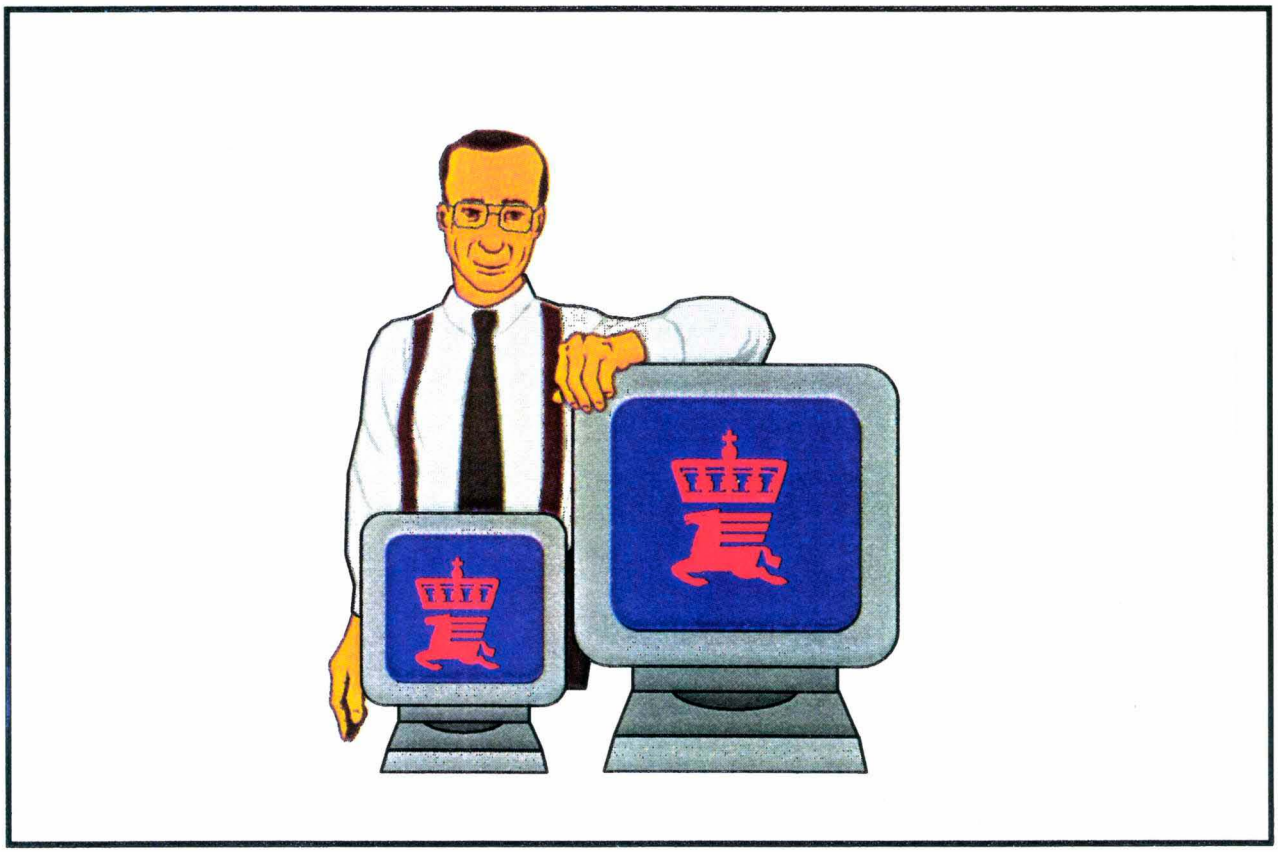
NOTAT

Nr 07
1995

NVE
NORGES VASSDRAGS-
OG ENERGIVERK

Erik Fagerberg (red.)

IT-SIKKERHETSDOKUMENTASJON



ADMINISTRASJONSAVDELINGEN

NVE
NORGES VASSDRAGS
OG ENERGIVERK

TITTEL Informasjonssikkerhet i NVE Sikkerhetsdokumentasjon	**NOTAT** DATO 27. juni 1995
FORFATTER Erik Fagerberg/Dataseksjonen(AD), Stein Bråthen/Avenir	

SAMMENDRAG

Denne dokumentasjonen er en del av NVEs komplette sikkerhetsdokumentasjon og omfatter de områder som er mest aktuelle for de fleste brukere av Informasjonsteknologi (IT).
Dokumentasjonen omfatter ikke de delene som berører den faglige drift av NVEs sentrale dataanlegg og datanett, ivaretatt av Datseksjonen (AD).

Innholdet består av:

- Policy-dokument fra NVEs ledelse.
- Generelle synspunkter på IT-sikkerhet.
- Avd.dir / seksjonssjefs spesielle ansvar.
- Ansvar tillagt alle IT-brukere.
- Hjelpetabell for kategorisering av data.
- Skjema for rapportering av sikkerhetsbrudd.
- Skjema for autorisering av nye brukere.
- Definisjoner av ord og uttrykk.

Denne dokumentasjonen er utarbeidet av Erik Fagerberg og Stein Bråten med basis i " Notat 01-94/ Informasjonssikkerhet i NVE", hvor NVEs IT-sikkerhetsstatus ble kartlagt.

EMNEORD /SUBJECT TERMS IT-sikkerhetsdokumentasjon	ANSVARLIG UNDERSKRIFT Erik Fagerberg Seksjonssjef / Dataseksjonen(AD)

Kontoradresse: Middelthunsgate 29
Postadresse: Postboks 5091 Maj
0301 Oslo

Telefon: 22 95 95 95
Telefax: 22 95 90 90
Int. tlf.: +47 22 95 95 95

Bankgiro: 0629.05.75026
Postgiro: 0802 5052055

Innholdsfortegnelse

1. SKRIV FRA LEDELSEN - POLICY OG ANSVAR 4

2. INFORMASJONSSIKKERHET I NVE 5
2.1 Innledning til sikkerhetsdokumentasjon 5
2.2 Sikkerhetsmål og policy 5
2.2.1 Policy 5
2.2.2 Hovedmål 6
2.3 Sikkerhetsorganisasjon og ansvar 6
2.3.1 Ansvarsforhold generelt 6
2.3.2 Sikkerhetsorganisasjon 7
2.3.3 Instrukser 8
2.4 Beskyttelse av informasjon 8
2.4.1 Beskyttelse av informasjon og behov for varierende grad av sikring 8
2.4.2 Offentlige lover og regler knyttet til informasjonssikkerhet 9
2.4.3 Beskyttelse av informasjon i seksjonene 10
2.4.4 Kategorisering og gradering av informasjon 10
2.5 Sikkerhetsbrudd og konsekvenser 12
2.5.1 Generelt om sikkerhetsbrudd 12
2.5.2 Eksempler på sikkerhetsbrudd 12
2.5.3 Rapportering av sikkerhetsbrudd 13
2.6 Behandling av forseelser 13

3. ANSVAR SEKSJONSSJEFER 14
3.1 Lederansvar 14
3.1.1 Oppsummering lederansvar 14
3.1.2 Oppfølging i egen seksjon 14
3.1.3 Seksjonssjefs forhold til utførende aktiviteter 16
3.1.4 Ansvar for fysisk sikring 16
3.1.5 Regler ved ansettelsesforhold og endring av arbeidsoppgaver 16
3.1.6 Taushetserklæring og sikkerhetsklarering 17
3.1.7 Spesielt vedr. sikring av datamedier 18
3.1.8 Instrukser 18
3.1.9 Instruks for seksjonssjefer 19
3.2 Beskyttelse av informasjon 20
3.2.1 Kategorisering av seksjonens informasjon 20
3.2.2 Behandling av gradert av informasjon 20
3.2.3 Aktiviteter for beskyttelse av informasjon 20
3.2.4 Dokumenthåndtering 21
3.2.5 Lagring av informasjon på lokal disk/disketter 22
3.3 Sletting av informasjon 22
3.3.1 Lover og regler - sletting av informasjon 22
3.3.2 Rutiner og prosedyrer for sletting av informasjon 23
3.3.3 Tiltak mot ukontrollert sletting av informasjon 23

4. ANSVAR OG OPPGAVER TILLAGT DEN ENKELTE BRUKER 25
4.1 Ansvar tillagt den enkelte bruker 25
4.1.1 Oppsummering brukeransvar 25

4.1.2 Brukerinstruks 26
4.2.1 Datavirus 27
4.2.2 Hjemme PC 27
4.2.3 Bærbare PC'er 28
4.2.4 Backup 28
4.2.5 Utlogging 28
4.2.6 Skjermbeskytter 29
4.2.7 Passordskifte 29
4.2.8 Rapportering av sikkerhetsbrudd 29
4.2.9 Sikring av utskrifter 29
4.2.10 Bruk av fellesdisker 29
4.2.11 Endring av PC oppsett 30
4.2.12 Forsendelse og mottak av disketter eller andre datamedier 30
4.2.13 Service på PC 30
4.2.14 Bruk av Internet 30

VEDLEGG 1 - TABELL FOR KATEGORISERING AV INFORMASJON

VEDLEGG 2- SKJEMA FOR RAPPORTERING AV SIKKERHETSBRUDD

VEDLEGG 3-SKJEMA FOR AUTORISERING

VEDLEGG 4- DEFINISJONER AV ORD OG UTTRYKK

1. SKRIV FRA LEDELSEN - POLICY OG ANSVAR

NVE har innført informasjonsteknologi (IT) innen de fleste områder i virksomheten, og omfanget øker i takt med tiden. Vi blir stadig mer avhengig av IT for å løse våre oppgaver, og sårbarheten øker jevnt. Offentlige myndigheter som Datatilsynet og Riksrevisjonen setter stadig høyere krav til sikkerheten i og rundt våre systemer.

For å redusere sårbarhet og risiko til et minimumsnivå, og overholde de offentlige krav, skal NVE i tiden som kommer arbeide målbevisst med forebyggende arbeid.

Som et hjelpemiddel er det derfor utarbeidet sikkerhetsdokumentasjon inneholdende rutiner, prosedyrer, veiledninger og instrukser som skal regulere ansvaret for sikkerhet og stille krav til hvordan sikkerhetsarbeidet skal gjennomføres.

* Stadig oftere leser vi om bedrifter og etater som har vært utsatt for datavirus, svindel, sabotasje, informasjonstyveri, brudd på personvernet ol. NVE har som et klart mål å unngå slike hendelser.

* Manglende bevissthet rundt informasjonssikkerheten kan innebære alvorlige konsekvenser for NVE.

* Tiltak rundt informasjonssikkerhet må derfor være en naturlig del av vårt daglige arbeid for alle brukere, ledere, ansatte med spesielt IT-ansvar, samt dataseksjonen/AD.

Instrukser knyttet til informasjonssikkerhet omfatter alle ansatte som behandler informasjon, men kravene vil variere avhengig av type informasjon, hvilke systemer som benyttes og hva slags utstyr som benyttes.

Ledelsen i NVE vil engasjere seg sterkt rundt informasjonssikkerhet i tiden som kommer, noe som sikkerhetsdokumentasjonen gir uttrykk for i kapitlene om policy, organisasjon og ansvar. Med sikkerhetsdokumentasjonen som utgangspunkt, og engasjerte medarbeidere, er det vår ambisjon å få etablert et riktig sikkerhetsnivå for NVE, også for fremtiden.

Erling Diesen
Vassdrags- og
energidirektør

Kjell Otto Bjørnå
avd. dir. / Adm. avd.

