmessig belastende.

NAV skal følge personopplysningslovens bestemmelser om innsyn i ansattes e-post og private filområder.

1.5 Taushetsplikt

Alle som utfører tjeneste eller arbeid for etaten er bundet av taushetsplikten som følger av arbeids- og velferdsforvaltningsloven, lov om sosiale ytelser i NAV og forvaltningsloven. Taushetsplikten skal ivaretas ved behandling av personopplysninger.

Ved organisering og tilordning av arbeidsoppgaver skal det legges vekt på begrensning av tilgang til personopplysninger til det som er nødvendig for å utføre oppgaven.

Alle medarbeidere skal påse at taushetsplikten ivaretas i samhandling med brukere, samhandlingspartnere og andre aktører.

Taushetsbelagt informasjon skal aldri utleveres uten at det foreligger lovhjemmel eller samtykke.

Det skal føres samlede oversikter i de forskjellige fagmiljøene og enhetene der Arbeids- og velferdsetatens har rutinemessige utleveringer av taushetsbelagte personopplysninger til eksterne. Oversikten skal inneholde rettslig grunnlag for utlevering, formål og hvilke type personopplysninger som utleveres.

1.6 Særskilte sikkerhets- og beskyttelsestiltak

Etaten skal sikre trusselutsatte brukere med adressesperre fra politi eller barnevernsmyndighet/skatteetaten (kode 6 og kode 7), slik at det ikke utleveres opplysninger om bostedsadresse eller annen informasjon som kan avsløre brukers tilholdssted.

2. STYRING AV SIKKERHET

Vil si å sikre at prosesser og tiltak for personvern, informasjonssikkerhet og beredskap er i tråd med og understøtter de mål og strategier som ledelsen har definert for virksomheten.

2.1 Ledelsens styring av sikkerhet

2.1.1 Prinsipper for sikkerhet

Styringsdokument for personvern, informasjonssikkerhet og beredskap i NAV definerer målene og strategiene for sikkerhet i NAV og hvordan disse bidrar til NAVs virksomhetsmål.

Arbeids- og velferdsetaten har felles prinsipper for risikostyring og felles mal for risikoanalyse som skal benyttes på alle områder i etaten. Disse definerer hvordan risikoanalyse skal gjøres, hva som er akseptabelt risikonivå og når det skal gjennomføres risikoreduserende tiltak.

I NAVs helhetlige metode for risikostyring er sikkerhetsområdet delt inn i to kategorier:

Kategori 1 – Beredskap og samfunnssikkerhet:

- Risiko for at vi ikke er forberedt til å håndtere hendelser eller har etablert tilstrekkelig grunnsikring
- Risiko for at katastrofer eller ulykker rammer NAV eller krever ekstraordinær innsats fra oss

Kategori 2 – Personvern og informasjonssikkerhet:

- Risiko for at vi behandler personopplysninger uten hjemmel
- Risiko for at personopplysningene ikke har den nødvendige kvalitet
- Risiko for at NAV ikke oppfyller brukerens rettigheter om innsyn
- Risiko for at taushetsbelagt informasjon kommer på avveie eller til uvedkommende
- Risiko for at vi ikke har tilstrekkelig integritet i den informasjon vi benytter i vår behandling
- Risiko for at IT-tjenester er utilgjengelig eller informasjon går tapt

For å ha tilstrekkelig sikkerhet må risikovurderinger gjennomføres årlig, og i tillegg ved endringer som har betydning for personvern, informasjonssikkerhet eller beredskap.

Den samlede risikovurderingen på sikkerhetsområdet skal danne grunnlag for etatens beredskapsplanlegging og for prioriteringer av forbedringstiltak. Sikkerhetsseksjonen skal løpende overvåke risikobildet. Vesentlige endringer rapporteres til ledelsen.

2.1.2 Periodisk gjennomgang av sikkerhetsprinsipper

Styringsdokument og overordnede sikkerhetskrav skal oppdateres årlig og ellers ved behov for dette. Dette er en del av arbeidet med kontinuerlig forbedring.

Arbeids- og velferdsdirektøren foretar i samråd med ledergruppen en årlig gjennomgang av sikkerhetstilstanden i etaten. I ledelsens gjennomgang gjennomgås risikobildet for sikkerhetsområdet basert på hendelser, avviksmeldinger, funn fra kontroller, kjente mangler og generelle trusselvurderinger. Utfra dette gjennomgås anbefalte tiltak og det besluttes retning og omfang for sikkerhetsarbeidet fremover. Ledelsens gjennomgang er også en del av underlaget for ledelsens uttalelse om styring og kontroll etter kravene i Økonomiregelverket.

3. ORGANISERING AV SIKKERHET

Vil si å sørge for at sikkerhetsarbeidet styres slik at sikkerheten opprettholdes i etatens informasjonsbehandling. I tillegg er hensikten å skape bred forståelse for relevante risikoer blant etatens ledere og medarbeidere.

3.1 Intern organisering av sikkerhet

3.1.1 Roller og ansvar for sikkerhet

Ansvar, plikter og oppgaver knyttet til sikkerhet skal være definert. Dette er gjort i styringsdokument for personvern, informasjonssikkerhet og beredskap og i Ansvarsdokument for arbeids- og velferdsdirektoratet.

- Enhver leder i etaten har ansvar for å ivareta og følge opp sikkerheten i egen enhet
- Medarbeidere som har en spesiell rolle innen sikkerhetsområdet, skal ha tilstrekkelig kompetanse og ressurser for å kunne ivareta sin rolle
- Alle medarbeidere er ansvarlig for forsvarlig håndtering av sikkerhet i sitt daglige arbeid

3.1.2 Arbeidsdeling

Arbeidsoppgaver og myndighet skal holdes atskilt der risikoen for utilsiktet eller tilsiktet sikkerhetsbrudd vil være for stor dersom alt legges til en og samme person.

3.1.3 Kontakt med myndigheter

For å sikre en best mulig forståelse av trusselbildet slik det er til enhver tid og hvilke tiltak som er effektive skal det være kontakt med aktuelle myndigheter og etater.

- Sikkerhetsseksjonen skal ha jevnlig kontakt med, Direktoratet for sivil beredskap (DSB), Nasjonal sikkerhetsmyndighet (NSM) og deres NorCERT, samt Arbeids- og sosialdepartementet, Direktoratet for forvaltning og IT (DIFI), Politiet og Politiets sikkerhetstjenester (PST) i spørsmål som gjelder personvern, informasjonssikkerhet og beredskap
- Kunnskapsavdelingen koordinerer kontakten med Datatilsynet
- Fylkeskontorene skal ha kontakt med Fylkesmannens beredskapsutvalg
- NAV kontorene skal ha kontakt med beredskaps- og sikkerhetsfunksjoner i kommunen

3.1.4 Kontakt med interessenter

For å sikre en best mulig forståelse av hvordan interessenter som berøres av NAVs sikkerhetsregime oppfatter og forholder seg til dette, er det viktig å ha kontakt med disse ved endringer i sikkerhetsregler og oppdatering av risikobildet. Oversikt over de viktigste interessentene finnes i vedlegg D.

3.1.5 Sikkerhet i prosjektstyring

Sikkerhetskravene i NAV gjelder også for prosjekter. Prosjektleder må være kjent med de sikkerhetskrav som er relevant for prosjektets oppgaver.

3.2 Mobilitetsløsninger og fjernarbeid

3.2.1 Regulering av mobilitetsløsninger

Det skal foreligge sikringstiltak for å beskytte mot risiko ved bruk av mobilt IT-utstyr.

Det skal være hensiktsmessige autentiseringsmetoder for å kontrollere fjernbrukeres tilgang til systemer.

3.2.2 Fjernarbeid

I rutiner og retningslinjer for fjernarbeid skal krav til sikkerhet for informasjon og utstyr ivaretas.

4. PERSONELLSIKKERHET

Vil si å ha tiltak og aktiviteter som støtter opp under en god sikkerhetskultur. Alle medarbeidere må være informert om sitt ansvar. Plikter og rettigheter skal være klart beskrevet og fastsatt. Alle medarbeiderne skal ha god kompetanse, ferdigheter, holdninger og adferd innenfor sikkerhet.

4.1 Før ansettelse

4.1.1 Bakgrunnssjekk

Ved alle tilsettinger skal det foretas referansesjekk og vurdering av ekthet i dokumentasjon som legges frem i henhold til etatens rekrutteringsrutiner.

Alle medarbeidere som behandler gradert informasjon etter sikkerhetsloven, skal være kompetente og inneha gyldig sikkerhetsklarering. Sikkerhetsseksjonen håndterer saker vedrørende sikkerhetsklarering.

4.1.2 Ansettelsesbetingelser

Taushetserklæring og sikkerhetsinstruks for medarbeider og leder er en del av arbeidsbetingelsene i NAV og skal undertegnes av alle medarbeidere og ledere.

4.2 Under arbeidsforholdet

4.2.1 Ledelsesansvar

Ledere er ansvarlige for at deres medarbeidere er orientert om etatens sikkerhetskrav og skal påse at disse følges.

4.2.2 Opplæring i sikkerhet og etablering av sikkerhetskultur

Alle medarbeidere, eksterne konsulenter og andre som arbeider på oppdrag for etaten skal ha nødvendig kompetanse og få nødvendig opplæring innen relevante sikkerhetsområder.

- Alle medarbeidere skal ha tilstrekkelig kompetanse om personopplysningsloven og personopplysningsforskriftens bestemmelser som er av betydning for deres arbeidsoppgaver
- Alle medarbeidere skal ha kjennskap til informasjonssikkerhetskrav og prosedyrer som gjelder for sine oppgaver
- Det skal være etablert tiltak og aktiviteter som støtter opp under en god sikkerhetskultur. Tiltakene skal følges opp og være målbare

Det skal i tillegg til grunnleggende opplæring i de ulike sikkerhetsområdene gis regelmessig informasjon og nødvendig opplæring for å sikre kunnskap om oppdaterte rutiner og krav og som en oppfriskning av den grunnleggende opplæringen.

