UiT

NORGES
ARKTISKE
UNIVERSITET

Styringssystem for informasjonssikkerhet

7.1.2015

http://www.colourbox.c

UNIVERSITETET I TROMSØ

Styringssystem for informasjonssikkerhet

Innhold

1 Innledning 1

1.1 Formål og hensikt 1

1.2 Styringssystemet for informasjonssikkerhet ved UiT 1

1.3 Avgrensning av styringssystemet 2

1.4 Behandlingsansvarlig og databehandlere 2

2 Sikkerhetspolicy 3

2.1 Sikkerhetsmål 3

2.2 Sikkerhetsstrategi 3

2.3 Klassifisering av informasjon 4

2.4 Akseptabel risiko 5

3 Roller, ansvar og oppgaver 6

4 Risikovurdering 9

5 Opplæring 10

6 Kontroll og oppfølging 11

6.1 Internrevisjon 11

6.2 Rapportering av avvik 11

6.3 Ledelsens gjennomgang 11

7 Vedlegg 13

7.1 Relevant regelverk 13

7.2 Prosedyrer, instrukser og rutiner 13

7.3 Mal for ROS- vurdering (risiko- og sårbarhetsvurdering) 13

7.4 Mal for databehandleravtale fra Datatilsynet 13

7.5 Mal for leverandøravtale 13

1 Innledning

1.1 Formål og hensikt

Universitetet i Tromsø – Norges arktiske universitet (UiT) er et nasjonalt og internasjonalt kraftsenter for kompetanse, vekst og nyskaping i nordområdene. Dette skal blant annet vises gjennom høy kvalitet på UiTs kunnskapsforvaltning og informasjonsverdier: forskningsdata, forskningsresultater og informasjon eller kunnskap som inngår i undervisning, forskning og formidling.

Et systematisk og planmessig arbeid for å sikre våre informasjonsverdier er derfor en sentral del av UiTs kunnskapsforvaltning. Både interne og eksterne aktører - ledere, ansatte, studenter, samarbeidspartnere og offentligheten for øvrig - skal kunne stole på at UiT ivaretar

1. informasjonens konfidensialitet - vi beskytter sensitiv eller viktig informasjon mot uautorisert innsyn, tilgang eller misbruk,
2. informasjonens integritet - vi beskytter sensitiv eller viktig informasjon mot uautorisert endring eller sletting,
3. informasjonens tilgjengelighet - vi sørger for at all informasjon er tilgjengelig for alle som skal ha tilgang til den.

UiT er underlagt en rekke lover og forskrifter som pålegger oss å ha tilfredsstillende informasjonssikkerhet. Dette gjelder blant annet forvaltningsloven med forskrift (e-forvaltningsforskriften), personopplysningsloven med forskrift og helseforskningsloven med forskrift. I tillegg inneholder andre lovverk, blant annet offentlighetsloven og arkivloven, bestemmelser som har betydning for arbeidet med sikring av informasjonen ved UiT. I Kunnskapsdepartementets (KD) tildelingsbrev til UiT for 2014 kreves det innføring av et styringssystem for informasjonssikkerhet som bygger på grunnprinsippene i anerkjente sikkerhetsstandarder. Styringssystemet for informasjonssikkerhet ved UiT ivaretar de kravene som lovverket og KD stiller til arbeidet med informasjonssikkerhet i universitets- og høyskolesektoren.

1.2 Styringssystemet for informasjonssikkerhet ved UiT

Styringssystemet for informasjonssikkerhet skal sørge for at UiTs informasjonsverdier håndteres på en systematisk, planmessig og tilfredsstillende måte. I dette dokumentet beskrives hovedtrekkene i styringssystemet, det vil si mål, strategi og organisering av arbeidet med informasjonssikkerhet. Styringssystemet inneholder blant annet beskrivelse av roller og ansvar, oversikt over informasjonsverdier og retningslinjer.