2. INFORMASJONSSIKKERHET I NVE

2.1 Innledning til sikkerhetsdokumentasjon

Informasjonssikkerhet er å oppnå tilstrekkelig sikring av informasjon, slik at informasjonen til enhver tid er:

1. Korrekt og fullstendig (sikring av kvalitet)
2. Tilgjengelig for autorisert bruk (sikring av tilgjengelighet)
3. Utilgjengelig for uvedkommende (sikring av konfidensialitet)

Brudd på informasjonssikkerhet foreligger derfor når informasjonen for kortere eller lengre tid er; feil, ufullstendig, utilgjengelig for autorisert bruk eller kjent for uvedkommende.

Sikkerhetsdokumentasjonen "Informasjonssikkerhet i NVE" er utarbeidet for at den enkelte medarbeider skal kunne gjennomføre de nødvendige sikkerhetsaktiviteter og følge de nødvendige regler for at et riktig sikkerhetsnivå skal kunne ivaretas.

Dokumentasjonen er inndelt i forskjellige kapitler, som er spesielt tilpasset for seksjonssjefer, brukere generelt og Dataseksjonen/AD. Hvert enkelt kapittel inneholder veiledninger, rutiner/prosedyrer og instrukser. Instruksene er meget kortfattet og henviser til den øvrige dokumentasjon. Innenfor seksjonene har det også vært behov for henvisninger til vedlegg og generell dokumentasjon som er felles for alle. Alle ledere kan også være brukere, og må derfor i tillegg forholde seg til kapitel 4 - ansvar og oppgaver tillagt den enkelte bruker.

Bruken av dokumentasjonen vil variere fra bruker til bruker og fra seksjon til seksjon. Noen behandler kritisk informasjon, noen benytter hjemme-PC, noen lagrer data lokalt osv. Avhengig av bruk vil følgelig krav variere. Det bør derfor utarbeides egne dokumentasjoner for de enkelte seksjoner ved hjelp av "klipp og lim" fra dokumentasjonen. Dette arbeidet kan man få hjelp til av Dataseksjonen.

2.2 Sikkerhetsmål og policy

2.2.1 Policy

NVE har som policy og ha informasjonssikkerheten på et riktig og forsvarlig nivå, ut i fra NVE's egenart og behov. Med et "riktig nivå" menes at NVE ikke skal overdrive sikkerhetsarbeid mht. ressursbruk og tiltak, men å finne et riktig nivå i forhold til den sårbarhet og risiko som til enhver tid finnes. Med et "forsvarlig nivå" menes at offentlige myndigheters krav til informasjonssikkerhet oppfylles, og at NVEs IT-miljø har en forventet servicegrad ovenfor både interne og eksterne brukere.

2.2.2 Hovedmål

Aktiviteter rundt informasjonssikkerhet skal gjennomføres for å oppnå en tilstrekkelig sikring av informasjon, slik at informasjonen til enhver tid er korrekt og fullstendig, tilgjengelig for autorisert bruk og utilgjengelig for uvedkommende.

Riksrevisjonen stiller bl.a. krav for sikring av kvalitet, og da spesielt rundt økonomisystemer og forsystemer til disse. Oppfyllelse av disse krav og NVEs egne krav til kvalitet er dermed et av våre hovedmål.

NVEs egne krav til tilgjengelighet til data-systemer og informasjon varierer noe fra system til system, men som hovedmål skal aldri et system være nede mer enn i et døgn, uansett problem. En tilgjengelighet på minimum 98% på månedsbasis anses som tilfredsstillende. Evt. krav fra Riksrevisjonen i denne sammenheng skal også dekkes. Et av våre hovedmål er å sikre en slik tilgjengelighet.

Datatilsynet (Personregisterloven) og Beskyttelsesinstruksen setter de strengeste kravene vedr. konfidensialitet til informasjon som NVE normalt arbeider med, men Offentlighetsloven og andre setter også krav. Disse krav er følgelig også sammenfallende med NVEs egne krav. Oppfyllelse av disse krav er dermed et av våre hovedmål. NVEs sikkerhetsdokumentasjon inneholder rutiner, veiledninger, prosedyrer og instrukser. Sikkerhetsdokumentasjonen beskriver også ansvarsforhold for at våre målsetninger kan oppfylles.

Sikkerhetsbestemmelser for kraftforsyningen inneholder bestemmelser for bl.a. sikring av informasjon. På noen områder skal også opplysninger om kraftforsyningen være sikkerhetsgradert, og i denne sammenheng kommer Sikkerhetsinstruksen til anvendelse. Oppfyllelse av disse bestemmelser er dermed et av våre hovedmål.

Alle våre medarbeidere skal være klar over at brudd på informasjonssikkerheten ved å ikke utføre de rutiner eller tiltak som er bestemt, kan få alvorlige konsekvenser for NVE og den enkelte medarbeider.

2.3 Sikkerhetsorganisasjon og ansvar

2.3.1 Ansvarsforhold generelt

Vassdrags- og energidirektør (VED) har et lovbestemt ansvar for sikkerhetspolicy og oppfølging av sikkerhetsarbeidet i NVE. Dataseksjonen/AD er en naturlig samarbeidspartner for ledelsen, ledelsens rådgiver og utførende organ.

Avd.direktører er ansvarlig for gjennomføring og oppfølging innen avdelingen. I dette ligger etablering av det sikkerhetsnivå som avdelingen må tilpasse mht. utstyr, systemer og den informasjonen som behandles. Avd. direktør må også påse at opplæring ol. foretas slik at praktisk gjennomføring er mulig. Normalt kan oppgaver delegeres til seksjonssjefer.

Seksjonssjef er ansvarlig for gjennomføring og oppfølging innen egen seksjon. I dette ligger etablering av det sikkerhetsnivå som seksjonen må tilpasse mht. utstyr, systemer og den informasjonen som behandles. Seksjonssjef må også påse at opplæring ol. foretas slik at praktisk gjennomføring er mulig.

Alle ansatte er ansvarlig for å gjennomføre de sikkerhetsaktiviteter som fremkommer av sikkerhetsdokumentasjonen i form av prosedyrer, tiltak og instrukser.

Dataseksjonen/AD har ansvar for at sikkerhetsdokumentasjonen er på et riktig nivå ut i fra retningslinjer som er gitt av ledelsen. Dataseksjonen/AD skal også hjelpe de enkelte seksjoner ved etablering og innføring av informasjonssikkerhet. I tillegg til å være et rådgivende organ for ledelsen vil Dataseksjonen/AD ha ansvar for tilsyn og daglig oppfølging av sikkerhetsarbeidet, samt rapporteringsplikt til ledelsen ved sikkerhetsbrudd. Dataseksjonens oppgaver er primært knyttet til bruk av EDB-systemer og sikring av informasjon i denne sammenheng samt tiltak for sikring av maskiner og nettverk. Det er også andre seksjoner i NVE som har et forvaltningsansvar for informasjonssikkerhet.

SB, AF, APO, AØ og HD har ansvar for andre områder innenfor informasjonssikkerhet.

Områder som ligger utenfor Dataseksjonens ansvarsområde er:

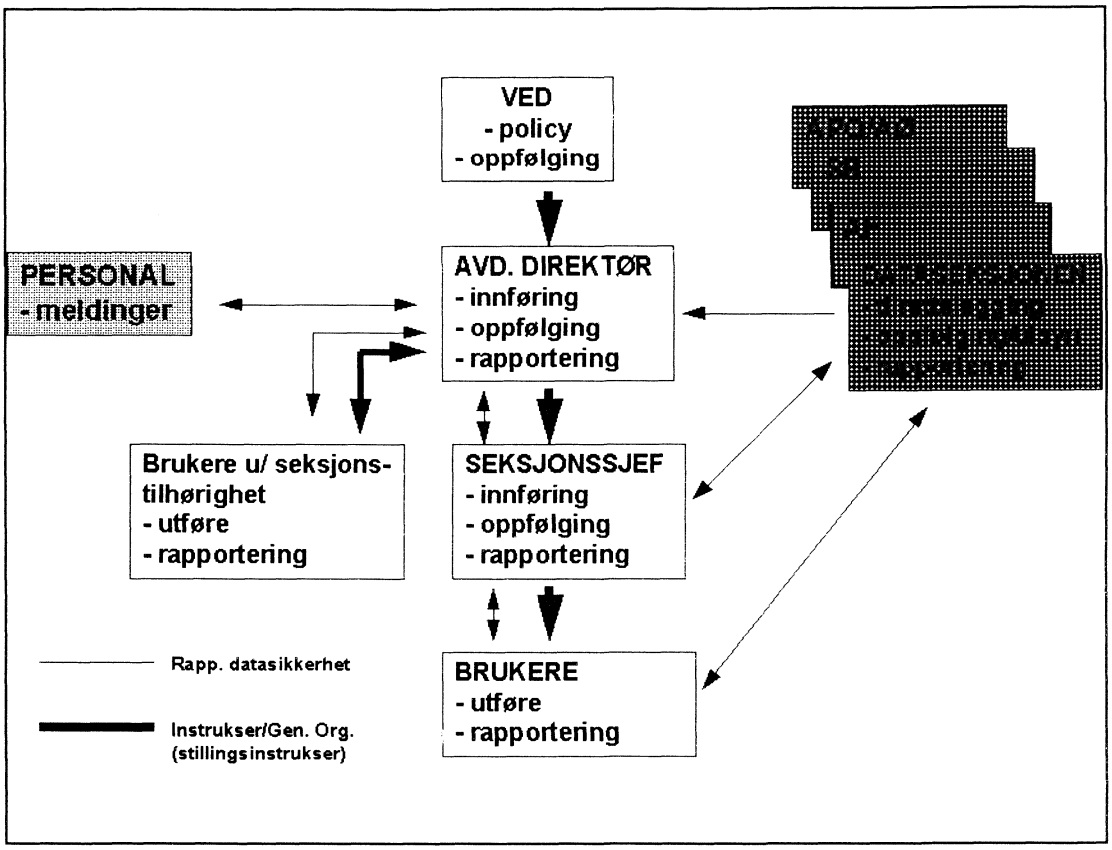
- fysisk sikring av bygg
- sikring av arkiver og dokumenter
- katastrofeplaner
- lokale reserveplaner og nødrutiner
- kontroll og oppølging av datakvalitet på fagsystemer
- sikkerhetskrav og oppfølging overfor kraftforsyningen (eksternt)
- oppfyllelse av de krav som Dataseksjonen, på vegne av VED, setter til den enkelte avdeling og seksjon.
- Informasjonssikkerhet i forbindelse med bruk av telefon og telefax.

2.3.2 Sikkerhetsorganisasjon

Sikkerhetsorganisasjon er definert i form av en praktisk modell for oppfølging av ansvar og gjennomføring av arbeidet med informasjonssikkerhet i NVE. Modellen viser også forholdet til rapportering og instrukser iht. linjeansvaret.

* Seksjonssjef har samme ansvar for sikkerhet for sin seksjon som linjeansvar ellers.
* Seksjonssjef kan delegere sine oppgaver, men ikke ansvar.
* Dataseksjonen/AD er sentral mht. rapportering av sikkerhetsbrudd, da alle sikkerhetsbrudd skal apporteres hit. Ved alvorlige hendelser skal sikkerhetsbrudd rapporteres videre. Dette fritar ikke avdelingssjef eller seksjonssjef for rapporteringsansvar.

Modell for sikkerhetsorganisasjon.



2.3.3 Instrukser

Instruksene regulerer ansvarsforhold i form av pålagte oppgaver og er en sentral del av sikkerhetsorganisasjonen i NVE. Instruksene i seg selv er ikke detaljerte nok for å sikre at våre mål oppfylles, men disse refererer til rutiner og instrukser som er detaljerte. Dette innebærer at instruksene skal sikre at NVEs mål for informasjonssikkerhet oppfylles.