4.2.3 Disiplinære prosesser

Brudd på sikkerhetsbestemmelsene skal følges opp av nærmeste leder i henhold til gjeldende regelverk og rutiner.

4.3 Etter endt arbeidsforhold

4.3.1 Ansvar ved endt arbeidsforhold

Taushetsplikten gjelder også etter at arbeidsforholdet er avsluttet.

Tilganger for alle medarbeidere, eksterne konsulenter, og ansatte hos tjenesteleverandører, skal fjernes eller justeres ved endringer når deres ansettelse, kontrakt eller avtale avsluttes, samt når ny rolle tildeles.

5. ADMINISTRASJON AV INFORMASJONSRESSURSER

Vil si å ha oversikt over hvor vi lagrer og behandler informasjon og oversikt over ansvarsforhold og klassifisering, slik at det kan gis riktig beskyttelsesnivå.

5.1 Ansvar for informasjonsressurser

5.1.1 Oversikt over informasjonsressurser

Det skal til enhver tid foreligge oppdaterte og korrekte oversikter over informasjon, systemer og IT-ressurser, der blant annet klassifisering av ressursene fremgår.

5.1.2 Eierskap til informasjonsressurser

Alle ressurser skal ha navngitte behandlingsansvarlige.

5.1.3 Akseptabel bruk av informasjonsressurser

Eiere av en informasjonsressurs er ansvarlig for å sikre ressursen og har ansvar for forsvarlig bruk, sletting eller kassering av ressursen.

Etatens IT-systemer skal kun benyttes til de formål som de er godkjent for. Bruk av NAVs fagsystemer skal kun skje etter tjenstlig behov.

Det skal kun benyttes IT-utstyr, lagringsmedia og programvare på NAVs nettverk som er godkjent av IT-avdelingen. Tilsvarende gjelder for bruk av mobilt utstyr mot NAVs nettverk. Særskilte behov for bruk av egen PC og/eller programvare utenom standard skal avklares med IT-avdelingen via enhetsleder. Mobilt utstyr, herunder hjemmekontorutstyr, skal benyttes slik at uvedkommende ikke får tilgang til jobbrelatert informasjon og data.

5.1.4 Tilbakelevering av NAVs eiendeler

NAVs eiendeler som en medarbeider disponerer skal leveres tilbake til NAV når medarbeideren slutter eller ikke lenger har tjenstlig bruk for dem.

Når en medarbeider eller andre som utfører arbeid for NAV må lagre informasjon på utstyr eller media som ikke tilhører NAV, skal dette slettes etter endt oppdrag med mindre annet spesifikt er avtalt.

5.2 Klassifisering av informasjon

5.2.1 Klassifisering

Informasjon, prosesser, IT-systemer og informasjonslagre skal klassifiseres for å indikere behovet for beskyttelse. Eieren av en ressurs er ansvarlig for klassifisering av den.

5.2.2 Merking av informasjon

Informasjon og dokumenter som skal ha begrenset spredning skal merkes med dette.

5.2.3 Behandling av informasjonsressurser

Bruk, lagring og arkivering av informasjon skal sikres i samsvar med klassifiseringen. Enhver som arbeider for etaten har et ansvar for å skjerme informasjon og systemer fra uautorisertes adgang og tilgang.

5.3 Håndtering av lagringsmedia

5.3.1 Håndtering av flyttbare lagringsmedia

For å hindre uautorisert utlevering, endring, fjerning eller ødeleggelse av informasjon som er lagret på flyttbare lagringsmedia, må alle medarbeidere vise ekstra aktsomhet i behandlingen av disse.

5.3.2 Rutiner for avhending av lagringsmedia

Alle data på lagringsmedia som har eller kan ha vært benyttet til å lagre taushetsbelagt informasjon fra NAV skal slettes på en sikker måte eller makuleres før avhending.

5.3.3 Fysisk transport av lagringsmedia

Lagringsmedier som inneholder informasjon, skal beskyttes mot uautorisert adgang, misbruk og ødeleggelse under transport utenfor etatens fysiske lokaler.

6. TILGANGSKONTROLL

Vil si å styre og kontrollere tilgang til informasjon og informasjonssystemer for å hindre uautorisert tilgang og sikre autorisert tilgang.

6.1 Virksomhetskrav til tilgangskontroll

6.1.1 Prinsipper for tilgangskontroll

Tilganger skal gis i henhold til prinsippet om tjenstlig behov. Medarbeidere skal kun gis de tilganger de trenger for å utføre sitt arbeid. Ut fra dette

- må tilgangskontrollen være tilstrekkelig presis og nøyaktig
- må tilgangsstrukturer ha fleksibilitet for endringer i organisering og oppgavedeling
- må tilganger kunne administreres effektivt
- må tilgang kunne differensieres ut fra de omgivelsene medarbeideren befinner seg i

6.1.2 Tilgang til nettverk og IT-tjenester

Medarbeidere skal kun gis tilgang til de IT-tjenester og de nettverk som er nødvendige for de oppgaver de gjør i sitt arbeid.

6.2 Administrasjon av brukeridenter og tilganger

6.2.1 Registrering og sletting av brukeridenter

Leder bestiller brukeridenter til sine medarbeidere og skal sørge for å sperre disse når medarbeidere slutter. Hver medarbeider skal i utgangspunktet ha kun en brukerident. Leder skal sikre at opplysninger for å identifisere medarbeideren er korrekte.

6.2.2 Tildeling av tilganger

Den ansvarlige for en informasjonsressurs eller et system er autorisasjonsmyndighet og fastsetter tilgangsregler og rutiner for autorisasjon. Det skal ajourføres en oversikt over hvem som innehar autorisasjonsmyndighet slik at de som skal registrere tilganger vet hvem som er berettiget til å autorisere.

Det skal være klart definert hvem som er ansvarlig for å autorisere en medarbeiders tilgang til informasjonsressurser. Som hovedregel ligger ansvaret til nærmeste leder eller prosjektleder. Autorisasjonsrutiner skal være dokumenterte. Leder kan delegere bestillingsoppgaver til andre medarbeidere i egen enhet, f.eks. en identadministrator. Tildelte tilganger skal være begrunnet i tjenstlig behov. Tildeling og fjerning av tilganger skal være dokumentert.

6.2.3 Kontroll med utvidede tilganger

Tildeling av privilegerte tilganger (systembrukere og systemroller med utvidede tilganger) skal skje kun til medarbeidere som leder finner skikket til dette og har tjenstlig behov.

6.2.4 Kontroll med hemmelig autentiseringsinformasjon

Autentiseringsinformasjon må ha sikker kryptering ved lagring og forsendelse. Den skal ikke gjøres kjent for andre enn den som trenger å kjenne autentiseringsinformasjonen.

6.2.5 Gjennomgang av tildelte tilganger

Alle ledere med personalansvar skal årlig foreta en gjennomgang av at tildelte tilganger er i tråd med tjenstlig behov.

6.2.6 Justering og fjerning av tilganger

Overflødige tilganger som en medarbeider har skal fjernes. Er tilgangen for vid, og det foreligger mer egnet tilgangsalternativ, må tilgangen justeres for mer nøyaktig å dekke tilgangsbehovet.

6.3 Medarbeiders ansvar for tilgangskontroll

6.3.1 Kontroll med hemmelig autentiseringsinformasjon

Brukerident og passord er personlig. Flere medarbeidere skal ikke bruke samme brukerident og passord skal ikke gjøres kjent for andre.

6.4 Identitets- og tilgangskontroll i systemer

6.4.1 Inndeling av tilganger til informasjon og funksjonalitet

Tilganger til informasjon og funksjoner skal deles inn slik at tilganger kan gis så nært opp til tjenstlig behov som mulig.

Tilgangskontroller skal ha styrke (robusthet) alt etter klassifiseringsnivået på det som skal beskyttes.

6.4.2 Identitetskontroll

Enhver som skal ha tilgang til informasjon i et system skal være entydig identifisert og forsvarlig autentisert før tilgang gis.

Autorisasjonsrutinene for de ulike systemer og informasjon må samordnes. Identitetskontroll til systemene bør i størst mulig grad gjenbrukes. For eksempel ved bruk av samme ident.

6.4.3 Passordhåndteringssystem

Ved bruk av passordhåndteringssystemer skal det sikres at passordene har tilstrekkelig styrke og at det er tilgangskontroll som sikrer at de er tilgjengelige kun for de som er autorisert til dem.

6.4.4 Bruk av programvare med sterke privilegier

Bruk av privilegerte tilganger skal kun skje til operasjoner som krever dette og i henhold til tjenstlig behov. Bruk av slike tilganger skal logges og loggen skal gjennomgås regelmessig.

6.4.5 Beskyttelse av kildekode

Tilgang til kildekode for tilgangsmekanismer skal være autorisert og endringer skal bare kunne gjøres av autoriserte personer.

7. KRYPTOGRAFI

Vil si å sikre konfidensialitet og integritet i informasjon.

7.1 Sikkerhet for kryptografi

7.1.1 Bruk av kryptografi og elektronisk signaturer

- For å sikre konfidensialitet skal informasjon som er taushetsbelagt eller har et særskilt beskyttelsesbehov krypteres når de sendes i usikrede kanaler.
- Når vi har behov for å ha sikkerhet om hvem som er avsender og å oppdage om det er skjedd endringer under overføring skal informasjon signeres elektronisk.
- Bruk av PKI skal skje i samsvar med kravspesifikasjon for PKI i offentlig sektor.