Styringssystemet består av tre hovedelementer:

1. Styrende - overordnet policy, herunder sikkerhetsmål og -strategi, roller og ansvar.
2. Gjennomførende - risikovurderinger samt konkrete rutiner og retningslinjer i vedleggene.
3. Kontrollerende – internrevisjon, rapportering av avvik og ledelsens gjennomgang.

1.3 Avgrensning av styringssystemet

Informasjonssikkerhet er et topplederansvar. Det operative ansvaret og det praktiske arbeidet med å ivareta informasjonssikkerheten kan delegeres til de enkelte enhetene ved UiT, jf. beskrivelsen av sikkerhetsorganisasjonen med roller og ansvar i punkt 3.

Styringssystemet for informasjonssikkerhet ved UiT omfatter

- alle brukere av UiTs IT-ressurser[1]
- alle UiTs studiesteder/campuser
- alle organisatoriske enheter[2]
- all teknologi[3]
- alle informasjonsverdier

Med informasjonsverdier menes utstyr, prosesser eller data som er tilknyttet informasjon og som virksomheten anser som nødvendig å beskytte. Hvordan man skal beskytte informasjonsverdiene avhenger av resultatene fra risikovurderinger. Informasjonssikkerhet knyttet til data er medie- og formatuavhengig, gjelder både informasjon som lagres og brukes i mobile enheter, cd-rom og på papir. Det kan være et IT-system, for eksempel personalsystem, læringsplattform og arkivsystem, eller en type informasjon, for eksempel studentinformasjon, pasientinformasjon eller data som inngår i et forskningsprosjekt.

1.4 Behandlingsansvarlig og databehandlere

To sentrale begrep går igjen i styringssystemet og personvernlovgivningen; behandlingsansvarlig og databehandler. Den behandlingsansvarlige er den som bestemmer formålet med behandlingen av personopplysninger, og hvilke hjelpemidler som skal benyttes. Databehandleren er den som behandler personopplysninger på oppdrag fra den behandlingsansvarlige. Det skal alltid inngås en databehandleravtale før eksterne aktører kan behandle personopplysninger for UiT, også i småskala.

[1] Studenter, ansatte, gjester, samarbeidspartnere etc.
[2] Avdelinger, fakulteter, institutter, sentre, museum, databehandlere
[3] IT-systemer, datanettverk, databaser/-registre etc.

2 Sikkerhetspolicy

God informasjonssikkerhet skal bidra til at UiT oppnår sine strategiske målsettinger og ivaretar sitt samfunnsoppdrag. Konfidensialitet, integritet og tilgjengelighet for UiTs informasjonsverdier skal ivaretas på en enhetlig og systematisk måte i hele organisasjonen. Informasjonsverdiene skal være tilgjengelig for de som skal ha tilgang (tilgjengelighet), de skal sikres mot utilsiktet og urettmessig endring (integritet), og de skal ikke være tilgjengelig for uvedkommende (konfidensialitet).

2.1 Sikkerhetsmål

Sikkerhetsmålene skal understøtte UiTs kjerneområder utdanning, forskning og formidling.

Følgende sikkerhetsmål skal oppnås:

- Arbeidet med informasjonssikkerhet skal til enhver tid være i tråd med de krav som stilles i lov og forskrifter som gjelder for UiT.
- Informasjonen som behandles ved UiT skal ha riktig sikkerhetsnivå basert på klassifisering og risikovurderinger.
- Ansatte, studenter, besøkende og samarbeidspartnere skal være kjent med UiTs krav til informasjonssikkerhet og etterleve disse kravene.
- UiT skal sørge for at sentrale tjenester, infrastruktur og informasjon er pålitelig og tilgjengelig for de som skal ha tilgang. Avvik og ekstraordinære hendelser skal håndteres på en planmessig og forutsigbar måte.