2.4 Beskyttelse av informasjon

2.4.1 Beskyttelse av informasjon og behov for varierende grad av sikring

Informasjonssikkerhet er ensbetydende med å beskytte informasjon. Informasjonen skal beskyttes mht. kvalitet, tilgjengelighet og konfidensialitet. I utgangspunktet skal all informasjon beskyttes iht. de krav som sikkerhetsdokumentasjonen spesifiserer.

NVE behandler mye informasjon både manuelt og elektronisk. Det stilles forskjellige krav til sikring avhengig av type informasjon. Kravene som gjelder er spesifisert under kap. 2.2 og 2.4.2 i dette dokumentet. De som behandler informasjon må være klar over hvilke krav som gjelder for den informasjon de behandler.

Noe informasjon kan betraktes som meget kritisk dersom dette kommer uvedkommende ihende og annen informasjon er kritisk med hensyn til kvalitet (riktighet). Situasjoner hvor spesiell informasjon ikke er tilgjengelig kan også bli kritiske. Informasjon kan bli kritisk dersom den sammenstilles med data fra andre databaser eller registre, selv om den alene ikke kan betraktes som kritisk.

Det er derfor behov for varierende grad av sikring for å unngå kritiske situasjoner og for å oppnå NVE's mål for informasjonssikkerhet. NVE's informasjon kan ikke uten videre benyttes på hjemme-PC eller på bærbare PC'er, noe informasjon er underlagt krav om nedlåsing i brannsikre skap, noe informasjon er underlagt krav om kryptering dersom disse sendes over linje, spesiell kritisk informasjon kan ikke lagres lokalt osv.

Det er likevel viktig at all informasjon sikres, selv om tiltakene kan være forskjellig. Det er derfor viktig at den enkelte seksjon og medarbeider vet hva slags informasjon de arbeider med, og om det er behov for spesiell sikring, eller om spesielle lover eller regler må følges.

De enkelte seksjoner og brukere må forstå hvorfor informasjon skal beskyttes - og at det kreves forskjellige sikringstiltak avhengig av varierende behov. Her følger noen eksempler som viser forskjellige utfordringer seksjonen må arbeide med:

-Type informasjon som behandles - lovbestemt og viktigheten av informasjonen
-Type utstyr - bruk av hjemme-PC'er, plassering av printer o.l.
-Maskiner med modem- tilknytning og muligheter for inntrengning.
-Tilgangsbegrensninger til systemer som er utsatt for manipulasjon/svindel.
-Sikring av lokal reservekopi - hyppighet i forhold til hvor kritisk situasjonen er

Dersom seksjonen ikke behandler kritisk eller sensitiv informasjon vil sikkerhetstiltakene i ovennevnte eksempler være enkle. Behandler derimot seksjonen sensitiv eller kritisk informasjon vil sikkerhetstiltak være avhengig av den kategori/gradering som bestemmes.

2.4.2 Offentlige lover og regler knyttet til informasjonssikkerhet

Det er viktig at den enkelte avdeling/seksjon er klar over hvilke lover og regler som gjelder. Det finnes en rekke lover og regler som vil gjelde alle seksjoner som f.eks. **Offentlighetsloven, Forvaltningsloven** og generelle **regler for arkivering.**

Dersom opplysninger om personer, sammenslutninger eller stiftelser behandles gjelder **Personregisterloven**. Det kan ikke systematisk lagres informasjon om personer uten at konsesjon er gitt og behandling av slik informasjon er underlagt spesielle krav som må følges. Dette gjelder både manuelle papirarkiver/dokumenter og elektronisk informasjon.

Opplysninger eller dokumenter som kan gjøre skade for NVE, offentlige interesser, en bedrift, institusjon eller enkeltperson ved at innhold blir kjent av uvedkommende er underlagt

Beskyttelsesinstruksen. Dersom slik informasjon behandles må gradering foretas og de aktuelle regler følges.

Sikkerhetsinstruksen kommer til anvendelse ved behandling av gradert informasjon i forbindelse med totalforsvaret som kraftforsyningen er en del av. Dette gjelder bl.a. GIS og Net-bas. Mange personer i NVE behandler slik informasjon og de fleste tilhører energiavdelingen og SB. Slike opplysninger er underlagt helt spesielle krav og skal behandles etter samråd med - eller instruks fra SB.

Riksrevisjonen kontrollerer NVEs oppfyllelse av **Regnskapsforskrifter** og **Arkivinstruksen.** Disse forskrifter er relatert til økonomisystemer og forsystemer til disse. Fokus er følgelig på datakvalitet og rekonstruksjon av hendelser. Viktige områder her i forhold til informasjonssikkerhet er autorisasjon/tilganger, databasemanipulasjon, kommunikasjon/modem, sikkerhetskopiering (også av "systemoperasjoner") og kontroll og oppfølging av alle logger inkl. de rullerende, som også må skrives ut.

Sikkerhetsbestemmelser for kraftforsyningen inneholder bestemmelser for bl.a. sikring av informasjon. På noen områder skal også opplysninger om kraftforsyningen være sikkerhetsgradert, og i denne sammenheng kommer Sikkerhetsinstruksen til anvendelse.

2.4.3 Beskyttelse av informasjon i seksjonene

Elektronisk informasjon som lagres sentralt har Dataseksjonen/AD ansvar for, men dette ansvaret er kun begrenset til linjer fra den enkelte seksjon og lagring på sentrale maskiner. Behandling av informasjon, bruk av utstyr lokalt og lokal lagring er seksjonen selv ansvarlig for. Seksjonen har også ansvaret for sikker lokal lagring av dokumenter, pairer ol.

Informasjonen skal beskyttes iht. de krav som er spesifisert i kapittel 4 - ansvar og oppgaver tillagt den enkelte bruker. Det er seksjonssjefs ansvar og koordinere og følge opp dette ansvaret i seksjonen.

Seksjonens ansvar kan i korte trekk oppsummeres slik:

- Kategorisering og gradering av den informasjon som behandles
- Fysisk sikring av lokaliteter
- Nedlåsing av dokumenter og forsvarlig forsendelse ol.
- Håndtering av datamedier som også inkl. gjenbruk av disketter og disker som må beskyttes ved service og salg av utstyr
- Beskytte mot uautorisert tilgang til systemer
- Beskytte mot datavirus
- Sikkerhetskopiering og lagring (ved lokal lagring)
- Sikkerhet ved bruk av hjemme-PC'er og bærbare PC'er
- Sikkerhet ved bruk av utstyr og programmer

2.4.4 Kategorisering og gradering av informasjon

Vi har foretatt en samordning av offentlige lover og direktiver med egne krav - mht. beskyttelse av informasjon (konf. tabell vedlegg 1). Tabellen er utarbeidet for å skape forståelse for beskyttelse av informasjon og må brukes av den enkelte avdeling/seksjon som selv må vurdere i

hvilken kolonne (lov, instruks eller egeninteresse) den enkelte informasjon inngår. Hver enkelt leder og saksbehandler må vurdere den informasjon de behandler ut i fra de prinsipper det er lagt opp til, og det gjeldene lovverk. Det kan være forhold som tabellen ikke dekker, eller forhold som gjør at informasjonen må beskyttes spesielt. Graderinger og lover som er gitt av forskjellige offentlige organer flyter over i hverandre med hensyn til krav om beskyttelse, men vi har forsøkt å samordne dette i ett felles tabellverk.

Dersom seksjonen behandler informasjon som skal beskyttes særskilt (konf. nedennevnte beskrivelser) bør tiltak diskuteres med Dataseksjonen/AD. Vi henviser i slike tilfelle til lovverket for behandling av slik informasjon. Dataseksjonen/AD vil også være behjelpelig med å fremskaffe dette. Dette gjelder primært Personregisterloven, Beskyttelsesinstruksen og Sikkerhetsinstruksen. I tillegg gjelder også "Sikkerhetsbestemmelser for kraftforsyningen", Offentlighetsloven, Forvaltningsloven og Arkivinstruksen som vi forutsetter er kjent.

Vi har delt informasjon opp i 4 kolonner, hvor kolonne 0 i utgangspunktet ikke trenger noen spesiell form for beskyttelse, mens kolonne 3 er den hvor beskyttelseskrav er størst. Konf. tabell for kategorisering - vedlegg 1. Med kategorisering mener vi å plassere den informasjon som behandles i den kolonne/lov som gjelder slik at nødvendige sikkerhetskrav kan oppfylles. Det vil ofte være en vurdering av hvor sensitiv informasjonen kan være og hvor denne skal plasseres. Dette gjelder spesielt forholdet mellom FORTROLIG og STRENGT FORTROLIG i Beskyttelesinstruksen og i forhold til interne notater, brev ol.

For kolonne 1 (personregisterloven) stilles det ofte helt spesielle krav til sikring av informasjon dersom virksomheten har fått konsesjon for opprettelse av registre/databaser med informasjon utover det som er normalt. Med dette menes informasjon utover det som er spesifisert i Personregisterloven, med standarder som er tillatt for forskjellige typer registre. Tabellen dekker følgelig ikke slike sikkerhetskrav selv om enkelte krav kan være dekket inn i NVEs ordinære sikkerhetstiltak. Interne notater ol. som har visse krav til konfidensialitet må vurderes behandlet iht. tiltak som er beskrevet her.

Graderingene FORTROLIG OG STRENGT FORTROLIG i Beskyttelsesinstruksen skal følge de sikringstiltak som gjelder hhv. BEGRENSET og KONFIDENSIELT i Sikkerhetsinstruksen med unntak av at Sikkerhetsinstruksen setter spesielle krav til autorisering.

Det er viktig å være klar over at informasjon som i en database eller register, ikke sikkerhetsmessig har noen betydning alene, kan få en sikkerhetsmessig betydning dersom slik informasjon sammenstilles med data fra andre databaser eller registre. I de tilfelle det åpnes for slike muligheter må de aktuelle sikkehetskravene følges.

Graderingene STRENGT FORTROLIG i Beskyttelsesinstruksen og KONFIDENSIELT i Sikkerhetsinstruksen, dvs. kolonne 3, krever såpass strenge sikkerhetskrav at dersom slik informasjon behandles må tiltak tilrettelegges i samråd med Dataseksjonen/AD og SB.

I utgangspunktet skal all informasjon sikres på en betryggende måte, men spesielle krav og regler må følges dersom spesielt sensitiv informasjon behandles eller vi håndterer svært viktig informasjon. Det er viktig at all informasjon som seksjonen behandler kategoriseres og at tabellen fylles ut/benyttes iht. dette.

Kategorisering og gradering av informasjonen er et linjeansvar.

2.5 Sikkerhetsbrudd og konsekvenser

2.5.1 Generelt om sikkerhetsbrudd

Sikkerhetsbrudd er definert som en hendelse hvor ett av følgende har inntruffet:

* Brudd på de lover og regler NVE er pålagt å følge
* Konfidensialiteten er brutt ved at uvedkommende har fått tilgang til informasjon. (inntrenging, informasjonstyveri, bortkommet PC, datamedie som reservekopi ol)
* Informasjonen er ikke tilgjengelig, slik at forsinkelser oppstår eller at oppgaver ikke kan utføres. (konfigurasjonsproblemer, diskkræsj, linje- eller nettverksproblemer ol.)
* Informasjonskvaliteten forringes ved feil eller en "uforklarlig årsak" (kan være databasemanipulasjon, ureglementert oppdatering av egne ansatte, feil som oppstår ved kommunikasjon ol.)

Dersom informasjon i form av papir, filer, disketter eller reservekopi er kommet på avveie vil dette betraktes som sikkerhetsbrudd, selv om ingen skade er kjent. Dersom filer er "borte" er dette et sikkerhetsbrudd, selv om ingen skade er skjedd. Dersom man har mistanke om at data er endret ureglementert eller er blitt feil ved en ukjent årsak, skal dette også betraktes som sikkerhetsbrudd. Datavirus, systemkræsj, informasjonstyveri, annen uautorisert bruk, databasemanipulasjon, sensitiv informasjon på avveie er eksempler på sikkerhetsbrudd.