7.1.2 Nøkkelhåndtering

- Lagre av nøkler må minst ha så høy sikkerhet som den informasjonen nøklene skal beskytte
- Nøkler må administreres i henhold til beste praksis for å unngå at nøkler kommer på avveie
- Eventuelle nøkler på avveie skal gjøres ubrukelige

8. FYSISK OG MILJØMESSIG SIKKERHET

Vil si å sikre autorisert adgang til etatens lokaler og informasjon slik at tyveri, innbrudd, misbruk, skade og forstyrrelse forhindres. Etatens lokaler skal sikres slik at medarbeidere og brukere i våre lokaler skal være trygge.

8.1 Sikre områder

8.1.1 Fysisk sikkerhet

Vi skal sikre våre lokaler og eiendeler på en slik måte at mennesker ikke kommer til skade eller at informasjon og utstyr ikke ødelegges eller kommer på avveie på grunn av uhell, tyveri eller sabotasje.

8.1.2 Fysisk adgangskontroll

Etatens lokaler skal være inndelt i ulike fysisk sikrede områder. Det skal etableres hensiktsmessig adgangskontroll for å sikre at kun autoriserte medarbeidere får adgang til de ulike områdene i NAVs lokaler som ikke er åpne for publikum. Fysisk adgang skal tildeles i tråd med prinsippet om tjenstlig behov.

8.1.3 Sikring av kontorlokaler og områder med publikumskontakt

Alle etatens lokaler skal være sikret med rømningsveier i tilfelle brann eller annet behov for at medarbeidere eller besøkende skal kunne rømme. Publikumsarealene skal utformes slik at medarbeidere og andre tilstedeværende blir beskyttet mot aggressive brukere. Publikumsarealene må utformes slik at brukeren i sin dialog med veileder er sikret mot at taushetsbelagt informasjon enkelt kan overhøres av andre som oppholder seg i lokalet.

Utgangspunktet for arbeidet med dette skal være «Minimumsstandarden med krav til fysisk utforming og sikring av NAV-kontor». Standarden revideres årlig. Alle NAV-kontor skal vurdere sine lokaler opp mot denne standarden og i samarbeid med kommunen bli enige om nødvendige tiltak. Kravene skal bidra til å øke tryggheten for ansatte og brukere som befinner seg i kontorlokalene.

Det er naturlig at også andre enheter som har brukerkontakt, vurderer sine lokaler og sikkerhetstiltak opp mot de delene av standarden som er relevant for dem.

Enheter med ambulante tjenester skal utarbeide egne rutiner for sikring av personell på oppdrag utenfor enhetens lokaler.

8.1.4 Beskyttelse mot eksterne og miljømessige trusler

Etatens lokaler skal ha hensiktsmessig beskyttelse mot skader ved brann, oversvømmelse, jordskjelv, eksplosjon, terrorhandlinger og andre former for naturlige eller framkalte ulykker.

8.1.5 Arbeid i sikrede områder

Arkiv og serverrom og andre områder som skal ha begrenset adgang, betegnes som sikrede områder. Tilgang til sikrede områder skal begrenses til ansatt personell med tjenstlig behov.

Områder med spesielle behov for sikring, kan ha egne retningslinjer for arbeid og adgang i lokalene og særskilte fysiske beskyttelsestiltak.

8.1.6 Områder for varelevering og varemottak

Det skal være kontroll med områder som er avsatt til varemottak for å hindre uautorisert adgang til lokalene.

8.2 Utstyr

8.2.1 Plassering og beskyttelse av utstyr

Etatens utstyr skal plasseres og beskyttes slik at det sikres mot skade og uautorisert bruk.

8.2.2 Støttetjenester for drift av IT-løsninger

Etaten har ansvar for å påse at funksjoner og støttetjenester som er plassert utenfor etatens ordinære lokasjoner er sikret etter samme retningslinjer som de med plassering inne i etatens lokasjoner. Eksempelvis eksterne leverandører av datalinjer, strøm osv.

8.2.3 Kablingssikkerhet

Kabling og annen infrastruktur skal sikres mot brudd og skade for å sikre uforstyrret drift.

8.2.4 Fjerning av eiendeler

Informasjonsressurser skal ikke fjernes fra etatens lokaler uten autorisasjon og skal ha sikring mot eventuelt tap av data.

8.2.5 Sikker avhending og gjenbruk

Utstyr skal avhendes sikkert og forsvarlig, etter formelle, dokumenterte og anerkjente prosedyrer, når det ikke lenger er behov for dem.

8.2.6 Utstyr uten tilsyn

Etatens eiendeler og utstyr som er plassert uten at de er bevoktet eller har tilsyn skal sikres særskilt mot tyveri, skade eller uautorisert bruk.

8.2.7 Orden på arbeidsplassene

Den enkelte medarbeider skal holde sin arbeidsplass ryddig og påse at dokumenter eller lagringsmedia med taushetsbelagte opplysninger ikke forsvinner, blandes sammen eller kommer uvedkommende i hende.

9. DRIFTSSIKKERHET

Vil si å sikre korrekt og stabil drift av informasjonsbehandlingsutstyr, redusere risikoen for systemfeil og uautorisert tilgang til konfidensiell informasjon samt hindre uberettigede endringer av informasjon og programvare.

9.1 Dokumenterte driftsprosedyrer og ansvarsforhold

For å sikre stabil drift skal driftsoppgaver knyttet til NAVs IT-systemer og infrastruktur utføres i henhold til dokumenterte driftsprosedyrer. Driftsprosedyrene skal beskrive detaljert utførelsen av hver enkelt oppgave. Dokumentasjonen av driftsprosedyrer skal være oppdaterte og være tilgjengelige for de som er autorisert og har behov for tilgang.

9.1.1 Endrings- og versjonskontroll

Endringer i IT-utstyr og applikasjoner skal kontrolleres ved hjelp av dokumenterte, formelle prosedyrer for endringskontroll.

9.1.2 Kapasitetsstyring

Bruk av informasjonsressurser skal overvåkes og det skal foretas beregninger over framtidige kapasitetsbehov for å sikre at etatens systemer oppnår påkrevd ytelse.

9.1.3 Adskillelse av miljøer for testing, utvikling og produksjon

Systemer og IT-utstyr for utvikling, testing, opplæring og produksjon skal holdes adskilt.

Oppgaver med og tilganger til produksjonsmiljø og testmiljø skal være adskilt der dette er mulig.

9.2 Beskyttelse mot skadelig programvare

9.2.1 Tiltak mot skadelig programvare

Det skal være kontroll med flyt av data til og fra interne nettverk og utstyr. All dataflyt som tillates gjort til og fra etatens nettverk og utstyr skal skannes for å luke ut skadelig programvare.

Det skal sikres at det ikke er mulig å installere skadelig programvare. I tillegg må det sikres at skadelig programvare ikke kan gjøre skade dersom den passerer etablerte sperrer.

Det skal etableres overvåking slik at skadelig programvare i etatens nettverk og utstyr blir avdekket.

Etaten skal ha sikringstiltak for gjenoppretting etter å ha vært utsatt for ødeleggende programkode.

9.3 Sikkerhetskopiering

9.3.1 Sikkerhets- og beredskapskopiering av informasjon

Tilgjengelighet til informasjon og programvare skal sikres:

- Sikkerhetskopier sikrer mot tap av data eller feil i normal drift, dvs. når alle våre systemer og infrastruktur er tilgjengelig
- Beredskapskopier sikrer gjenopprettelse ved driftsavvik der deler av systemer og infrastruktur er skadet eller ikke tilgjengelig
- Kopiering skal skje regelmessig og testes jevnlig
- Oppbevaringstiden for data og systemer skal bestemmes ut fra lover og forskrifter

9.4 Logging og sikkerhetsovervåking

9.4.1 Hendelseslogging

Sikkerhetshendelser og viktige ordinære hendelser skal logges. Alarmering skal skje der en hendelse er så alvorlig at den må håndteres raskt. Varsling skal skje når det kan være behov for vurdering av hendelsen i ettertid.

Det skal fastsettes lagringstid for hendelseslogger for å sikre framtidig oppfølging eller kontroll. Loggene skal oppbevares i henhold til dette.

9.4.2 Beskyttelse av logger

IT-utstyr og systemer som benyttes til logging og til lagring av logginformasjon skal beskyttes mot manipulering og uautorisert tilgang. Logger som skal kunne benyttes som bevis for hendelser skal sikres slik at det kan dokumenteres at de ikke er blitt manipulert.

9.4.3 Logging av administrator- og systemoperatøraktiviteter

Bruk av administratortilganger og systemoperatøraktiviteter er viktige hendelser som skal logges. Særskilt skal bruk av kommandoer med sterkere privilegier loggføres og kontrolleres.

9.4.4 Synkronisering av klokker

Logging, sikkerhetsfunksjonalitet og samhandling mellom systemer er avhengig av en felles nøyaktig tidsangivelse. Systemklokkene i alle relevante systemer og IT-utstyr som behandler informasjon skal synkroniseres med en autoritativ kilde til tid.

9.5 Kontroll med systemdriftsprogramvare

9.5.1 Rutiner for installasjon av programvare i produksjonsmiljø

- Installasjon av programvare i produksjonssystemer skal følge dokumenterte rutiner
- Det skal være dokumenterte rutiner for konfigurasjonsstyring og det skal finnes en oversikt over konfigurasjonen av systemer og komponenter
- Det skal være skille og klare rutiner for flytting av kode mellom ulike miljøer som utvikling, test, brukertest og produksjon for å understøtte integritet, validitet og kvalitet i programvare, parametere og konfigurasjonsdata.

9.6 Beskyttelse mot tekniske sårbarheter

9.6.1 Håndtering av tekniske sårbarheter i systemer

Det skal være dokumenterte rutiner for sikkerhetspatching av programvare.

Det skal være rutiner for å gjøre seg kjent med sikkerhetsutfordringer i programmer og utstyr vi bruker. Informasjon om sikkerhetstilstand, inkludert sikkerhetsmessige mangler og tekniske sårbarheter, skal ajourholdes av de som er ansvarlig for systemenes sikkerhet. Det skal gjennomføres risikovurderinger av hvilke konsekvenser dette har for NAVs bruk.