2.2 Sikkerhetsstrategi

Arbeidet med informasjonssikkerhet er viktig i alle ledd av organisasjonen. Sikringstiltakene skal være både av teknisk, organisatorisk og personellmessig karakter.

Følgende strategi er førende for hvordan UiT skal oppnå sine sikkerhetsmål:

- UiTs sikkerhetsorganisasjon med tilhørende roller og ansvar skal være tydelig og kjent.
- Ledere har et særskilt ansvar for sikkerheten, og skal gis nødvendig opplæring og oppfølgning. De skal tilrettelegge for god informasjonssikkerhet innen sitt ansvarsområde og følge dette opp på lik linje med økonomi- personal- og fagansvar.
- Opplæring og tilgjengelige retningslinjer skal bidra til at den enkelte ansatte og student skal være i stand til å etterleve kravene til informasjonssikkerhet.
- Det skal være en felles tilnærming til risikovurderinger med tilhørende akseptkriterier, jf. punkt 2.4.
- UiT skal etablere og ivareta kontinuitets- og beredskapsplaner for kritiske tjenester og infrastruktur.
- Styringssystem for informasjonssikkerhet og underliggende rutiner og policyer skal revideres jevnlig og minst hvert tredje år.

- Universitetets informasjonsbehandling skal beskyttes mot alle identifiserbare trusler. Dette omfatter både interne og eksterne, samt tilsiktede og utilsiktede, trusler.
- Sikkerhetstiltak skal forhindre at ansatte, studenter og andre skal kunne forårsake informasjonssikkerhetsbrudd, både uaktsomt og forsettlig.

2.3 Klassifisering av informasjon

En forutsetning for å kunne si noe om behovet for sikkerhetstiltak er at det er foretatt en klassifisering av informasjonen som behandles. Blant annet så er det nødvendig med en slik oversikt for å oppfylle plikter i personopplysningsloven med forskrift. Dette innebærer for eksempel å etablere formål og hjemmel til å behandle personopplysninger, plikt til å gi innsyn og informasjon, samt ivareta melde- og konsesjonsplikt. All informasjon skal klassifiseres med hensyn til akseptabelt sikkerhetsnivå, tilgangsbegrensning og akseptabel bruk. Denne klassifiseringen er med på å avgjøre hvilken grad av sikring, både IT-teknisk og fysisk, informasjonen skal underlegges.

Klassifisering av informasjon er delt inn i tre nivåer[4]:

1. **Åpen** informasjon er informasjon der det ikke påhviler noen restriksjoner for hvem som kan ha tilgang. Denne informasjonen kan fritt sendes i e-post, per post og lagres hos tredjepart uten spesiell avtale. Denne informasjonen kan behandles og lagres på alle deler av UiTs IT-systemer. Eksempler kan være en nettside som presenterer UiT som virksomhet eller beskriver en enhet, eller studiemateriell for et emne eller kurs som ligger åpent men som likevel er merket med lisens eller opphavsrett.

2. **Intern** informasjon er informasjon som er beregnet kun på ansatte eller studenter ved UiT, eller andre navngitte enkeltpersoner eller grupper som UiT samarbeider med. Dette omfatter blant annet informasjon som er unntatt offentlighet, upubliserte artikkel- eller bokmanus, ikke-konfidensielle forskningsdata som ikke er godkjent for publisering/offentliggjøring av prosjektleder, utkast til strategier/planer eller ikke-publiserte forslag til forskningsprosjekter.[5]

3. **Konfidensiell** informasjon er informasjon som er omfattet av lovbestemt og avtalemessig taushetsplikt. Dette kan være taushetsbelagt informasjon, sensitive personopplysninger, konfidensielle forskningsdata, medisinske data, økonomiske data eller data med konfidensialitetsklausuler. Denne informasjonen skal kun være tilgjengelig for medarbeidere med strengt kontrollerte rettigheter. I spesielle tilfeller kan konfidensiell eller sensitiv informasjon også gjøres tilgjengelige for eksterne aktører, for eksempel når personopplysninger etter spesielle avtaler skal formidles til andre. Dette skal i så fall skje under de samme strengt kontrollerte tilgangsrettighetene som gjelder for UiTs egne medarbeidere med slike rettigheter. Slik informasjon kan ikke lagres hos tredjepart uten at det

[4] Nivåene samsvarer med det som er anbefalt i UNINETTs Fagspesifikasjon - UFS136: Retningslinjer for klassifisering av informasjon (https://www.uninett.no/webfm_send/758).