2.5.2 Eksempler på sikkerhetsbrudd

Sikkerhetsbrudd skal i utgangspunktet ikke forekomme dersom instrukser blir fulgt i alle ledd i NVE. Konsekvenser av sikkerhetsbrudd kan være små. Alvorlige konsekvenser kan oppstå ved slurv og ubevisste handlinger, som på forhånd virker bagatellmessig. Bevisst sabotasje og hacking kan få meget alvorlige konsekvenser. Sikkerhetsbrudd (og konsekvenser) vil bli redusert ved økt forståelse og bevissthet rundt skadevirkninger og konsekvenser dette kan medføre.

Sikkerhetsbrudd kan forekomme på alle områder som er omtalt i sikkerhetsdokumentasjonen og vi vil her kun trekke frem noen eksempler for å få frem en bedre forståelse av dette.

Datavirus rammer NVEs nett
Dette kan skje dersom noen kopierer inn informasjon fra disketter som mottas fra andre eller bruk av ulovlige programmer som spill ol. Det finnes eksempler på datavirus som har medført at virksomheter har vært ute av stand til å bruke sin informasjon eller systemer på flere uker. De verste eksempler er der virus også har rammet reservekopier og informasjonen er blitt totalt utilgjengelig. Antivirusprogrammer er en sikkerhet, men langt fra tilstrekkelig for å unngå virus. En tilsynelatende uskyldig handling kan påføre NVE virus og konskvensene kan bli formidable. En liten "glipp" som f.eks. å ta med en "arbeids diskett" som inneholder virus, som eksempelvis stammer fra et "spill" på hjemme PC'en, kan få store følger.

PC'er med sensitiv informasjon stjeles
Bærbare PC'er er svært utsatt for tyveri. Formålet er ofte i tillegg til å stjele PC'en, å utnytte den sensitive informasjonen som måtte ligge der.

Uautorisert bruk (tilgang)
Flere bedrifter er rammet av at uvedkommende har klart å manipulere data. Dette har skjedd via PC'er som ikke er avlogget eller ved hacking inn mot bedriftens maskiner. Dersom data ikke er kryptert/forseglet er det viktig at lokalitetene er sikret slik at avlytting av passord og identer ikke kan forekomme. Forsøk på manipulasjon (eller sabotasje) kan f.eks. ramme NVE's økonomisystemer, GIS, informasjon om magasininnhold eller persondata. Det er også viktig at passord holdes hemmelig slik at dette ikke blir utnyttet av eksterne eller andre i organisasjonen. Misbruk på grunn av at passord er blitt kjent for uvedkommende har vært et problem for en rekke bedrifter, og betydelig svindel og datatyveri er foretatt.

Konsekvenser for andre
NVE kan bidra til at det skapes problemer med betydelige konsekvenser for andre som f.eks. ved at markedsinformasjon går på tvers av konkurrenter i kraftforsyningen eller sensitive opplysninger om et selskap eller offentlige interesser kommer på avveie. Større konsekvenser kan være i forbindelse med presseomtaler da dette erfaringsmessig setter både kilde og den informasjonen gjelder i et dårlig lys. Konsekvenser ved brudd på lover og regler vil variere avhengig av hvordan informasjon kommer på avveie. Ved utgivelse av markedsinformasjon kan dette få økonomiske konsekvenser for de dette gjelder.

2.5.3 Rapportering av sikkerhetsbrudd

Det er lagt opp til egen rutine for rapportering av sikkerhetsbrudd (definisjon i kap.2.5). Det er viktig at rapporteringskravet blir overholdt. Sikkerhetsbrudd og mistanker om sikkerhetsbrudd skal rapporteres til nærmeste overordnede og Dataseksjonen/AD. Dette gjelder selv om ikke noen skade er skjedd. Dette er meget viktig for Dataseksjonen/AD, slik at nye eller korrigerende tiltak skal kunne iverksettes. Statistikk vil også gi en klar indikasjon på behov for opplæring, informasjon, endringer av konfigurasjoner ol. Sikkerhetsbrudd som påvirker seksjonen negativt skal også rapporteres oppover i linjeorganisasjonen.

2.6 Behandling av forseelser

Et sikkerhetsbrudd kan komme av en hendelse som kan være et hendelig uhell eller feil behandling som ingen kan lastes for. Hendelsen kan også være av en "rimelig uskyldig" karakter selv om noen kan lastes for dette.

Et sikkerhetsbrudd kan også være et resultat av en alvorlig forseelse eller gjentatte hendelser som gir klar indikasjon på at ansatte ikke vil rette seg etter NVEs instrukser. Dataseksjonen/AD og seksjonssjefer pålegges å rapportere alvorlige og/eller gjentatte sikkerhetsbrudd oppover i linjeorganisasjonen, slik at tiltak kan gjøres for å unngå denne form for sikkerhetsbrudd i fremtiden.

3. ANSVAR SEKSJONSSJEFER

3.1 Lederansvar

3.1.1 Oppsummering lederansvar

Gjennomføring og oppfølging av informasjonssikkerhet er en del av linjeansvaret, og er pålagt av NVEs øverste ledelse i form av instrukser. Seksjonssjef er ansvarlig for innføring av de sikkerhetstiltak som er nødvendig for seksjonen, avhengig av hva slags informasjon og utstyr som seksjonen har i besittelse. Videre er seksjonssjef ansvarlig for å følge opp at de nødvendige sikkerhetstiltak i form av fysiske tiltak, prosedyrer og rutiner blir gjennomført.

Sikkerhetsdokumentasjonen skal være et hjelpemiddel for å ivareta dette ansvaret. Konf. generelt om ansvar og organisasjon rundt sikkerhetsarbeidet i kapittel 2.

3.1.2 Oppfølging i egen seksjon

Seksjonssjef kan ved behov få støtte fra Dataseksjonen/AD som har det sentrale ansvaret på vegne av ledelsen for etablering og dokumentasjon av sikkerhetstiltak som ivaretar NVEs krav på et riktig nivå. Det finnes også andre seksjoner i NVE som har et overordnet ansvar innen andre områder for informasjonssikkerhet. I denne forbindelse henvises det til "ansvarsforhold generelt" kap. 2.3.1.

For at oppfølging skal kunne skje på en forsvarlig måte må sikkerhetsdokumentasjonen "innføres" i seksjonen slik at alle får den nødvendige forståelse for hvorfor tiltak skal gjennomføres.

Oppfølging i den enkelte seksjon innebærer:

Påse at seksjonen gjennomfører de pålagte sikkerhetstiltak
Påse at kompetansenivået er tilstrekkelig og evt. gjennomføre opplæring sammen med Dataseksjonen.
Ajourhold av seksjonens tilpassede sikkerhetsdokumentasjon
Melde endringer til Dataseksjonen dersom det inntreffer forhold som vil påvirke sikkerheten
Rapportering av sikkerhetsbrudd til Dataseksjonen

Påse at seksjonen gjennomfører de pålagte sikkerhetstiltak

Seksjonssjef må følge opp at brukerne følger de pålagte instrukser da det alltid er en fare for at ikke målbare sikkerhetstiltak kan skli ut. Med ikke målbare sikkerhetstiltak menes rutiner og prosedyrer som man ikke kan se resultater av - før ett sikkerhetsbrudd oppstår og som forårsaker en eller annen form for konsekvens. Manglende utførelse av sikkerhetsaktiviteter kan derimot bli ekstremt målbare dersom et sikkerhetsbrudd skulle inntreffe.

Oppfølging kan bestå av en uformell prat med den enkelte, stille spørsmål eller at det utarbeides et spørreskjema med jevne mellomrom, f.eks. halvårlig. Status bør også tas opp på ledermøter og seksjonsmøter med jevne mellomrom. Er man usikker bør også stikkprøver tas, og i denne forbindelse kan Dataseksjonen/AD være behjelpelig.

Påse at kompetansenivået er tilstrekkelig og evt. gjennomføre opplæring sammen med Dataseksjonen/AD.

Det er viktig at hele seksjonen er bevisst på informasjonssikkerhet og vet hvorfor tiltak skal gjennomføres. Å ha oversikt over mulige konsekvenser seksjonen kan påføre NVE og hvordan tiltak skal gjennomføres er en forutsetning. Det er derfor viktig at det pr. seksjon tas en gjennomgang/diskusjon rundt mulige konsekvenser i forbindelse med opplæring og bevisstgjøring. Dette bør gjennomføres minimum årlig.

Ajourhold av seksjonens tilpassede sikkerhetsdokumentasjon

Sikkerhetsdokumentasjonen vil bli ajourholdt av Dataseksjonen/AD slik at nye versjoner (eller sider) vil bli utsendt til de enkelte seksjoner. Endringer og forhold som vil påvirke seksjonen må tilpasses i seksjonens dokumentasjon og nødvendige tiltak må gjennomføres. Nødvendige tiltak som må gjennomføres vil bli beskrevet ved oversendelse av nye versjoner. Dette vil være på generell basis slik at seksjonen må vurdere hva som angår dem selv.

Melde endringer til Dataseksjonen/AD dersom det inntreffer forhold som vil påvirke sikkerheten

En rekke forhold kan endre kravene til informasjonssikkerhet for seksjonen. Dersom kravene endres må normalt også gjennomføring av de enkelte sikkerhetsaktiviteter endres. Det er derfor viktig at Dataseksjonen/AD får beskjed slik at dokumentasjonen også kan endres. Dersom man er usikker på om kravene endres, må dette tas opp med Dataseksjonen/AD.

Eksempler på forhold som kan endre kravene til informasjonssikkerhet:

- Endringer i den informasjonen som seksjonen behandler og som er underlagt strengere regler vedr. gradering og konfidensialitet
- Installasjon av EDB-utstyr i seksjonen, eller at bærbare PC'er eller hjemme-PC'er tas i bruk
- Tar i bruk nye dataprogrammer
- Etablering av kommunikasjon mot eksterne systemer
- Etablering av automatikk for å motta informasjon fra eksterne kilder for oppdatering i lokale systemer som kontorstøtte, økonomisystem, lagersystem osv.
- Etablering av personregistre
- Endring av systemoppsett eller lokalt nettverk (konfigurasjon)
- Flytting av datautstyr

Rapportering av sikkerhetsbrudd til Dataseksjonen/AD

Sikkerhetsbrudd skal rapporteres til Dataseksjonen/AD. Sikkerhetsbrudd er forhold som påvirker sikkerhet eller sårbarhet for NVE eller seksjonen negativt. Sikkerhetsbrudd kan f.eks. være:

* Datavirus eller mistanke om datavirus
* Identer og passord er blitt kjent for andre enn "eier"
* Informasjon er mistet eller stjålet. (PCer, disketter, dokumenter er kommet bort)
* Mistanke om, eller feil i datagrunnlag ved at informasjonskvaliteten forringes
* Feil eller unormale hendelser på datautstyr

* Informasjon ikke tilgjengelig
* Brudd på sikkerhetsrutiner eller prosedyrer

Sikkerhetsbrudd skal rapporteres for at risiko for slike hendelser i ettertid skal begrenses mest mulig.

Sikkerhetsbrudd som påvirker seksjonen eller NVE negativt eller har med forsømmelse av oppgaver og ansvar å gjøre, skal rapporteres videre oppover i linjeorganisasjonen. Dette er seksjonssjefs ansvar.