9.6.2 Restriksjoner på programvare og utstyr som kan brukes

Programvare som skal benyttes på NAVs plattformer skal være godkjent av NAV for bruk. IT-utstyr som skal brukes i NAVs nettverk skal være oppført i *Generell produktliste for NAV* (GPL).

9.7 Gjennomgang og oppfølging av IT-systemer

9.7.1 Gjennomføring av egenkontroll av IT-systemer

Det skal gjennomføres egenkontroll av de mest kritiske IT-systemer. Dette skal gjøres av de som er ansvarlig for sikkerheten for det enkelte system. Det innebærer både å vurdere sikkerheten ut fra etatens sikkerhetskrav og systemets klassifisering, samt en supplerende risikovurdering.

Mangler som framkommer skal det foreslås forbedringstiltak for. Disse skal inngå i tiltaksplaner med plassering av ansvar og realistiske frister for utbedring.

10. SIKKER KOMMUNIKASJON

Vil si å sikre informasjon i våre datanettverk og ved utveksling av informasjon med andre.

10.1 Nettverkssikkerhet

10.1.1 Sikring av nettverk

- Ansvar for sikring av nettverk skal gis til navngitt kontorsjef i IT infrastruktur- og plattformtjenester
- Personell som utfører konfigurasjon av nettverk skal ikke være de samme som opererer servere for andre formål.
- Det skal være sikkerhetsbarrierer som skiller ulike nettverk fra hverandre.
- Det skal være overvåking av trafikk for å avdekke uautoriserte trafikkmønstre.
- Når usikrede nettverk benyttes for å kople sammen nettverk på samme sikkerhetsnivå skal trafikken sikres mot avlesing.
- For delte nettverk, særlig de som strekker seg ut over virksomhetens ansvarsområde, skal medarbeiderne eller de eksterne konsulentenes muligheter til å kople seg til nettverket begrenses i samsvar med kravene til tilgangskontroll.

10.1.2 Sikring av nettverkstjenester

Sikkerhetsfunksjoner, tjenestenivåer og krav til administrasjon av alle nettverkstjenestene må identifiseres og inngå i avtaler om nettverkstjenester. Når disse tjenestene ytes av ekstern tjenesteleverandør skal dette inngå i formell avtale.

10.1.3 Inndeling av nettverk

Nettverk skal kunne deles opp i soner og undersoner med egnede kriterier for plassering av informasjonsressurser i sonene. Det skal sikres at kun nettverkstrafikk som er nødvendig kan passere mellom sonene. Tilgang til nettverkssonene skal følge av tilgangsbehovet til systemer og funksjoner i de enkelte nettverkssonene.

Driftsadministrasjon skal foretas fra separate nettverkssoner (Admin-soner), for ulike typer driftsadministrasjon. Driftsadministrasjon foretas i størst mulig grad i et såkalt Kontrollplan, separert fra et Brukerplan.

10.2 Informasjonsoverføring

10.2.1 Prinsipper og prosedyrer for informasjonsutveksling

Utveksling av informasjon mellom NAV og andre skal kun skje når det finnes rettslig grunnlag for dette. Utvekslingen skal skje slik at konfidensialitet, integritet og tilgjengelighet sikres i henhold til regler og avtalte betingelser.

10.2.2 Avtaler om informasjonsutveksling

Avtaler skal utarbeides når man skal utveksle elektronisk informasjon mellom etaten og eksterne parter.

10.2.3 Sikker elektronisk meldingsutveksling

Informasjon som utveksles elektronisk skal være tilstrekkelig beskyttet i forhold til konfidensialitet, integritet og tilgjengelighet. Kvalitet og sporbarhet skal også sikres.

Informasjon, funksjonalitet og tjenester som etaten tilrettelegger for sine brukere og for sine samarbeidspartnere, skal sikres for å unngå ufullstendig overføring, feilredigering, urettmessig tilgang til informasjon, funksjonalitet og tjenester.

10.2.4 Sikring mot uautorisert utlevering av informasjon

Når vi utleverer informasjon til andre skal vi avklare at vi har rett til å utlevere den og sikre i avtale om utlevering av informasjon at den ikke distribueres videre til tredjepart uten at vi har gitt tillatelse til dette.

11. SIKKER ANSKAFFELSE OG UTVIKLING AV IT-SYSTEMER

Vil si å påse at sikkerhet er en integrert del av anskaffelses-, utviklings- og forvaltningsprosesser for informasjonssystemer og datautstyr.

11.1 Sikkerhetskrav til IT-systemer

11.1.1 Krav til sikkerhet i analyse og spesifikasjon

Fagansvarlig har ansvaret for å påse at sikkerhet ivaretas i systemer de har eierskap til. Når det er behov for nye eller endrede IT-løsninger skal fageier beskrive behovet og gjøre en vurdering av personvernkonsekvenser og klassifisering av informasjon og prosesser som er berørt. Klassifiseringen skal angi skadepotensial dersom konfidensialitet, integritet eller tilgjengelighet ikke blir ivaretatt. Klassifiseringen skal danne grunnlag for at relevante krav til sikkerhet skal kunne stilles.

Før løsningsbeskrivelse utarbeides skal det kvalitetssikres at vurdering av personvernkonsekvenser og klassifisering er foretatt. Krav til sikkerhet skal deretter velges ut basert på disse og inngå i de samlede kravene til løsning.

Løsninger som etableres skal ivareta kravene etaten har til sikkerhet. Eventuelle avvik fra kravene skal dokumenteres og må aksepteres av de som får ansvar for konsekvensene.

Sikkerhetsseksjonen er fageier for sikkerhetsfunksjonalitet og skal godkjenne kravspesifikasjoner, løsningsforslag og design for slik funksjonalitet.

Sikkerhetsseksjonen skal godkjenne sikkerhetsrelaterte deler av brukerhistorier og kravspesifikasjoner for informasjonssystemer før tilbudsforespørsel sendes ut eller (ved egenutvikling) før utvikling tar til.

Krav til sikkerhet i applikasjoner inngår i felles kvalitetskrav til utvikling av IT-løsninger. Dette er krav til konfidensialitet, integritet og tilgjengelighet til prosesser som løsningen skal understøtte og informasjon som lagres og behandles i løsningen. Kravene skal være dokumentert og skal gi tilstrekkelig sikkerhet basert på fageiers klassifisering av skadepotensial, herunder kritikalitet. Til kvalitetskrav skal det følge en beskrivelse av hvordan de skal verifiseres på et så tidlig stadium som mulig i utviklingsprosessen.

11.1.2 Sikring av applikasjoner som er tilgjengelige i offentlige nettverk

Integriteten til data og informasjon som NAV gjør tilgjengelig gjennom applikasjoner i offentlige nettverk skal beskyttes slik at det ikke kan gjøres uautoriserte endringer.

Konfidensialiteten i løsningene må sikres slik at det ikke avsløres informasjon for uvedkommende.

Det skal gjennomføres verifikasjon av at våre systemløsninger som er tilgjengelige i åpne nettverk ikke lar seg kompromittere på grunn av feil eller kjente svakheter.

11.1.3 Beskyttelse av transaksjoner i applikasjonstjenester

Det skal etableres sikring av transaksjonsbehandling slik at transaksjoner blir behandlet korrekt og komplett og at det ikke oppstår feil i meldingsflyten i en verdikjede.

11.2 Sikkerhet i utviklings- og vedlikeholdsprosesser

11.2.1 Krav til sikkerhet i systemutvikling

Systemutvikling og forvaltning skal følge dokumenterte prosesser. Prosessene skal sikre en forsvarlig utvikling med etterlevelse av krav til personvern og informasjonssikkerhet.

11.2.2 Versjonskontroll og endringsstyring

Det skal etableres versjonskontroll av IT-systemer. Det skal være endringsstyring av versjonene slik at det er trygghet for at det er den riktige versjonen som testes og at det er den testede versjonen som settes i produksjon etter godkjent test.

Endringer relatert til funksjonelle sikkerhetskrav under utviklingen, skal avklares med Sikkerhetsseksjonen.

Etablering av versjoner og endringer som omfatter eller berører sikkerhetskrav skal dokumenteres. Dokumentasjonen skal være tilgjengelig for Sikkerhetsseksjonen.

11.2.3 Sikkerhetsmessig gjennomgang før produksjonssetting

Før produksjonssetting av løsninger og leveranser av ny sikkerhetsfunksjonalitet gir Sikkerhetsseksjonen en sikkerhetsmessig vurdering, mens IT-arkitektur tilsvarende gir en vurdering av kvalitetskrav, som skal ligge til grunn for fageiers godkjenning og helhetlige risikovurdering av løsningene. Eventuelle avvik og mangler skal følges opp med kompenserende tiltak slik at risikoen blir på et akseptabelt nivå.

Informasjon om tekniske sårbarheter skal dokumenteres. Etter at testing mht. sikkerhet er gjennomført, skal det gjennomføres en risikovurdering der relevante og vesentlige scenarier gjennomgås og nødvendige tiltak beskrives.

11.2.4 Begrensninger i endringer av programvarepakker

Modifiseringer i standard programvare, såkalt hyllevare, skal begrenses til nødvendige endringer. Ved alle slike endringer skal det verifiseres at sikkerhetskravene fortsatt er oppfylt.

11.2.5 Prinsipper for sikker systemutvikling

Systemutvikling skal skje på en sikker måte. Det må sikres at det ikke legges inn skadelig eller irrelevant kode i systemene og at programbiblioteker som tas i bruk ikke er manipulerte eller inneholder skadelig eller irrelevant kode.

11.2.6 Sikre utviklingsmiljøer

Utviklingsmiljøet i NAV skal sikres for å unngå uautorisert tilgang eller endringer i kode og hindre tap eller skade på ferdig kode eller kode under utvikling.

11.2.7 Systemutvikling utført av eksterne

NAV skal overvåke og følge systemutviklingsoppgaver som er satt ut til eksterne. De produkter og tjenester etaten mottar fra tredjepart skal inspiseres og verifiseres.