[5] Jf. Uninetts veileder i styringssystem for informasjonssikkerhet i UH-sektoren versjon 1.0 s. 16

finnes en spesifikk avtale for dette. All overføring og behandling av konfidensiell informasjon må sikres tilstrekkelig mot uautorisert innsyn.

2.4 Akseptabel risiko

Ved all informasjonsbehandling eksisterer det en risiko for brudd på kravene om integritet, konfidensialitet og tilgjengelighet. Det er derfor viktig å ha en forsvarlig risikostyring. For å oppnå dette må det fastsettes kriterier man kan styre etter (akseptkriterier), slik at det er mulig å avgjøre når en risiko overstiger et på forhånd akseptert nivå. Dette nivået betegnes som akseptabel risiko, og kan omtales som den risikoen UiT godtar i informasjonsbehandlingen. Denne vurderingen er ikke nødvendigvis fritt opp til UiT å avgjøre, men kan også være underlagt lovpålagte krav[6].

For å oppnå tilfredsstillende informasjonssikkerhet skal informasjonen klassifiseres enten som åpen, intern eller konfidensiell, jf. punkt 2.3. Det presiseres at dette gjelder både elektroniske og fysiske data.

UiT har fastsatt følgende kriterier for informasjonssikkerhet innenfor UiTs kjerneområder;

Personopplysninger

- Universitetet behandler personopplysninger av stor betydning for studenter og ansatte, herunder opplysninger om søkere til studieplasser, tidligere studenter/ansatte og søkere til fond som universitetet forvalter. Feil i disse opplysningene kan medføre forsinkelser og økonomisk tap for denne gruppen.
- For personopplysninger aksepteres ikke brudd på konfidensialitet eller integritet. Dette gjelder i særlig grad for sensitive personopplysninger[7]. Kortere avbrudd i personopplysningers tilgjengelighet aksepteres.

Forskningsdata

- Det må skilles mellom forskningsdata som ikke er klar for publisering og forskningsresultater som kan publiseres.
- Det aksepteres ikke brudd på konfidensialiteten og integriteten til konfidensielle forskningsdata som ikke er godkjent for publisering/offentliggjøring av prosjektleder. Kortere avbrudd i forskningsdataens tilgjengelighet aksepteres.
- For forskningsresultater som er klar for publisering skal tilgjengelighet og integritet prioriteres foran konfidensialitet.
- Elektroniske systemer som benyttes til lagring av forskningsdata skal oppfylle kravene til oppbevaring av personidentifiserende opplysninger stilt i personopplysningsloven med forskrift.

[6] Eksempelvis for personopplysninger så inneholder personopplysningsforskriften flere bestemmelser for ivaretakelse av tilfredsstillende informasjonssikkerhet.

[7] I personopplysningsloven § 2 defineres sensitive personopplysninger som opplysninger om rasemessig eller etnisk bakgrunn; politisk, filosofisk eller religiøs oppfatning; at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling; helseforhold; seksuelle forhold eller medlemskap i fagforeninger.

- Dokumenter og andre opplysninger i forskningsprosjekter som faller inn under helseforskningsloven, skal behandles i tråd med Internkontrollsystem for helseforskning.
- Direkte identifiserbare og avidentifiserte forskningsdata skal overføres kryptert.