3.1.3 Seksjonssjefs forhold til utførende aktiviteter

Ansvar som er pålagt seksjonssjef er beskrevet i dette kapittel, mens den enkelte brukers ansvar er beskrevet i kapittel 4. Seksjonssjef er som bruker også underlagt de sikkerhetskrav som fremkommer i kapittel 4. Seksjonssjef har også det overordnede ansvaret for at den enkelte bruker er kjent med informasjonssikkerhet og er i stand til å ivareta sitt ansvar.

Her beskrives hvordan seksjonssjef skal ivareta informasjonssikkerhet i sin seksjon. Hovedtyngden av seksjonens utførende sikkerhetsaktiviteter er detaljert beskrevet i kapittel 4, slik at ansvaret må ses i forhold til dette.

3.1.4 Ansvar for fysisk sikring

Fysisk sikring i tilknytning til informasjonssikkerhet i seksjonen er et lederansvar. Fysisk sikring er beskrevet i tilknytning til den enkelte bruker i kapittel 4. Det er viktig at alle aktiviteter rundt fysisk sikring blir koordinert i den enkelte seksjon av seksjonssjef. Å skape bevissthet blant de ansatte slik at alle forstår sitt ansvar og mulige konsekvenser gjelder også fysisk sikring. Fysisk sikring henger også sammen med kategorisering og gradering av informasjon. Avhengig av seksjonens informasjon, og hvor sensitiv denne er samt muligheter for uautoriserte til å tilegne seg denne, vil være avgjørende for hva slags sikkerhetstiltak som er nødvendig.

Informasjon som går tapt kan ofte rekonstrueres ved hjelp reservekopier, kopier i arkiv, ved henvendelse til samarbeidspartnere, kraftselskap osv. Men det kan være informasjon som ikke kan rekonstrueres, og konsekvensene kan være store. Konsekvenser i form av merarbeid, økonomisk tap og lovbrudd må gjennomgås, og nødvendige tiltak må innarbeides i den enkelte seksjon.

Fysisk sikring er primært tiltak for å forhindre innsyn og informasjonstyveri. Låsing av seksjonens lokaliteter og sikring av dokumenter og datamedier er det viktig å ha et bevisst forhold til.

Fysisk sikring er mer detaljert beskrevet i kapittel 3.4.

3.1.5 Regler ved ansettelsesforhold og endring av arbeidsoppgaver

Det er seksjonssjefs ansvar at ansatte kun får tilgang til den informasjonen de har behov for ("need to know" prinsippet). Dette gjelder tilgang til informasjon på sentrale servere, sentrale systemer, lokale PC'er, lokale nett og dokumentarkiver.

Ved ansettelse skal seksjonssjef sikre at brukere kun får tilgang til nødvendig informasjon. Det skal kun autoriseres for lesetilgang (spørring) dersom behovet for endring/oppdatering (registrering)

ikke er der. Endringer i arbeidsforhold skal straks meldes Dataseksjonen/AD, slik at endringer i autorisasjonsforhold foretas (konf. vedlegg 3 - skjema for autorisering). Når det gjelder lokale PC'er må dette administreres av seksjonen. Lokale PC'er som ikke er tilkoblet sentrale maskiner, med sensitive data, skal også sikres med passord og ident. Før nyansatte får tilgang til systemer/informasjon skal behov og sikkerhetskrav vurderes.

Seksjonssjef må være spesielt klar over potensielt misbruk av identer ved fratredelser, slik at det må vurderes å begrense tilganger i god tid før ansettelsesforholdet er ferdig. . Spesielt utsatt er personer under oppsigelse som kan føle seg urettferdig behandlet slik at fare for "hevn" er tilstede. Ansatte som skal begynne i virksomhet som kan dra nytte av informasjonen kan også være en fare (konf. først og fremst konkurransesituasjonen i kraftforsyningen).

Seksjonssjef må jevnlig kontrollere brukerprofilen i egen seksjon og påse at dette er i overenstemmelse med de tilganger som er godkjent, samt revidering av denne. "Lokal autorisasjon" på f.eks frittstående PC'er må følges opp tilsvarende.

3.1.6 Taushetserklæring og sikkerhetsklarering

Den enkelte seksjon (avdeling) må vurdere taushetserklæring og sikkerhetsklarering for den enkelte bruker i forhold til:

* Offentlige lover og direktiver
* Fare for lekkasje av sensitive opplysninger til uvedkommende

Det finnes ingen generelle pålegg iht. norsk lov om at ansatte skal undertegne taushetserklæring. Enkelte lover setter krav til taushetserklæring som f.eks. Personregisterloven (Datatilsynet) som setter krav til taushetserklæring for ansatte eller andre som arbeider med konsesjonspliktige personregistre.

Videre er det en rekke bestemmelser i Datasikkerhetsdirektivet som er utfyllende bestemmelser til Sikkerhetsinstruksen og Beskyttelsesinstruksen. Dette er instrukser som skal ivareta rikets sikkerhet og beskyttelse av informasjon av andre grunner enn det som gjelder rikets sikkerhet. Det siste gjelder opplysninger som kan gjøre skade på personer, bedrifter, institusjoner eller offentlige interesser. Alle seksjoner som håndterer slik informasjon skal være klar over dette og følge de regler som er gitt i direktivet. Det er krav om taushetserklæring dersom ansatte har tilgang til informasjon som er underlagt Sikkerhetsinstruksen.

Det forekommer at det behandles informasjon som reguleres (i lovs form) av Sikkerhetsinstruksen. Dette er informasjon som kan sette rikets sikkerhet i fare dersom uvedkommende får dette i hende. Ved behandling, eller at seksjonen er i besittelse av slik informasjon, skal også sikkerhetsklarering foreligge for de personer som har mulig tilgang til disse. I tillegg skal taushetserklæring undertegnes.

Innhentelse av taushetserklæring og autorisasjon av brukere er et linjelederansvar. Sikkerhetsklarering foretas av SB for ansatte i NVE, men linjeledere må følge opp dette i hhv. egen avdeling og seksjon.

3.1.7 Spesielt vedr. sikring av datamedier

Det er viktig at seksjonen har kontroll over datamedier og er bevisst på den fare datamedier utgjør mht. at uvedkommende kan tilegne seg sensitiv informasjon.

Følgende må følges opp spesielt:

* Lokale sikkerhetskopier på disketter skal ikke være fritt tilgjengelig i lokalitetene. (unntak dersom det kun er informasjon av kategori 0)
* Disketter som er formatert etter bruk kan for andre være enkelt å få tilgjengelig på nytt. Disketter som har hatt sensitiv informasjon, og er blitt formatert, skal behandles som om det fortsatt er sensitiv informasjon på disse.
* Ved salg av PC'er eller at noen skal benytte NVEs PC'er som hjemme-PC må det sikres at det ikke har vært sensitiv informasjon på disken. Er man usikker må dette tas opp med Dataseksjonen/AD. Selv om disken er formatert og overskrevet en rekke ganger kan informasjon rekonstrueres.

Konf. forøvrig kapittel 3.2 - Beskyttelse av informasjon

3.1.8 Instrukser

Generelt om instrukser

Det er utarbeidet instrukser for seksjonssjefer, brukere generelt og for seksjoner med ansvar for datasystemer og utstyr. Instrukser for seksjonssjefer er omtalt her.

Instrukser er en del av linjeansvaret og må oppfattes som en del av det ansvar som stillingen medfører, og må dermed inngå som en del av de "daglige oppgaver". Instrukser er gitt av toppledelsen i NVE og følges opp som linjeansvar forøvrig i NVE. Dataseksjonen har ansvaret for tilsyn og forvaltning av sikkerhetsdokumentasjonen. I dette ligger også forvaltning av instrukser som er knyttet til sikkerhetsdokumentasjonen.

Instrukser - ansvar og plikter

Det vil være stor forskjell på hva de enkelte seksjoner har av ansvar og plikter knyttet til sikkerhet. Seksjoner som f.eks. ikke behandler gradert informasjon, ansatte som ikke har hjemme-PC, ansatte som ikke har bærbar PC, seksjoner som kun bruker standard programvare og ikke benytter kommunikasjon utover NVEs standard nett, vil ha minimalt å forholde seg til, i forhold til seksjoner der dette gjelder.

Det er seksjonssjefs ansvar å holde seg orientert om hva som gjelder av sikkerhetstiltak inkludert rutiner ol. for egen seksjon. For å gjøre det enklere for de enkelte seksjoner kan Dataseksjonen/AD yde bistand ved seksjonsvis innføring og forvaltning av de nødvendige sikkerhetstiltak. Det er også den enkelte seksjons ansvar å ajourholde egen tilpasset sikkerhetsdokumentasjon når oppgradering kommer fra Dataseksjonen/AD.

Seksjonssjef må forholde seg til instrukser som er pålagt den enkelte bruker og de instrukser som er pålagt seksjonssjef.

3.1.9 Instruks for seksjonssjefer

Nedenfor er de gjeldende instrukser beskrevet. Hvordan man konkret skal forholde seg til instrukser er omtalt i kapitlene for leder- og brukeransvar.

* **Seksjonssjef skal sørge for at seksjonens samlede sikkerhetsaktiviteter er tilrettelagt og organisert.**

* **Seksjonssjef skal følge opp at instrukser for brukere blir fulgt.**

* **Seksjonssjef skal sørge for at seksjonens informasjon blir kategorisert og at nødvendig gradering blir foretatt.**

* **Seksjonssjef skal sørge for ajourhold av seksjonens sikkerhetsdokumentasjon.**

* **Seksjonssjef skal sørge for at alle sikkerhetsbrudd og mistanker om sikkerhetsbrudd blir rapportert til avdelingsdirektør med kopi til Dataseksjonen/AD.**

* **Seksjonssjef skal gi beskjed til Dataseksjonen/AD dersom forhold som påvirker informasjonssikkerheten endrer seg.**

* **Seksjonssjef skal innhente nødvendige taushets-erklæringer og sørge for at sikkerhetsklareringer blir foretatt.**

* **Seksjonssjef skal ha oversikt over autorisasjoner i seksjonen, ajourhold av disse og begrense disse maksimalt iht. den enkelte brukers behov.**

* **Seksjonssjef skal påse at seksjonens informasjon blir fysisk beskyttet iht. de krav som finnes.**

3.2 Beskyttelse av informasjon

Kapittel 2.4 omhandler beskyttelse av informasjon som alle må være klar over. Kapittel 4 omhandler det som den enkelte bruker må forholde seg til. Vi relaterer her beskyttelse av informasjon til lederansvaret.

3.2.1 Kategorisering av seksjonens informasjon

Det er ikke like viktig å beskytte all informasjon. Informasjon skal sikres avhengig lovverket, og til en viss grad etter behov, da sikring også er et kostnadsspørsmål. Sikring av sensitiv informasjon på en bærbar PC er f.eks. et krav. Sikring av informasjon kan gjøres ved å kryptere disken, men dette koster, slik at dette ikke settes som et generelt krav, men kun dersom det oppbevares sensitiv informasjon på hjemme-PC eller bærbar PC.

Sensitive dokumenter skal låses ned i innbruddsikre skap. Dersom alle dokumenter til enhver tid skulle vært nedlåst i slike skap, hadde dette både vært et praktisk og kostnadsmessig problem.

For at seksjonen i det hele tatt skal ha et forhold til det å sikre informasjon, må informasjonen være kategorisert. Det er hver enkelt seksjons ansvar å foreta nødvendig kategorisering og gradering av informasjon. Med kategorisering menes å vurdere informasjon slik at det kan bestemmes under hvilken lov eller instruks informasjonen inngår. Dette gjelder også notater, brev ol.

3.2.2 Behandling av gradert av informasjon

Gradert informasjon skal behandles iht. Beskyttelsesinstruksen og sikkerhetsinstruksen. Sikkerhetstiltak og behandling fremkommer i tabellen i vedlegg 1, og i tillegg henvises det til kapitel 2.4 og ovennevnte instrukser/regelverk for detaljert informasjon. Dersom seksjonen er i tvil om hvordan tiltak skal etableres kan Dataseksjonen/AD bistå.