11.2.8 Sikkerhetstesting av systemer

- Sikkerhetskravene skal testes gjennom de ulike stadier i utviklings- eller endringsprosessen.
- Produkter og tjenester etaten mottar fra tredjepart skal inspiseres og verifiseres mot sikkerhetskravene i den underliggende kravspesifikasjonen.
- Ved utvikling av ny sikkerhetsfunksjonalitet skal Sikkerhetsseksjonen ha testplaner til uttalelse og forelegges testrapport.
- Samfunnskritiske og virksomhetskritiske applikasjoner skal ved alle endringer spesielt testes for å sikre at endringen ikke får negative følger for NAVs drift eller sikkerhet.

11.2.9 Akseptansetest av systemer

Test og aksept av løsninger skal skje på bakgrunn av testkrav blant de krav til sikkerhet som gjelder for løsningen. Testing skal dokumenteres i testrapporter. Her skal det fremgå hvordan krav til sikkerhet er ivaretatt og testet. Dersom det oppdages avvik eller svakheter i testen skal det dokumenteres hvordan dette påvirker risikoen til IT-systemet og hvordan dette skal håndteres.

11.3 Testing og testdata

11.3.1 Beskyttelse av testdata

Testmiljøer skal sikres slik at:

- testing i hovedsak ikke skjer ved bruk av reelle personopplysninger
- opplysninger som kan knyttes til reelle personer beskyttes mot uautoriserte oppslag i miljøer for test, utvikling og opplæring
- data til test har tilstrekkelig kvalitet til at testene sikrer systemenes korrekthet
- data og miljøer for test, utvikling og opplæring ikke forveksles med reelle data henholdsvis produksjonsmiljø

12. LEVERANDØRSTYRING

Vil si å sikre NAVs informasjon og verdier som er tilgjengelig for leverandører og å sikre et avtalt nivå for sikkerhet i tjenesteleveranser.

12.1 Informasjonssikkerhet i leverandørrelasjoner

12.1.1 Prinsipper for sikkerhet i leverandørrelasjoner

Etatens sikkerhetskrav gjelder også for tjenester etaten kjøper og for de personene som utfører disse tjenestene.

12.1.2 Sikkerhetskrav i avtaleverk

Sikkerhetskrav skal innarbeides i anbudsdokumenter og avtaler med leverandører. Det skal alltid vurderes om det skal utarbeides en tjenestenivåavtale for sikkerhet. Bruk av underleverandører skal dokumenteres.

I tilfeller der leverandøren behandler personopplysninger på vegne av etaten skal det inngås en skriftlig databehandleravtale. Der leverandøren behandler eller har tilgang til etatens informasjon fra andre land, må det sikres at juridisk og kontraktmessig ansvar for å beskytte informasjonen er ivaretatt.

12.1.3 Informasjonssikkerhet i tjenesteleveransene

Det skal sikres at leverandører innfører, foretar og vedlikeholder sikkerhetskontrollene, tjenestedefinisjonene og leveringsgraden som er avtalt.

12.2 Sikkerhet i leverandørstyring

12.2.1 Overvåking og gjennomgang av tjenesteleveranser

Tjenester, rapporter og oversikter som leveres av tredjepart, skal overvåkes og gjennomgås regelmessig.

12.2.2 Endringsstyring av leverandørtjenester

Endringer i tjenesteyting skal administreres slik at det tas hensyn til kritiske aspekter ved systemene og prosessene som inngår. Ved vesentlige endringer foretas en revurdering av risiko og krav til sikkerhet.

13. SIKKERHETSHENDELSER OG AVVIK

Vil si å identifisere sårbarheter og avvik som har eller kan ha betydning for sikkerheten. Hensikten er å benytte dette til preventive tiltak for å hindre fremtidige sikkerhetsavvik og begrense eventuelle skadevirkninger.

Avviksrapportering må ikke forveksles med varsling av krisehendelser. Til slik varsling benyttes egen varslingsprosedyre beskrevet i den enkelte beredskapsplan.

13.1 Styring av sikkerhetshendelser og forbedringsaktiviteter

13.1.1 Definert ansvar og oppgaver knyttet til avvikshåndtering

Bruk av informasjonssystem i strid med fastlagte rutiner samt andre sikkerhetsbrudd skal behandles som avvik. Resultatet av avviksbehandlingen skal registreres.

13.1.2 Rapportering av sikkerhetshendelser

Alle medarbeidere er ansvarlige for å rapportere sikkerhetshendelser og avvik som de oppdager eller blir gjort kjent med til enhetsleder. Sikkerhetshendelser og avvik skal rapporteres så snart som mulig gjennom avviksrapporteringssystemet (ASYS).

13.1.3 Rapportering av sikkerhetssvakheter

Innrapporterte sikkerhetssvakheter rapporteres og kategoriseres i avvikssystemet på lik linje med sikkerhetshendelser.

13.1.4 Håndtering av sikkerhetshendelser

Den enkelte sikkerhetshendelse skal håndteres av nærmeste leder hvor håndtering av hele hendelsen ligger innen eget ansvarsområde. Avvik utenfor eget myndighetsområde eskaleres i linjen.

13.1.5 Læring fra avvikshendelser

De samlede sikkerhetsavvikene og -svakhetene skal systematiseres og analyseres periodisk. Analysen skal benyttes som grunnlag for risikostyring på sikkerhetsområdet og til informasjon for felles læring for å forebygge sikkerhetshendelser.

13.1.6 Dokumentering av bevis

For å sikre bevis ved interne granskninger eller ved mulig straffesak som følge av sikkerhetsbrudd, skal databevis sikres på en slik måte at databeviset har størst mulig selvstendig bevisverdi i henhold til gjeldende lover og regler.

14. KONTINUITET OG BEREDSKAP

Vil si å være forberedt på å kunne takle uforutsette alvorlige hendelser og katastrofer. Her legges det vekt på å beskytte, skjerme og sikre mennesker og verdier samt å sørge for kontinuitet i driften. Dette kan også innebære å etablere reserveløsninger for eventuelle avbrudd i etatens kritiske virksomhets- og driftsprosesser samt å sikre at de gjenopptas i tråd med de rammer som er avtalt for informasjonssystemene

14.1 Kontinuitet i informasjonssystem

14.1.1 Planlegging for kontinuitet i IT-tjenester

Krav til tilgjengelighet (oppetider) skal være dokumentert for alle IT-tjenester. IT-systemer er klassifisert etter kritikalitet ved brudd på tilgjengelighet. Basert på disse kravene og klassifiseringene skal det lages planer for å sikre kontinuerlig tilgjengelighet innenfor disse tidene.

Kritikalitetsklassifiseringen og liste over prioriterte NAV-tjenester sammen med interne avhengigheter er styrende for rekkefølgen gjenoppretting skal skje i ved driftsavbrudd.

14.1.2 Implementering av kontinuitetstiltak

Ved avvik på krav til tilgjengelighet og basert på risikovurderinger skal det etableres tiltak for å sikre mest mulig kontinuitet i tilgjengelighet i tråd med behovene som er definert for IT-tjenester og systemer.

14.1.3 Verifikasjon av kontinuitetstiltak

Funksjoner for å sikre kontinuitet og rutiner for gjenopprettelse av stabil drift skal gjennomgås og testes regelmessig. Tilgjengelighet til IT-tjenester og systemer skal måles opp mot definerte krav.

14.2 Redundans

14.2.1 Tilgjengelighet i driftsmiljøer

For å sikre tilgjengelighet på sentrale IT-løsninger skal NAV operere med to adskilte driftssteder slik at man er i stand til å drifte løsningene selv om et av stedene skulle være utilgjengelig.

Dublering av datalinjer, strømforsyning og lagring skal vurderes for kritisk infrastruktur. En dublering må etableres slik at de separate løsningene i så liten grad som mulig kan rammes av en felles feil eller hendelse.

14.3 Beredskap

14.3.1 Beredskapsplaner og beredskapsorganisasjon

I alle NAV-enheter skal det til enhver til foreligge oppdaterte beredskapsplaner. Oppgaver og ansvar som er fordelt i planverket skal være kjent blant de involverte og det skal være rutiner for å utpeke stedfortredere for de som har roller i beredskapsplanen. Planverket skal gjennomgås årlig med tanke på endring i trusselbildet og erfaring fra gjennomførte øvelser.

Beredskapsplaner skal omfatte håndtering av hendelser som kan ramme samfunnet og som påvirker ekstraordinære behov for NAVs tjenester eller utfordrer NAVs mulighet til å levere disse på tid, ulykker og andre alvorlige hendelser som kan ramme Arbeids- og velferdsforvaltningen. Beredskapsplanene skal omfatte vold og trusselhendelser i enhetene og være i tråd med HMS-rutine 2: Forebygging og oppfølging av vold og trusler. NAV har også et særskilt ansvar for arbeidskraftberedskap som også skal omfattes av beredskapsplanene.

Beredskapsplaner for direktoratet skal ta høyde for at de oppgaver og ansvar som NAV har i følge Sivilt beredskapssystem (SBS) er ivaretatt. Beredskapsplanene for fylkeskontorene skal omfatte de oppgaver man påtar seg i samarbeidet med Fylkesmannens beredskapsutvalg.

NAV-kontorene skal samhandle med kommunal beredskapsorganisasjon for å sikre at oppgaver som NAV-kontoret får fra kommunen i krisesituasjoner kan håndteres og for å kunne sikre evt. felles beredskapsfunksjoner og støtte til NAV-kontorets beredskapsplan.

Sikkerhetsseksjonen koordinerer søknader knyttet til fritaksordningen fra mobilisering for medarbeidere i Arbeids- og velferdsetaten.

14.3.2 Trening i beredskapsarbeid

Evnen til å håndtere beredskapssituasjoner skal trenes på alle nivåer i etaten gjennom regelmessige beredskapsøvelser.