Eksamensoppgaver og eksamensbesvarelser

- Det aksepteres ikke brudd på konfidensialiteten og integriteten til eksamensoppgaver (tekster/forslag) og eksamensbesvarelser. Det samme gjelder uferdige eller innleverte studentoppgaver (bachelor/master) og avhandlinger (ph.d./dr. philos) som ikke skal publiseres eller offentliggjøres.
- Korte avbrudd i tilgjengelighetene aksepteres kun der det ikke vanskeliggjør gjennomføring av eksamen eller innlevering og sensurering av eksamensbesvarelser, studentoppgaver eller avhandlinger.

3 Roller, ansvar og oppgaver

Oversikt over de som har roller, ansvar og oppgaver i styringssystemet for informasjonssikkerhet ved UiT:

- universitetsstyret
- universitetsdirektør
- IT-direktør
- informasjonssikkerhetsrådgiver(e)
- Avdeling for IT
- Avdeling for bygg og eiendom
- enhetsledere (dekaner, avdelingsdirektører, museumsdirektør og biblioteksdirektør)
- systemeiere
- brukere
- Computer Security Incident Response Team (CSIRT)
- Informasjonssikkerhetsforum

I det følgende gis en nærmere beskrivelse av hvilket ansvar og hvilke oppgaver som er lagt til de ulike rollene.

Universitetsstyret

- behandler og vedtar styringssystemet for informasjonssikkerhet ved UiT
- kan stille krav til det videre arbeidet med informasjonssikkerhet ved UiT

Universitetsdirektør

- er behandlingsansvarlig for alle personopplysninger, dette omfatter også å bestemme formålet med behandling av personopplysninger, samt å ha dokumentert oversikt over disse
- har ansvar for informasjonssikkerhet på et overordnet nivå, herunder å sette av tilstrekkelige ressurser til arbeidet med informasjonssikkerhet, inkludert opplæring og kompetanseheving
- har ansvaret for at styringssystemet for informasjonssikkerhet blir implementert og vedlikeholdt, samt for organiseringen av sikkerhetsarbeidet
- skal iverksette årlig internrevisjon, jf. punkt 6.1.
- skal årlig gjennomgå status for arbeidet med informasjonssikkerhet[8]
- skal oppnevne medlemmer av informasjonssikkerhetsforumet

IT-direktør

- er informasjonssikkerhetsansvarlig og har forvaltningsansvaret for informasjonssikkerheten ved UiT
- har instruksjonsmyndighet overfor alle andre enheter ved UiT i saker som angår informasjonssikkerhet
- skal påse at holdningsskapende programmer gjennomføres

Informasjonssikkerhetsrådgiver(e)

- skal utøve IT-direktørens myndighet i saker om informasjonssikkerhet
- skal være rådgiver for linjeorganisasjonen i spørsmål relatert til informasjonssikkerhet
- skal lede CSIRT-teamet og Informasjonssikkerhetsforum
- skal utarbeide og vedlikeholde overordnet beredskapsplan for IKT
- skal følge opp avvik på overordnet nivå og sørge for at disse blir kanalisert til og fulgt opp av berørte enheter
- skal drive opplysningsvirksomhet, rådgivning og opplæring innen informasjonssikkerhet
- skal vedlikeholde overordnet policy og rutiner for informasjonssikkerhet
- skal iverksette og delta i revisjoner og risikovurderinger ved behov
- skal utarbeide årlig rapport til ledelsens gjennomgang
- skal holde oversikt over databehandleravtaler som inngås på UiT

[8] Jf. ledelsens gjennomgang

Avdeling for IT

- skal bistå systemeier ved utforming av krav til informasjonssikkerhet ved anskaffelse av nye system
- har ansvar for drift av IT-systemene, og skal ivareta tilfredsstillende informasjonssikkerhet på IT-infrastruktur basert på risikovurderinger
- skal, på bakgrunn av risiko- og sårbarhetsanalyser, utarbeide en kontinuitets- og beredskapsplan (KBP) som dekker kritiske og viktige informasjonssystemer og infrastruktur
- skal dokumentere systemer/infrastruktur med tilhørende sikkerhetstiltak
- skal utarbeide og vedlikeholde sikkerhetspolicy, retningslinjer og prosedyrer for den tekniske infrastrukturen
- skal overvåke vesentlige endringer i trusler mot UiTs informasjonsverdier