3.2.3 Aktiviteter for beskyttelse av informasjon

Seksjonens informasjon har seksjonssjef på vegne av seksjonen ansvar for. Informasjon på sentrale servere har Dataseksjonen/AD ansvaret for, men egen seksjon har ansvaret for de tilganger som er tildelt de enkelte brukere.

Vi har delt beskyttelse av informasjon inn i 3 områder i forhold til formål med beskyttelse:

* Tilgjengelighet. Sikre informasjonens tilgjenegelighet
* Kvalitet. Sikre mot manipulasjon og feil i datagrunnlaget
* Konfidensialitet. Sikre mot innsyn eller tyveri av informasjon

Avhengig av hva vi sikrer oss mot, vil også tiltakene være forskjellige. Nedenfor er de 3 områder grovt beskrevet.

Tilgjengelighet
Seksjonen har ansvaret for å ta sikkerhetskopi(backup) og forsvarlig lagring av denne dersom data lagres lokalt. Her kan også krav om ekstern lagring gjøres gjeldende. Sentral lagring er

Dataseksjonens ansvar. Virus kan også forårsake at informasjon ødelegges og blir utilgjengelig. Sikring av tilgjengelighet vil omfatte:

* Sikkerhetskopiering og lagring av denne
* Sikring av kritisk manuell informasjon som vanskelig kan rekonstrueres
* Sikring mot datavirus som også i verste fall kan ramme sikkerhetskopi
* Følge regler for konfigurasjonsendringer ol. for å ivareta stabil drift

Kvalitet

I forbindelse med kvalitet skal det sikres mot ødeleggelse (feil og annen forringelse) eller manipulasjon av informasjon. Dette kan være sabotasje,virus,utro tjenere,uautorisert endring av konfigurasjoner, men også uhell. Aktiviteter er beskrevet i kapittel 4 -brukeransvar. Økonomiske data er spesielt utsatt for manipulasjon. Sikring av kvalitet vil omfatte:

* Tilgangskontroll
* Datadisiplin, bl.a. ved å holde passord hemmelig for alle.
* Databasekontroll/systemtilganger (ansvar tillagt Dataseksjonen/AD)
* Kommunikasjonskontroll. Ikke la det være åpning for inntregning.
* Kontroll av resultater - fagseksjon

Konfidensialitet

De største utfordringene er knyttet til konfidensialitet for den enkelte seksjon. Aktiviteter i forbindelse med kategorisering av informasjon er en meget viktig oppgave i denne sammenheng. Konfidensialitet berører de fleste områder som er omtalt i kapittel 4. Konfidensialitet vil være knyttet til:

* Sikring av datamedier
* Gjenbruk av disketter med sensitiv informasjon
* Salg av PC'er med disker hvor sensitiv informasjon har vært lagret.
* Beskyttelse av data på hjemme PC'er
* Beskyttelse av all manuell informasjon
* Beskyttelse ved tilgangskontroll (autorisasjon og identer) både til lokale PC'er og sentrale maskiner/servere
* Fysisk sikring av PC'er og lokaler
* Sikring av datanettet

3.2.4 Dokumenthåndtering

Arkivinstruksen gir instrukser om hvordan NVE's dokumenter skal arkiveres og oppbevares. Datasikkerhetsdirektivet inneholder også konkrete tiltak for beskyttelse med datateknisk vinkling. Sikkerhetsinstruksen og Beskyttelsesinstruksen inneholder regler for sikring av informasjon og dokumenter. Dokumenter og datamedier må ses i sammenheng som en del av informasjonsbehandlingen. For behandling av all informasjon, papirbasert og elektronisk, gjelder de samme prinsipper og krav som sikkerhetsdokumentasjonen dekker.

Sikring ved behandling av gradert informasjon gjelder også manuelle dokumenter av enhver art. Dette gjelder bla.a. dokumenter under produksjon, til printer, mottak fra eksternt, intern forsendelse, under behandling, til makulering og lagring.

3.2.5 Lagring av informasjon på lokal disk/disketter

Informasjon bør lagres på de sentrale servere og systemer fremfor lokal PC, fordi man da er:

* sikret daglig sikkerhetskopiering, men med mulighet for tap av informasjon i inntil en dag.
* bedre sikret mht. skjerming av informasjon for innsyn.
* sikret mot at informasjon på PC stjeles (sammen med PC).

Det henstilles derfor til seksjonene å lagre all elektronisk informasjon sentralt. Evt. disketter som benyttes til sikkerhetskopiering (som en ekstra sikkerhet ved sentral lagring) skal oppbevares i låsbare brannsikre skap når de ikke er under direkte oppsyn, dersom det finnes kritisk eller sensitiv informasjon på disse. Reservekopier er ikke nødvendig ved lagring sentralt, og det oppfordres derfor til å ikke ta slike reservekopier, dersom informasjonen ikke anses som kritisk å miste.

Reservekopier/backup ved lokal lagring skal låses inn i brannsikre og låsbare skap og lagres utenfor den bygning hvor PC'er står. Dette er avhengig av kategorisering av den informasjon dette gjelder.

Gradert informasjon som lagres utenfor huset krever helt spesielle sikkerhetstiltak.

Informasjon som graderes etter Sikkerhetsinstruksens gradering KONFIDENSIELT (tabellens kolonne 3) skal ikke tas med utenfor huset eller lagres lokalt. Informasjon med høyere graderinger i Sikkerhetsinstruksen skal lagres helt spesielt. Dersom seksjonen behandler slik informasjon skal dette gjøres i samråd med Dataseksjonen/AD eller SB.

3.3 Sletting av informasjon

Sletting av informasjon bør gjøres av egeninteresse for avdelingen, og må gjøres iht. de lover og regler som gjelder. Av egeninteresse bør det ryddes opp for å få bedre oversikt og enklere gjenfinning av aktuell informasjon. Sletting av informasjon på harddisker må også ses i forhold til sentral lagring og sikkerhetskopi.

3.3.1 Lover og regler - sletting av informasjon

For registre som NVE har konsesjon fra Datatilsynet for å benytte vil krav om sletting være gitt ut i fra konsesjonen. Generelt seet sier Personregisterloven at personopplysninger en ikke lenger har bruk for skal slettes , og dersom det er tvil om opplysningenes riktighet skal dette rettes op eller slettes.

Sikkerhetsinstruksen og Beskyttelsesinstruksen inneholder også detaljerte regler for sletting av informasjon.

Offentlighetsloven begrenser bl.a. det å slette informasjon. Intensjonen er bl.a. å hindre sletting av informasjon av offentlig interesse.

Informasjon underlagt ovennevnte lover og instrukser er avdelingens/seksjonens ansvar å forholde seg til. Det forutsettes at regelverket er kjent for de sim er ansvarlig for denne type informasjon eller registre.

3.3.2 Rutiner og prosedyrer for sletting av informasjon

Informasjon som slettes av egeninteresse kan slettes uten noen form for rutine som ivaretar sikkerheten. Beskyttelsesinstruksen og Sikkerhetsinstruksen samt Datasikkerhets-direktivet somt ar for seg den teknologiske delen av disse setter krav til hvordan informasjon skla slette. I denne sammenheng nevner vi spesielt:

* Krav iht. gradering
* Gjelder alle former for datamedier og papir
* Makulering av datamedier hvor f.eks. sikkerhetskopiermer tatt
* Overskriving eller fjerning av områder kan rekonstrueres - dette må forhindres
* Ved salg av utstyr må det sikres at informasjon ikke kan bli tilgjengelig

Personregisterloven setter ikke så detaljerte krav som nevnt for ovennevnte instrukser, men dersom de samme hensyn tas ved fjerning av personopplysninger er vi på den sikre siden.

3.3.3 Tiltak mot ukontrollert sletting av informasjon

For å redusere risiko for ukontrolert sletting av informasjon kan man på enkelte områder gi Les/kopitilgang for de fleste, slik at det kun er bestemte personer som kan endre eller slettes informasjon. Avdelingen/Seksjonen bør derfor definere områder som erkristisk med hensyn på sletting.

Daglig sikkerhetskopiering av lokale disker vil også sikre at informasjon kun tapes for den dagen sletting skjer.

Sikker oppbevaring av datamedier inkl. sikkerhetskopi er en forutsetning for all informasjon.

Det bør også legges opp til at informasjon ikke slettes ved en feil. Dette kan bla. a. gjøres ved at en må bekrefte kommandoer for fjerning av dokumenter.

Avdelingen/Seksjonen bør gjennomgå sin informasjon og vurdere risiko for - og konsekvenser ved ukontollert sletting av informasjon.

3.4 Fysisk sikring

Beskyttelse av informasjon består av en rekke forskjellige tiltak på forskjellige områder fra datatekniske til manuelle og administrative forhold. Fysisk sikring er et viktig område og vi beskriver derfor dette separat som en oppsummering.

Fysisk sikring må være i overenstemmelse med kategorisering/gradering, og viktighet av den informasjon som seksjonen forvalter

Tiltak for fysisk sikring av seksjonens informasjon kan kort oppsummeres slik:

Avlåsing av seksjonen etter arbeidstid for å sikre datautstyr, disker, tilgjengelige arkiver,dokumenter osv.

Avlåsing av kontorer når ingen er til stede for å sikre utstyr, dokumenter og datamedier.

Innbruddssikre og brannsikre skap for å sikre dokumenter og datamedier mot tap og innsyn. Det kan også være påkrevd å oppbevare harddisker i slike skap.

Ekstern oppbevaring av kopier av dokumenter

Koble vekk modem når dette ikke er i bruk.

Utskrift av gradert informasjon. Det skal være etablert rutiner slik at uautorisert innsyn i gradert informasjon unngås. Man skal straks etter bestilling av utskrift stå ved skriveren, vente og ta ut dokumenter. Ved kø på skriveren, eller utskriftsproblemer, og man blir opptatt med noe annet, slik at nevnte rutine ikke kan følges, skal dokumenter fjernes fra utskriftskøen.

Fysisk sikring av hjemme-PC/bærebar PC og tilhørende data. Disse skal sikres mot uvedkommende og konsekvenser ved f.eks. tyveri må vurderes. Her kan det være krav om nedlåsing av disketter og disk eller kryptering av disk.

Beskyttelse av identer/tilganger ved å holde passord hemmelig og skifte av passord samt å slå av PC når den ikke er i bruk

Lagring av informasjon på lokale disketter og disker

Reservekopi(backup) og lagring av lokale data

Kontroll av ukjente personer I tillegg til at uvedkommende kan få tilgang til datamedier, dokumenter o.l. kan f.eks. personer som utgir seg for å være fra Telenor, eller andre leverandører, enkelt avlytte idnter, passord eller annen informasjon i lokalene. Rutiner for kontroll av ident og kontakt med "oppdragsgiver" er påkrevd dersom ukjente befinner seg i lokalene.

Ovennevnte tiltak må vurderes av seksjonssjef som ansvarlig og øvrige medarbeidere iht. hva slags informasjon som skal beskyttes.

4. ANSVAR OG OPPGAVER TILLAGT DEN ENKELTE BRUKER

4.1 Ansvar tillagt den enkelte bruker

4.1.1 Oppsummering brukeransvar

Den enkelte bruker er ansvarlig for å følge de retningslinjer som er nedfelt i "Sikkerhetsdokumentasjonen".
Brukeren skal uten opphold rapportere sikkerhetsbrudd til nærmeste overordnede i linjeledelsen.
Brukeren må også ha et bevisst forhold til hvilke data som må beskyttes. Til dette kan tabellen i "Vedlegg 1 - Sikkerhetsdokumentasjonen" være til hjelp.