14.3.3 Evaluering etter øvelser og beredskapshendelser

Alle øvelser og reelle beredskapshendelser skal evalueres.

15. ETTERLEVELSE

Vil si å sikre at lover, forskrifter og avtaleforpliktelser etterleves og sikre samsvar med etatens styrende dokumenter for sikkerhet.

15.1 Etterlevelse av lover, regler og kontraktsforpliktelser

15.1.1 Identifisering av lov- og kontraktsforpliktelser

Sikkerhetsseksjonen skal ajourholde oversikt over lover, forskrifter og kontraktsmessige forpliktelser som regulerer sikkerhetsområdet. Oversikt over relevante lover og forskrifter innenfor sikkerhetsområdet er dokumentert i vedlegg A.

15.1.2 Beskyttelse av opphavsrett og intellektuelle rettigheter

Bruksrett, eiendomsrett og disposisjonsrett til programvare som brukes i NAV skal være dokumentert i kjøps- og bruksavtaler.

15.1.3 Beskyttelse av regnskap og dokumentasjon

Økonomireglement for staten gir retningslinjer for sikring av regnskap og regnskapsdokumentasjon. Arkivloven regulerer sikring av dokumenter i elektroniske og papirbaserte arkiver. Det er egne krav og rutiner knyttet til dette ut over de som er gitt i styringssystemet for sikkerhet.

15.1.4 Beskyttelse av personopplysninger og personvern

Overholdelse av personvernlovgivningen er beskrevet i kapittel 1 om Personvern.

15.1.5 Regelverk for kryptografi

NAVs bruk av kryptografi skal være i henhold til kravspesifikasjon for PKI i offentlig sektor og E-forvaltningsforskriften og E-signaturloven.

15.2 Sikkerhetsgjennomganger

15.2.1 Uavhengig gjennomgang av informasjonssikkerhet

Internrevisjonen gjennomfører uavhengige sikkerhetsgjennomganger (revisjoner iht. godkjent revisjonsplan) for NAV. I tillegg vil sikkerhetsområdet være gjenstand for revisjon og kontroll fra Riksrevisjonen og tilsyn og kontroll fra Datatilsynet og Nasjonal sikkerhetsmyndighet.

15.2.2 Etterlevelse av prinsipper og sikkerhetskrav

Alle enheter skal gjennomføre egenkontroll og kontrollaktiviteter for å dokumentere og sikre at enhetens arbeid samsvarer med etatens sikkerhetskrav. Sikkerhetsseksjonen gjennomfører en årlig spørreundersøkelse til lederne av enhetene for å dokumentere egenkontrollen.

For å verifisere etterlevelse og skaffe kunnskap om sikkerhetstilstanden og sikkerhetsutfordringer i etaten skal det hvert år gjennomføres sikkerhetsbesøk ved et utvalg av NAVs enheter eller andre virksomheter som er underlagt NAVs sikkerhetsregime.

Sikkerhetsbesøkene skal gjennomføres på en felles måte, og det skal lages en rapport fra hvert besøk med tiltak på lokalt og sentralt nivå for å ha tilfredsstillende sikkerhet og etablere forbedringer av hvordan NAV arbeider med sikkerhet.

Etaten skal følge opp at etatens databehandlere etterlever de krav som er satt til personvern og sikkerhet i databehandleravtalene. Den som har ansvaret for behandlingen som skal foregå, skal inngå en slik avtale skriftlig og skal påse at vilkårene i avtalen etterleves.

Funn og erfaringer fra egenkontroll, sikkerhetsbesøk og avvikssystem benyttes som grunnlag for ledelsens gjennomgang på sikkerhetsområdet og til å oppdatere det overordnede risikobildet på sikkerhetsområdet.

Sikkerhetsseksjonen skal samarbeide med internrevisjonen slik at gjennomføring av sikkerhetsbesøk blir mest mulig fordelt utover i organisasjonen. Internrevisjonen bygger sin vurdering på rapporteringen fra Sikkerhetsseksjonen.

15.2.3 Gjennomgang av etterlevelse av tekniske krav

Informasjonssystemene bør kontrolleres jevnlig for å sikre at de er i samsvar med vedtatte sikkerhetsstandarder og krav.

VEDLEGG A: RELEVANTE LOVER, FORSKRIFTER OG REGELVERK

Det stilles krav til sikkerhet i en rekke lover og forskrifter. Tabellen nedenfor gir en oversikt over de mest sentrale bestemmelser på nasjonalt nivå som Arbeids- og velferdsetaten må forholde seg til på sikkerhetsområdet. Oversikten er ikke uttømmende.

Relevante lover forskrifter og regelverk	Formål med regelverket	Relevans for sikkerhet i Arbeids- og velferdsetaten?
Personopplysningsloven og personopplysningsforskriften	Sikre personvernet til bruker gjennom korrekt og sikker behandling av personopplysninger.	Krav til behandling av personopplysninger og ivaretakelse av registrertes personvernrettigheter. Krav til melde- og konsesjonsplikt til Datatilsynet. Krav til internkontroll og gjennomføring av planlagte og systematiske tiltak. Krav til sikring av personopplysninger.
Forvaltningsloven	Loven skal sikre rettssikkerhet for den enkelte og rett saksbehandling i den enkelte sak.	Krav til taushetsplikt, habilitet, partsinnsyn, rettsanvendelse, saklig grunnlag mm, Rettsgrunnlag for dispensasjon fra taushetsplikten for utlevering av opplysninger fra NAV til forskningsformål.
Forskrift om elektronisk kommunikasjon med og i forvaltningen (e-forvaltningsforskriften)	Sikker og effektiv elektronisk kommunikasjon med og i forvaltningen	Krav til fremgangsmåter, tjenester og produkter for å sikre autentisering, ikke-benekting integritet, konfidensialitet og tilgjengelighet.
Offentleglova med forskrifter	Legge til rette for åpenhet i forvaltningen og sikre merinnsyn. Legge til rette for viderebruk av offentlig informasjon.	Dokumenter skal ikke unntas offentlighet med mindre det er hjemlet i lov eller forskrift.
Lov om arbeids- og velferdsforvaltningen (NAV loven) med forskrifter	Legge til rette for en effektiv arbeids- og velferdsforvaltningen og sikre en samordnet anvendelse av lover som forvaltes av Arbeids- og velferdsetaten.	Definisjon av behandlingsansvaret i Arbeids- og velferdsetaten Krav til taushetsplikt Samarbeid, oppgave- og informasjonsdeling i det felles lokale NAV kontor Krav til beredskapsplaner og beordring ved krise.
Folketrygdloven med forskrifter	Sikre inntekt og kompensere for utgifter ved arbeidsløshet, fødsel, sykdom og alderdom.	Behandlingsgrunnlag for trygdeytelser og kontrollformål. Saksbehandlingsregler.
Arbeidsmarkedsloven med forskrifter	Inkluderende arbeidsliv og lav arbeidsledighet	Opplysningsplikt ovenfor Arbeids- og velferdsetaten uten hinder av taushetsplikt for offentlige og private aktører.
Lov om sosiale tjenester i NAV med forskrift	Fremme økonomisk trygghet for vanskeligstilte	Krav til beredskapsplan, journalføring og saksbehandling. Krav om taushetsplikt. Innhenting av opplysninger i samarbeid med klient.
Sikkerhetsloven med forskrifter	Legge forholdene til rett for effektivt å kunne motvirke trusler mot riket sikkerhet, ivareta den enkelte rettsikkerhet, grunnlag for kontroll med	Loven gjelder sikkerhetsgradert informasjon og eventuell skjermingsverdige objekter som Arbeids- og velferdsetaten har ansvaret for.

Relevante lover forskrifter og regelverk	Formål med regelverket	Relevans for sikkerhet i Arbeids- og velferdsetaten?
	forebyggende sikkerhetstjeneste	
Forskrift om informasjonssikkerhet	Forskriften har samme formål og virksomhet som sikkerhetsloven	Krav om utvikling, merking, forsendelse, oppbevaring og tilintetgjøring av kryptomateriell
Forskrift om personellsikkerhet.	Forskriften har samme formål og virksomhet som sikkerhetsloven	Krav og retningslinjer om sikkerhetsklarering og autorisasjon ihht sikkerhetsloven
Forskrift om sikkerhetsadministrasjon	Forskriften har samme formål og virksomhet som sikkerhetsloven	Sikkerhetsadministrasjon for å motvirke sikkerhetstruende virksomhet som sabotasje, spionasje og terrorhandlinger. Den stiller bl a krav til virksomhetens sikkerhetsorganisasjon og sikkerhetsleder.
Forskrift om sikkerhetsgraderte anskaffelser	Forskriften har samme formål og virksomhet som sikkerhetsloven	Ved anskaffelse av varer og tjenester skal anskaffelsesmyndigheten vurdere behovet for å sikkerhetsgradere anskaffelsen. Utvelgelse av leverandør for slik anskaffelse skal skje i samsvar med de alminnelige bestemmelser for forvaltningens anskaffelsesvirksomhet.
Forskrift om objektsikkerhet. (objektsikkerhets-forskriften)	Forskriften har samme formål og virkeområde som sikkerhetsloven	Grunnlag for å vurdere om noen av våre installasjoner skal klassifiseres som skjermingsverdig
Beskyttelsesinstruksen	Behandling av dokumenter som trenger beskyttelse av andre grunner enn nevnt i sikkerhetsloven.	Beskyttelsesgradene FORTROLIG og STRENGT FORTROLIG skal benyttes når dokument kan unntas offentlighet.
Arkivloven med forskrift	Trygge arkiv som har mulig kulturell, rettslig eller forvaltningsmessig verdi	Krav til fysisk sikring av arkivrom, organisering av arkivsystem, lagring og lagringsmedia samt rutiner for utlån
Åndsverkloven	Beskytte opphavsretten til den som skaper et åndsverk, herunder dataprogram	Krav til å ikke låne ut eller kopiere programvarelisenser. Kopiering til nødvendig, eget bruk er lovlig.
Arbeidsmiljøloven	Regulerer forholdet mellom arbeidstaker og arbeidsgiver	Krav til arbeidsmiljø og regulering av kontrolltiltak i virksomheten
Helseregisterloven	Informasjonsutveksling i helsetjenesten uten å krenke personvernet	Krav til planlagte og systematiske tiltak som sørger for tilfredsstillende informasjonssikkerhet.
Helse- og sosialberedskapsloven (helseberedskapsloven)	Beredskap for helse og sosialtjenesten	Gjelder for offentlig sosiale tjenester
E-signaturloven med forskrifter	Sikker og effektiv bruk av elektronisk signatur	Krav til kvalifiserte sertifikater og utstedere av disse samt fremstillingssystemer for e-signaturer.
Lov om offentlige anskaffelser	Effektiv ressursbruk ved offentlige anskaffelser.	Krav til god forretningsskikk, konkurranse, forutberegnelighet, gjennomsiktighet og etterprøvbarhet.
Reglement for økonomistyring i Staten	Sikre effektiv bruk av statlige midler slik at mål og resultatkrav oppnås.	Krav til styringsprinsipper, styringsinformasjon og internkontroll. Integritetskrav til informasjonen.
Folkeregisterforskriften	Utfyllende bestemmelser om Folkeregisteret	Hjemmelsgrunnlag for vedtak om adressesperre for trusselutsatte personer. Gradering etter Beskyttelsesinstruksen av adresseopplysninger i Folkeregisteret med kode 6 (STRENGT FORTROLIG) eller 7 (FORTROLIG). Bestemmelser om utlevering av slike opplysninger.

Relevante lover forskrifter og regelverk	Formål med regelverket	Relevans for sikkerhet i Arbeids- og velferdsetaten?
Forskrift om arbeidsgiver og arbeidstakerregisteret	Register som har til formål å tjene NAVs og andre offentlige virksomheters behov for opplysninger om arbeidsforhold.	Rettslig grunnlag for behandling av personopplysninger i sentralt register. Bestemmelser om hvem som har behandlingsansvar og hvem som skal ha tilgang til opplysningene. Bestemmelser om utlevering opplysninger om personer som har adressesperre kode 6 og 7.
Lov om arbeidsgivers innrapportering av ansettelsesforhold mm. (a-opplysningsloven) med forskrift	Elektronisk innrapportering fra arbeidsgiver til offentlige virksomheter om inntekt, arbeidsforhold og skatteopplysninger-	Rettslig grunnlag for EDAG ordningen. Regulerer tilgang til opplysningene. Bestemmelser om innsynsrett, Definisjon av behandlingsansvar for Fellestjenester.
Forskrift om utskriving av verneplikt (vernepliktsforskriften)	Sikre forsvaret stabil tilførsel av godt egnet personell, og bidra til Forsvarets operative evne gjennom en allmenn verneplikt.	Grunnlag for å behandle søknader om fritak fra tjeneste i Forsvaret for personer i NAV som dekker en samfunnskritisk funksjon.

VEDLEGG B: OVERSIKT OVER OPERATIVE SIKKERHETSKRAV

Operative retningslinjer beskriver *hvordan* sikkerhetskravene utføres og etterleves i praktisk handling.

Innenfor hvert fokusområde er det derfor utarbeidet ett eller flere dokumenter som omsetter overordnede krav til operative retningslinjer.. Oversikten oppdateres ved endringer. Ansvarlig for dette er IT-avdelingen v/Sikkerhetsseksjonen.

	Fokusområde	Operative retningslinjer
1	Personvern og taushetsplikt	Her vil det bli endringer ved innføring av styringssystem for Personvern 1 Brukers rett til innsyn v1.0 2 Melde og konsesjonsplikt for etatens behandling av personopplysninger v1.3 3 Navs praksis for håndtering av trusselutsatte brukere v1.3 4 Personvernerklæring - krav til elektronisk publikumsinformasjon om etatens behandling av personopplysninger v1.0 5 Planlegging og gjennomføring av etatens brukerundersøkelser overfor sluttbrukere v1.1 6 Autorisasjon for tilgang til person med STRENGT FORTROLIG adresse v1.3 7 Endring, oppdatering og sletting av personopplysninger v1.1 8 Bruk av trusselutsattes personopplysninger v1.0 9 Samtykke som behandlingsgrunnlag v1.0 10 Retningslinjer for lydopptak av telefonsamtale med bruker v1.0 11 Tiltak – databehandleravtaler v1.0
2	Ledelsens styring av sikkerhet	1 Helhetlig risikostyring på sikkerhetsområdet v1.1
3	Organisering av sikkerhetsarbeidet	Ingen operative retningslinjer på området
4	Personellsikkerhet	1 Sikkerhetsklarering og autorisasjon v1.1
5	Administrasjon av informasjonsressurser	1 Klassifisering - retningslinje v1.0 2 Klassifisering v1.0

	Fokusområde	Operative retningslinjer	
6	Tilgangskontroll	1	Autorisasjon v1.0
		2	Identitetskontroll v1.0
		3	Tilgangskontroll v1.0
		4	Brukeridenter og tilgangsrettigheter - rutiner for administrasjon v1.0
		5	Dokumentasjon - rollebeskrivelser fagsystemer v1.0
		6	Autorisasjon og tilgangskontroll for tiltaksdeltakere, studenter, hospitanter og personer under myndighetsalder v1.0
		7	Innsyn – Prosedyre for innsyn i logger v 1.0
7	Kryptografi		Ingen operative retningslinjer på området
8	Fysisk og miljømessig sikkerhet	1	Fysisk sikring - krav og retningslinjer v1.1
9	Driftssikkerhet	1	Sikkerhet i dokumentasjon av systemer v1.1
		2	Sikkerhetsovervåkning v1.2
		3	Tilgjengelighet v1.0
		4	Lagringsmedier - krav til sikring av utstyr og informasjon v1.0
		5	Oppsett av IT-maskin - med krav til herding med mer v1.0
		6	Kapasitetsplanlegging - krav til kapasitets- og ressursplanlegging v1.0
10	Sikker kommunikasjon	1	E-post - retningslinjer for bruk v1.0
		2	Prosedyre for sending av E-post med kryptert vedlegg
		3	Sikkerhetspolicy for nettverkssoner v1.2
		4	Elektronisk forsendelse v1.1
		5	Innhenting og mottak v1.2
		6	Utlevering og intern spredning v1.1
		7	Retningslinjer for databehandleravtaler v1.1
		8	E-post - krav til drift og oppsett av e-postsystem v1.0
		9	Søknad om tilgang til eksternt nettsted på tynnklient
		10	Retningslinjer for opplasting av informasjon fra Internet hjemmeområde Skrivbart til Internet
11	Anskaffelse, utvikling og vedlikehold av informasjonssystemer	1	Anskaffelse, utvikling og vedlikehold av IT - systemer v1.2
		2	Akseptansekriterier for idriftsettelse av endrede og nye systemer v1.0
		3	Sikkerhet i testmiljøer og for testdata v.1.0

	Fokusområde	Operative retningslinjer
12	Håndtering av underleverandører	Ingen operative retningslinjer på området
13	Håndtering av avvik og sikkerhetshendelser	1 Rapportering av avvik v1.0
14	Kontinuitets- og beredskapsplanlegging	1 Beredskapshåndbok for NAV 2 Fritak og utsettelse ved mobilisering v1.0
15	Etterlevelse av lover og regler	Ingen operative retningslinjer på området

VEDLEGG C: DEFINISJONER

Dette vedlegget inneholder definisjoner brukt i dette styringsdokumentet og underliggende dokumenter som angir krav og operative føringer. Vedlegget er ikke konsistenssjekket mot begrepskatalogen. Dette er arbeid som vil gjøres i en senere revisjon.

Alarmering	Varsling av hendelse for umiddelbar håndtering. En sikkerhetsalarm er det å sende informasjon om en sikkerhetshendelse til noe eller noen som forutsettes å reagere på alarmen.
Ansvar	Et sett med fullmakter (myndighet) og plikter innen et område.
Autentisering	Verifikasjon av at en person eller en datamaskinprosess er den som den utgir seg for å være. Kan skje ved forskjellige identifikasjonsmekanismer.
Autorisasjon	Bemyndigelse, godkjenning. Innen sikkerhet; tillatelse til å utføre visse oppgaver og/eller få tilgang til visse informasjonsressurser.
Autorisering	Å tildele autorisasjon innebærer å beslutte om tilgang skal gis for et subjekt til bestemt informasjon og funksjonalitet og hvilken type tilgang som skal gis (lese, skrive osv.)..
Beredskap	Evne til å håndtere og redusere skadevirkninger av uønskede hendelser som kan føre til skade på eller tap av verdier.
Digital signatur	Et dataelement som følger en elektronisk melding eller et dokument, og som knytter dokumentet til en person, en maskin eller et datasystem. Dette gjør det mulig for mottaker å finne bevis på hvor dokumentet kommer fra og om dokumentet er forfalsket. Normalt er dataelementet en hash-verdi for dokumentet, kryptert med en privat nøkkel, når PKI-løsning er i bruk. Denne bindingen er slik at signaturen er praktisk umulig å forfalske. Den kan verifiseres av en mottaker, eller av en uavhengig tredjepart, ved hjelp signererens tilhørende offentlige nøkkel. Hvis en bokstav i dokumentet endres og dokumentet re-signeres, vil både hash-verdi og kryptert verdi endres, og den digitale signaturen kan ikke godkjennes.
Elektronisk signatur	Data i elektronisk form som er knyttet til andre elektroniske data, og som brukes til å kontrollere at disse stammer fra den som fremstår som undertegner.
Formell fagansvarlig	Premissgiver og bestiller av tjenester. Ansvarlig for at akseptabelt sikkerhetsnivå basert på risikostyring opprettholdes, samt at krav til personvern er oppfylt for egne tjenesteområder.
Informasjonsaktiva	Informasjon og data som har verdi for etaten. Det gjelder også informasjonsbærere som IT-utstyr, arkiv, dokumenter og mennesker.