4.1.2 Brukerinstruks

Nedenfor er de gjeldende instrukser beskrevet. Hvordan man konkret skal forholde seg til instruksen er omtalt senere i kapittel 4.

* **Brukeren skal til enhver tid gjøre det som er mulig for å bekjempe datavirus på egen (og andres) PC.**

* **Brukeren skal ta de nødvendige forholdsregler for å sikre sin bærbare PC eller hjemme PC.**

* **Brukeren skal vurdere nøye hvilke data som kan lagres på den bærbare PC eller hjemme PC.**

* **Brukeren skal selv sørge for kopiering av data som er lagret lokalt på PC.**

* **Alle brukere bør bruke en passordbeskyttet skjermbeskytter.**

* **Brukeren skal selv sørge for å skifte passord.**

* **Brukeren skal umiddelbart rapportere sikkerhetsbrudd.**

* **Brukeren skal aldri sende sensitive data til en skriver uten å ta spesielle forholdsregler.**

* **Det er forbudt å lagre enbrukerversjoner av programvare og spill på NVE's nettverksdisker.**

* **Alle medarbeidere er ansvarlig for å ha det nødvendige kompetansenivå for å ivareta NVE's bestemte sikkerhetsnivå. Er man i tvil så skal nærmeste overordnede og/eller Dataseksjonen kontaktes for nærmere opplysninger.**

4.2 Sikkerhetstiltak (tiltak, rutiner og prosedyrer)

4.2.1 Datavirus

Den vanligste årsaken til virusinfeksjon er bruk av disketter som kommer fra andre systemer.

Blandt 'andre' systemer er den private hjemme PC en av de smittekildene som er mest utbredt. Grunnen til at en PC som står hjemme ofte kan være årsaken til et virusangrep, er at disse PC'ene ofte også blir brukt til forskjellige spill.
De som lager et virus bruker ofte spill for å få spredt det. Lager man da et dokument hjemme, for deretter å ta det med seg på diskett til kontoret, kan viruset bli overført til NVE's datasystemer.

Datavirus kan også komme inn i NVE's systemer via disketter eller datalinjer fra eksterne brukere, og den økende bruken av bærbare PC'er vil etter hvert bli en betydelig trussel for datasikkerheten i NVE, hvis ikke mottiltak gjennomføres.

Tiltak for bekjempelse av datavirus.

1. Alle disketter som skal brukes i NVE skal virustestes først

2. Alle bærbare (eller stasjonære) PC'er som har vært tilkoblet andre nett, eller brukt disketter som ikke er virustestet i NVE, skal testes i sin helhet før de taes i bruk i NVE's datanett.

3. Det er ikke tillatt å piratkopiere programvare.

4. Disketter skal kun legges inn dersom man kjenner avsender (som en seriøs samarbeidspartner) og man vet hva innholdet er og hva det skal brukes til. Legg aldri inn tilfeldige demonstrasjonsprogrammer som følger med tidskrifter, deles ut på messer o.l.

5. Vis stor aktsomhet ved kopiering av såkalt " fri programvare" som tilbys på Internet. Slik programvare skal under ingen omstendighet legges ut på NVE's interne nett

6. Alle PC'er skal virustestes med jevne mellomrom.

7. Hvis virus oppdages skal PC'en slås av og Dataseksjonen/AD skal varsles umiddelbart.

4.2.2 Hjemme PC

Etterhvert som utbredelsen av hjemme PC'er øker kan problemene dette skaper for IT-sikkerheten i NVE bli store, hvis vi ikke tar en del forholdsregler.

<u>Backup</u>
Blir det lagret dokumenter på PC'en, må disse med jevne mellomrom kopieres til disketter. Harddisken på PC'en vil før eller siden ryke. Uten kopi vil dataene være tapt.

Viruskontroll
Spilleprogrammer o.l. må kun legges inn på PC'en fra forseglede originale disketter.
NVE's antivirusprogrammer kan kopieres til den enkelte ansattes hjemme PC. Ta kontakt med Dataseksjonen/AD.

Kopiering av programvare
1. All kopiering av programvare er i følge norsk lov forbudt, medmindre det er spesielle avtaler mellom leverandør og bruker om dette.
2. NVE har inngått slike avtaler med en del leverandører.
3. Pr. juni 1995 kan følgende program kopieres til ansattes hjemme PC'er:
   F-prot Virus Control
   Word Perfect
   Lotus 1-2-3
   Freelance Graphics

Graderte dokumenter.
Graderte dokumenter bør ikke brukes på en hjemme PC. Hvis noen må bruke graderte dokumenter hjemme må PC'en beskyttes særskilt med kryptering, innelåsing ol.
Opplysninger som ikke er gradert, men som kan skade NVE eller andre i forbindelse med informasjonslekkasje skal heller ikke lagres ukryptert.
Informasjon gradert etter Sikkerhetsinstruksen skal ikke lagres eksternt (utenfor NVE).

4.2.3 Bærbare PC'er

Bærbare PC'er er populære objekter for tyver. Vurder derfor svært nøye hvilke data du lagrer før du tar den med deg ut av NVE. Merk at data fra og med kolonne 1 (Tabell - Vedlegg 1) skal holdes nedlåst.

4.2.4 Backup

Med det datanettverket NVE nå har, burde problemene med backup av egen PC være eliminert. Alle bevaringsverdige dokumenter kan lagres på en enkel måte på de sentrale nettverksdiskene. Dataseksjonen sørger for at disse blir kopiert hver dag.

Lokal lagring av sensitive data forutsetter at du har en utskiftbar harddisk som kan låses inn, eller at du kun lagrer på disketter som oppbevares nedlåst.

Den enkelte bruker er selv ansvarlig for forsvarlig backup av det som lagres lokalt.

4.2.5 Utlogging

Hvis du er inlogget på en av Unix maskinene med brukernavn og passord, skal ikke PC'en forlates før du er utlogget.

4.2.6 Skjermbeskytter

En effektiv måte å hindre andre i å komme inn på dine private områder på fellesdiskene, selv om du er innlogget, er å benytte den beskyttelsen du kan få i Windows/Kontrollpanel/ Skrivebord/Skjermbeskytter.(Forutsetter Windows 3.1 eller nyere).
Hvis du legger inn passord her må de som ikke kjenner passordet skru PC'en av og på for å få brukt den, men da kobles nettverksdiskene fra.

4.2.7 Passordskifte

Passordet skal bestå av minst 6 tegn, og det må være en blanding av karakterer og tall. Bruk aldri egennavn eller ord du finner i en ordliste.
Passord skal ikke skrives ned eller lånes ut til andre.
Alle bør skifte passord en gang i blandt. Hvor ofte, er avhengig av hvilke data som behandles.
Maksimums varighet for et passord skal være 6.mnd.
Bruksanvisning for passordskifte finnes i "Brukerveiledning for basis maskin og programvare i NVE"

4.2.8 Rapportering av sikkerhetsbrudd

Et sikkerhetsbrudd er enhver hendelse som har, eller kunne ha, resultert i tap eller skade på organisasjonens verdier, eller en handling som er et brudd på organisasjonens sikkerhetsprosedyrer.

Sikkerhetsbrudd skal umiddelbart rapporteres til nærmeste overordnede og Dataseksjonen/AD.
Bruk "Skjema for rapportering av sikkerhetsbrudd"

Vi kan da oppnå følgende:
- skaffe oversikt over kildeproblemer
- avdekke behov for opplæring
- bidra til endrede rutiner og prosedyrer for sikrere drift
- bidra til å rekonstruere problemer i ettertid.

4.2.9 Sikring av utskrifter

Papirutskrifter, inneholdende graderte data, skal ikke sendes ut til felles skrivere uten at det taes spesielle forholdsregler.

* Utsenderen skal stå ved skriveren når utskriften kommer.
* Hvis utskriften av en eller annen grunn ikke kommer, skal den umiddelbart fjernes fra utskriftskøen. Dataseksjonen kan, om ønskelig, være behjelpelig med dette.

4.2.10 Bruk av fellesdisker

Alle i NVE kan lagre data på nettverksdiskene (Eks; M: , F: , K:)
Det er imidlertid ikke tillatt å lagre enbruker versjoner av programvare eller spill på disse diskene, og om så skjer vil det bli ansett som sikkerhetsbrudd og behandlet deretter.

4.2.11 Endring av PC oppsett

Det er ikke tillatt å endre grunnoppsettet (DOS, Nettverksprogramvare) på PC'er som er knyttet til NVE's datanett, uten på forhånd å ha konsultert Dataseksjonen/AD.

4.2.12 Forsendelse og mottak av disketter eller andre datamedier

All forsendelse av datamedier i form av disketter, taper, harddisker eller annet må ikke inneholde opplysninger som kan skade NVE eller andre. Alle disketter som sendes ut skal være ubrukte for å sikre at "gammel" informasjon ikke blir tilgjengelig for uvedkommende.

4.2.13 Service på PC

PC'er med informasjon om NVE eller andre, som kan skade NVE eller andre dersom informasjonen blir kjent for uvedkommende, skal aldri avleveres for service eller lånes bort. Ved behov for service på slike PC'er skal Dataseksjonen/AD kontaktes.

4.2.14 Bruk av Internet

Den sterkt økede bruk av Internet i NVE medfører fare for virusangrep, så selv om tilgangen utenfra og inn til NVE's datanett er sterkt begrenset, bør vi ta noen enkle forholdsregler:

* Ikke bruk PC-baserte produkter som grensesnitt mot Internet (eks; Mosaic for Windows), da disse produktene, i motsetning til Unix baserte produkter, ofte brukes som inngangsportal til interne datanett.
* Det er ikke tillatt å hente programvare(free-ware) på nettet for deretter å gjøre denne tilgjengelig på NVE's datanett.