Informasjonssikkerhet	Tiltak som beskytter informasjonsaktiva mot ulike trusler og sårbarheter for å forebygge og redusere omfanget av skader. Oppnås gjennom ivaretakelse av konfidensialitet, integritet og tilgjengelighet.
Integritet	Integritet for informasjon innebærer at informasjonen, herunder endringer av informasjonen, er ekte (autentisk), kommer fra oppgitt og berettiget kilde, at innholdet er ekte, og at visse restriksjoner på informasjonen er oppfylt (krav til format og eventuelle integritetsrestriksjoner).
Internkontrollsystem	Tiltak som skal sikre og dokumentere at aktivitetene utøves i samsvar med krav fastsatt i medhold av lov, forskrift eller andre fastsatte eller avtale normer. Tiltakene skal være systematiske og dokumentert.
Ikke-benekting	Vedkjenning**.** *Engelsk: Non-repudiation*. Sikkerhet for at den som har sendt eller mottatt informasjon gjennom elektronisk meldingsformidling ikke kan nekte for dette i ettertid. Slik sikkerhet oppnås som regel ved hjelp av digitale signaturer.
IT-sikkerhetshendelse	En IT-sikkerhetshendelse, eller flere hendelser, beskriver at det har oppstått en situasjon hvor konfidensialitet, integritet eller tilgjengelighet *kan bli* kompromittert.
IT-sikkerhetsbrudd	Beskriver at det har oppstått en situasjon hvor konfidensialitet, integritet eller tilgjengelighet *er* kompromittert.
Katastrofe	En brå, uventet og skjebnesvanger hendelse som setter organisasjonen ut av stand til å utføre kritiske virksomhetsfunksjoner for en gitt periode, og som resulterer i stor skade og eller tap.
Konfidensialitet	Konfidensialitet for informasjon innebærer at uvedkommende ikke får tilgang til informasjonen. Dvs. at både personer og datamaskinprosesser, som ikke er berettiget tilgang til informasjonen, ikke får tilgang til den. For å ivareta konfidensialitet må tilgangskontroll, lagring, sending og mottak, sletting osv. gjøres forsvarlig.
Konsekvens	Mulig følge av uønsket hendelse. Konsekvenser kan uttrykkes med ord eller om en tallverdi for omfanget av skader på mennesker, miljø og materielle verdier.
Krise (krisesituasjon)	En hendelse som har potensial til å true viktige verdier og svekke en organisasjons evne til å utføre viktige funksjoner. Den kan oppstå plutselig, enten som følge av naturfenomener, menneskelige handlinger eller teknologisk svikt. En krise kan utvikle seg til en *katastrofe.*

Krisehåndtering	Betegnes som summen av de aktiviteter og tiltak som virksomheten gjennomfører på grunn av krisen for å sikre liv, helse, samfunnsviktige funksjoner og materielle verdier, begrense skadeomfang og bringe krisen til opphør.
Kritikalitet	Kritikalitet kan beskrives ved en skala som indikerer relativ viktighet av informasjonen eller informasjonssystemet i etaten, basert på hvor stor skade som kan oppstå ved brudd på konfidensialitet, integritet eller tilgjengelighet.
Kryptering	Omskrivning/koding av en tekst slik at uvedkommende ikke skal forstå den. Normalt skjer kryptering i henhold til faste algoritmer og nøkkelkoder som er avtalt mellom sender og mottaker.
PKI	«Public key infrastructure», som er systemer for å håndtere krypteringsnøkler via en tiltrodd tredjepart slik at informasjon kan sendes med beskyttelse for integritet og konfidensialitet.
Policy	I etaten benyttes policy som fellesbetegnelse for styringsprinsipper, krav og operative føringer som skal bidra til måloppnåelse.
Samfunnskritisk	Kritisk for samfunnet. Et informasjonssystem eller en infrastruktur er samfunnskritisk hvis samfunnets funksjonsevne i stor grad påvirkes av at systemet eller infrastrukturen ikke fungerer.
Sikringstiltak	Midler og handling for å beskytte et objekt slik at planlagt sikkerhet og akseptabel risiko oppnås. Inkluderer policy, prosedyrer, operative dokumenter, rutiner, kontrolltiltak og organisasjonsstrukturer.
Systemansvarlig	Leverandør som skal vedlikeholde systemet, levere tilpasninger og endringer i henhold til bestillinger og premisser.
Ressurs	Med ressurs menes alt som har verdi for Arbeids- og velferdsetaten. Dette kan være mennesker, eiendeler, informasjon, tjenester, omdømme, Software og/ eller hardware
Risiko	Risiko beskriver fare for tap, usikkert eller uberegnelig utfall av at en trussel materialiseres. I forbindelse med informasjonssikkerhet er risiko en funksjon av sannsynligheten eller muligheten for at en sikkerhetshendelse vil inntreffe og den forventede skadevirkningen hendelsen kan medføre. Risiko og sikkerhet blir ofte definert som komplementære størrelser, slik at den ene størrelsen kan beregnes ut fra den andre. Høy risiko tilsvarer lav sikkerhet, og omvendt.
Risikovurdering	Prosess som består av å identifisere risiko og sammenligne med gitte risikokriterier for å bestemme risikoens betydning.
Risikohåndtering	Prosess for å velge og iverksette tiltak som skal endre risiko.

Risikostyring	Koordinerte aktiviteter for å styre og kontrollere en virksomhet med hensyn til risiko. Omfatter typisk risikovurdering, risikohåndtering, risikoaksept og risikokommunikasjon.
Robusthet	Robustheten til et system er dets evne til å tåle påkjenninger (mestre trusler og sikkerhetshendelser).
Sikkerhet	Begrepet sikkerhet er i dette styringssystemet benyttet om hele personvern-, informasjonssikkerhets-, og beredskapsområdet
Sporbarhet	Et prinsipp som sikrer at behandlingen av en sak kan rekonstrueres i ettertid. Det skal være mulig å etterspore hva som har skjedd (audit trail). Sporbarhet oppnås for eksempel ved å anvende logging, som dokumenterer handlinger og hendelser og bidrar til at handlinger og hendelser lar seg rekonstruere i ettertid.
Sårbarhet	Sårbarheten for et system er et uttrykk for de svakheter og mangler som finnes i systemet og spesielle omstendigheter som øker sannsynligheten eller muligheten for at trusler vil materialisere seg i en sikkerhetshendelse. Sårbarheten reduseres ved å øke robustheten.
Tilgjengelighet	Tilgjengelighet til informasjon innebærer at informasjonen fins, og at berettigede brukere får tilgang til informasjonen når de har behov for det. Tilgjengelighet for system eller prosess innebærer at berettigede brukere får tilgang til system eller prosess og tilhørende informasjonsressurser når de har behov for det.
Trussel	En handling eller hendelse som kan fremkalle frykt, og som kan påføre et objekt tap eller skade dersom den inntreffer. I forbindelse med IT-sikkerhet er trusler ulike situasjoner som kan føre til at konfidensialitet, integritet og tilgjengelighet blir kompromittert.
Varsling	Å melde fra til ansvarlig person for vurdering av håndtering av en hendelse. Et varsel av en sikkerhetshendelse er det å sende informasjon om en sikkerhetshendelse til noe eller noen som forutsettes å vurdere hva som bør gjøres på grunnlag av hendelsen.

VEDLEGG D: INTERESSENTER TIL SIKKERHETSARBEIDET

For å sikre en best mulig forståelse av hvordan interessenter som berøres av NAVs sikkerhetsregime oppfatter og forholder seg til dette, er det viktig å ha kontakt med disse ved endringer i sikkerhetsregler og oppdatering av risikobildet. Nedenfor gis en oversikt over de viktigste interessenter i denne sammenheng. (Interessentanalysen er ikke uttømmende)

Interessent	**Interesseområde**	**Påvirkes av sikkerhet**	**Bidrar til Sikkerhet**
Brukere	Personvern og sikring av rask og korrekt behandling	Det er deres informasjon som behandles	
Medarbeidere	Personvern og sikring av rask og korrekt behandling	Informasjon om seg selv i systemene	Primære behandlere av informasjon
Ledere	Hvordan kunne ivareta sikkerhet for sin enhet og samtidig levere resultater som kreves	Begrensinger i sikkerhetsregi met	Ansvar for sikkerhet på eget område. Rollemodeller for etterlevelse.
Internrevisjonen	Kontroll med etterlevelse Interne misligholdsaker		Gjør uavhengige revisjoner
HR-avdelingen	Avvikshåndtering Trusler og vold Fysisk sikring		Gir kunnskap om erfarte trusler
Økonomi- og styringsavdelingen	Regimeansvar for risikostyring. Internkontroll/kvalitets-arbeid. Prosessmodellering. Virksomhetsstyring. Virksomhetsarkitektur. Utviklingsporteføljen	Utviklings-porteføljen må forholde seg til krav til sikkerhet	Felles risikostyring. Samordning av kvalitetsarbeid. Kartlegger prosesser i NAV som grunnlag for å målrette sikkerhet bedre
NAV Kontroll	Identitetskontroll Misbruk av ytelser		Innspill til risikoområder
Seksjon for informasjonsforvaltning	Informasjonsarkitektur		Angir kritikalitet og formål for informasjon i felleskomponenter
Arbeids- og sosialdepartementet	Beredskapshåndtering og personvern		Krav og føringer
Direktoratet for sivil beredskap	Beredskap og samfunnssikkerhet		Risikobilde og SBS
Nasjonal Sikkerhetsmyndighet	Beredskap og informasjonssikkerhet		Risikobilde
Datatilsynet	Personvern		Avklaringer og reguleringer