VEDLEGG 1 - TABELL FOR KATEGORISERING AV INFORMASJON

VEDLEGG 2- SKJEMA FOR RAPPORTERING AV SIKKERHETSBRUDD

VEDLEGG 3-SKJEMA FOR AUTORISERING

VEDLEGG 4- DEFINISJONER AV ORD OG UTTRYKK

VEDLEGG 1

Informasjonssikkerhet i NVE

	0	1	2	3
HENV. LOV/ GRADERING	Ingen	Personregisterloven/ Forvaltningsloven (dok. m/t.plikt)	Beskyttelsesinstruksen FORTROLIG Sikkerhetsinstruksen BEGRENSET (**)	Beskyttelsesinstruksen STRENGT FORTROLIG Sikkerhetsinstruksen KONFIDENSIELT (***)
EGENPROD. DOKUMENTER	- D u/ oppl. om P/F/I - D u/oppl. som kan skade NVE eller andre - D m/ liten betydning dersom disse går tapt	- D m/oppl. om P/F/I - D m/oppl. om NVE som ikke skal off.gjøres - D m/oppl om andre/annet som ikke skal off.gjøres - D hvor ekstraarbeid er påkrevd dersom disse går tapt - Konsesjonsplikt (*)	- D m/oppl. om P/F/I, NVE eller det off. som kan skade disse dersom innhold blir kjent for uvedkommende - D dersom disse går tapt medfører problemer og kostnader og rekonstruere	D m/oppl. om P/F/I, NVE eller det off. som kan gjøre betydelig skade for disse dersom innhold blir kjent for uvedkommende - D dersom disse går tapt medfører store kostnader, betydelige problemer å rekonstruere
EKSTERNE DOKUMENTER	- Som ovenfor - D som ikke er påført gradering	- D m/oppl. om P/F/I - D m/oppl. om NVE som ikke skal off.gjøres - D m/oppl om andre/annet som ikke skal off.gjøres - Dok. som vanskelig kan fås på nytt fra avsender/kilde	- D m/oppl. om P/F/I, NVE eller det off. som kan skade disse dersom innhold blir kjent for uvedkommende - D dersom disse går tapt medfører problemer og kostnader og rekonstruere - D som ved manipulasjon/ feilaktig endring kan gjøre skade	D m/oppl. om P/F/I, NVE eller det off. som kan gjøre betydelig skade for disse dersom innhold blir kjent for uvedkommende - D dersom disse går tapt medfører store kostnader, betydelige problemer å rekonstruere - D som ved manipulasjon/ feilaktig endring kan gjøre betydelig skade
TILTAK KONFIDENS.	- Ingen, men må vurderes av SB	- Need to know-prinsippet må følges - Tilgangskontroll - Rutine for print - Begr. lovlig innhold - D skal låses ned - Taushetserklæring	- Spesiell klarering av personell med tilgang - Taushetserklæring - Kryptering v/transmisjon - Datamedier ut av huset skal være kryptert (inkl. hjemme-PC og bærbar PC/spes. beh) - Sikre print mot innsyn - Regler for sletting av informasjon - Lagrinsmedia overskirves 7 g.anger (salg/service) - Krav til konfigurasjonskontroll - Krav til fysiske sikringstiltak i miljøet rundt utstyr/nett/kabling - Aksesskontroll mot pereferiutstyr (printere ol)	- Spesiell klarering av personell med tilgang - Sikkerhetsklarering - Temptest trusselvurdering - Kryptering v/transmisjon og nett utenfor kontrollert område - Datamedier skal ikke ut av huset. (evt. destruksjon før dette tas ut) - Spes. beh. v/forsendelse - Forsendelse: REK/verdi - Sikre print mot innsyn
TILTAK KVALITET	- Ingen, men må vurderes av SB	- Oppl. om P/F/I skal sikres korrekt innhold - Kontroll vurderes av SB	- Prosedyre/rutine for sikring mot manipulasjoner/endr.	- Prosedyre/rutine for sikring mot manipulasjoner/endr. - Godkjent/klarert utstyr
TILTAK TILGJENGELIG	- Ingen, men må vurderes av SB	- Backup skal oppb. låst og eksternt - Daglig backup - Kopier skal være nedlåst	- Backup skal oppb. låst og eksternt/sikres mht. tilgang - D/Datamedier nedlåst - Krav til fysiske sikringstiltak i miljøet rundt utstyr/nett/kabling	- Backup skal oppb. låst og eksternt/sikres mht. sikkerhets-klarering - D/Datamedier nedlåst i spes. stålskap

* For registre/databaser med spesiell konsesjon kan ytterlige krav være spesifisert av Datatilsynet

** For sikkerhetsinstruksen gjelder i tillegg spesiell autorisering. Konf. forklaring hvor sammenkobling av registre kan kreve høyere gradering

*** Som (**). Dersom informasjon i kategori 3 behandles skal sikkerhetskrav tilrettelegges i samråd med Dataseksjonen

For sikkerhetstiltak i kolonner med høyere nummer, gjelder også sikkerhetstiltak som er beskrevet i lavere kolonner dersom dette ikke fremkommer

Informasjonssikkerhet i NVE - Vedlegg 1 -forkortelser

D	Dokument, brev, notater, saksmapper. Gjelder også dokumenter i form av filer
evt.	Eventuelt
F	Foretak, firmaer eller offentlig virksomhet
I	Institusjoner, foreninger, stiftelser eller organisasjoner
inkl.	Inkludert
m/	Med
mht.	Med hensyn til
off.	Offentlig
ol.	Og lignende
oppb.	Oppbevares
oppl.	Opplysninger/informasjon
P	Person
P/F/I	Konferer P, F og I
REK	Rekommandert
SB	Saksbehandler
Spes.	Spesiell
u/	Uten
v/	Ved

SKJEMA FOR RAPPORTERING AV SIKKERHETSBRUDD

Rapport av:

Navn:
Avdeling:
Dato:
Rapport til:

Mottatt i Dataseksjonen:

Signatur:
Dato:
Arkivnr:

Forklaring sikkerhetsbrudd:

(Bruk evt. tilleggsark)

Sikkerhetsbruddet gjelder følgende utstyr (der utstyr er involvert):

□ Frittstående PC □ PC i nett verk □ Terminal □ Annet:_____

Type sikkerhetsbrudd:

□ Uvedkommende kjenner passord □ Tyveri av PC □ Sabotasje

□ Uautorisert innsyn □ Piratkopiering □ Virus

□ Uforklarlig hendelse/PC □ Info-lekkasje □ Manglende backup

□ Endring av konfigurasjon □ Brudd på instruks □ Manglende kryptering

□ Tap av data □
Annet:_____

Forklaring (type sikkerhetsbrudd/konsekvens):_____

OPPFØLGING I DATASEKSJONEN

Status problem:

Tiltak iverksatt:

Oppfølging:

Viderapport til:_____ Rapport av:_____ Dato:_____

AUTORISERING AV NYE BRUKERE

Navn	
Seksjon	Initialer
Ansettelses dato	Sluttdato

Trenger tilgang til/Skal fjernes fra følgende databaser:

Databasenavn	Tilganger

Underskrift seksjonssjef/avdelinsdirektør:_____

Skjemaet sendes til Dataseksjonen/AD og de aktuelle databaseadministratorer

VEDLEGG 4

Informasjonssikkerhet i NVE

DEFINISJONER OG FORKLARINGER AV ORD OG UTRYKK

Autentisering
Det er prosessen for å bekrefte en oppgitt ident. Autentisering skal sikre at systemet til enhver tid kjenner riktig ident til de som bruker systemet. Brukerenes ident benyttes ved tilgangskontroll og logging.

Autorisasjon
Skriftlig godkjenning av at en person gis adgang til informasjon av en gitt kategori eller gradering eller adgang til et system.

Brukerprofil
En brukers tilganger og rettigheter til systemer. Brukerprofilen forteller hvilke systemer han har tilgang til og hva han har lov til å foreta seg i disse systemer. Det kan utarbeides standard "brukerprofiler", hvor en bruker blir knyttet til en på forhånd definert profil.

EDB-sikkerhet
Sikre informasjonens kvalitet/integritet, tilgjengelighet og konfidensialitet i og rundt EDB-systemer. EDB-sikkerhet er den delen av informasjonssikkerhet som er knyttet til maskiner, systemer og nettverk. Se pkt. 2.1 i håndboka for mer utdypende forklaring.

Fysisk sikring
Fysisk sikring er fysiske og tekniske hindringer satt sammen for å forhindre, oppdage eller begrense inntrengning av forskjellige slag. Dette kan være manuelle tiltak som f.eks. inngangskontroll og nedlåsing av datamedier eller tekniske tiltak som f.eks. å begrense ødeleggelser fra strømnettet.

Informasjonssikkerhet
Sikre informasjonens kvalitet/integritet, tilgjengelighet og konfidensialitet. Dette gjelder all informasjon uansett om denne ligger i et EDB-system, i et arkiv, som et notat eller på datamedier. Informasjonssikkerhet dekker også informasjon i form av tale, telefon og fax. Se pkt. 2.1 i håndboka for mer utdypende forklaring.

Instrukser
Instrukser er i NVE noe de ansatte er pålagt å rette seg etter og må oppfattes som en del av de oppgaver og ansvar som er tillagt stillingen. NVEs sikkerhetsinstrukser vil være en del av stillingsinstruksen, for de av de ansatte som har slike.

Konfidensialitet
Konfidensialitet er å sikre at informasjon ikke blir kjent for uvedkommende.

Konsekvens
Konsekvens i forbindelse med informasjonssikkerhet er den faktiske betydningen et sikkerhetsbrudd får eller kan få.

Kritisk informasjon
Informasjon som kan gjøre betydelige skade for NVE eller andre dersom denne blir kjent for uvedkommende.
Informasjon som av en eller annen grunn ikke blir tilgjengelig, og en slik situasjon kan påføre NVE eller andre betydelig skade.
Dersom informasjonen (kvalitet) blir forringet, manipulert eller feilaktig vil dette kunne medføre betydelig skade for NVE eller andre.

Kvalitet (Informasjonskvalitet)
Blir også ofte omtalt som informasjonsintegritet. Forsikring om at informasjonen er korrekt og adekvat representerer informasjonen i et objekt.

Reservekopi (backup)
En kopi av den informasjon som skal sikres dersom originalen blir ødelagt ved ett uhell, sabotasje e.l. Dette kan være reservekopier i form av papir på eksempelvis et fjernlager eller kopier av datafiler eller databaser på datamedier.

Risiko
Risiko indikerer sannsynnligheten for at en trussel utvikler seg til et sikkerhetsbrudd.

Sårbarhet
Sårbarhet er et "produkt" av hvilke trusler som finnes, hvilken risiko det er for at disse skal inntreffe og hvilke konsekvenser ett sikkerhetsbrudd kan få.

Sikkerhetsbrudd
Sikkerhetsbrudd må ses i sammenheng med målet for informasjonssikkerhet som er å forhindre at informasjonen blir tilgjengelig for uvedkommende, informasjonen blir forringet/ødelagt eller at informasjonen ikke blir tilgjengelig. Sikkerhetsbrudd inntreffer dermed når NVE ikke klarer å ivareta målet. Sikkerhetsbrudd er i NVE definert som:
1) Skade på fysisk utstyr, dokumenter og arkiv
2) Informasjonen er ikke lenger korrekt og fullstendig
3) Informasjonen er ikke tilgjengelig for autorisert bruk
4) Informasjonen er tilgjengelig for ikke autoriserte personer

Sikkerhetsdokumentasjon
Felles begrep for all den dokumentasjon som finnes om informasjonsikkerhet i NVE. Dette er i form av håndbok informasjonssikkerhet, instrukser, skriv som omhandler informasjonssikkerhet og sikkerhetsrutiner (driftsrutiner ol.) som foreligger for de enkelte system eller som er av generell karakter.

Sikkerhetsklarering
Prosess for å klarere en ansatt for tilgang til gradert informasjon. Dette er en prosess hvor også eksterne er involvert

Sikkerhetstiltak
Tiltak som har til formål å unngå sikkerhetsbrudd og dermed ivareta NVEs mål med informasjonssikkerhet. Dette kan være tekniske tiltak hvor ansvaret ligger hos Dataseksjonen eller hos den lokale enhet. Dette kan også være tiltak av ren fysisk karakter.

Tilgjengelighet
Tilgjengelig i forbindelse med informasjonssikkerhet dekker tilgjengelighet til papirer i alle slag former, dokumenter i arkiv, informasjon lagret på lokale PC'er og informasjon lagret på sentrale servere og maskiner. Sikring av tilgjengelighet innebærer dermed også forholdet til forsendelser ol.

Trussel
En hendelse/forhold som kan gi opphav til sikkerhetsbrudd.

Denne serien utgis av Norges vassdrags- og energiverk (NVE)
Adresse: Postboks 5091 Majorstua, 0301 Oslo

I 1995 ER FØLGENDE NOTATER UTGITT:

Nr 1 IKKE OFFENTLIG

Nr 2 Østen A.Tilrem: Tensiometeret. (21 s.)

Nr 3 Nils-Otto Kitterød: Geostatistikk i geohydrologi. (13 s.)

Nr 4 Marleen v. Stam Rydehell (red.): NVEs IT-strategi (21 s.)

Nr 5 Per Einar Faugli: Ressursforvaltning og geofag. (s.)

Nr 6 Marleen van Stam Rydehell (red.): Handlingsplan for NVEs IT-strategi. (29 s.)

Nr 7 Erik Fagerberg (red.): IT-sikkerhetsdokumentasjon. (30 s.)