Avdeling for bygg og eiendom

- skal sørge for at sikring av tilgang til bygninger, rom og områder er i tråd med kriterier for akseptabel risiko
- skal bistå enheter ved risikovurderinger av fysisk sikkerhet og ved gjennomføring av nødvendige fysiske sikringstiltak

Enhetsledere

- er ansvarlig for å tilfredsstille krav til informasjonssikkerhet i egen enhet
- skal gjennomføre risikovurderinger
- skal iverksette tiltak dersom det er nødvendig for å ivareta informasjonssikkerheten i egen enhet
- skal rapportere resultat fra risikovurderinger med handlingsplan og avvik til informasjonssikkerhetsrådgiver
- skal følge opp avviksmeldinger i egen enhet og sørge for at disse blir lukket
- skal informere ansatte i egen enhet om de rutiner og retningslinjer som gjelder til enhver tid og sørge for at kravene i styringssystemet til egen enhet blir fulgt

Systemeier

- skal etablere og vedlikeholde rutiner for å ivareta sikkerhetsmålene
- skal stille krav til informasjonssikkerhet i anskaffelse, utvikling og vedlikehold av informasjon og informasjonssystemet, i samråd med Avdeling for IT
- skal sørge for at tilganger blir gitt etter tjenstlig behov, avsluttet når behovet opphører, samt at nødvendig opplæring blir gitt
- skal, i samråd med informasjonssikkerhetsrådgiver, sørge for at databehandleravtaler inngås
- skal utføre risikovurdering av systemet i henhold til punkt 4, og dokumentere at risikovurderinger er utført
- skal iverksette eventuelle tiltak på bakgrunn av risikovurderinger

Brukere av IT-tjenester (ansatte/studenter)

- har plikt til å gjøre seg kjent med og følge de sikkerhetsrutiner og retningslinjer som til enhver tid gjelder for sikker håndtering av informasjonsverdier og personopplysninger
- har plikt til å forhindre og rapportere hendelser som kan innebære avvik, samt rapportere avvik når disse oppstår, gjennom avviksmeldingssystemet

Computer Security Incident Response Team (CSIRT)

- skal iverksette, eller beordre iverksatt, ethvert tiltak som vurderes som tjenlig for å avverge skade på UiTs IT-systemer og data
- skal rapportere om sikkerhetshendelser, skadepotensial, skadeomfang og iverksatte tiltak til IT-direktøren

Informasjonssikkerhetsforum

- skal gi råd om tiltak/initiativ som fremmer informasjonssikkerheten
- skal koordinere planleggingen og gjennomføringen av tiltak og initiativ på informasjonssikkerhetsområdet som omfatter hele institusjonen
- skal gjennomgå rapporterte avvik og sikkerhetshendelser, og påse at disse blir lukket
- skal gjennomgå rapport til ledelsens gjennomgang
- skal bidra til implementering av styringssystemet i organisasjonen
- skal jevnlig gjennomgå styringssystemet for informasjonssikkerhet med tilhørende dokumenter og generelle ansvarsforhold, samt vurdere behov for endringer

4 Risikovurdering

Risikovurderinger skal avdekke mulige uønskede hendelser/trusler som kan føre til brudd på informasjonssikkerheten ved UiT. Vurderingene er derfor sentral i arbeidet med å sikre trygg og sikker behandling av UiTs informasjonsverdier. I tillegg til å avdekke hva som kan gå galt, skal de avdekke hva vi har gjort og hva vi ytterligere kan gjøre for å hindre at uønskede hendelser inntreffer, samt redusere konsekvensene dersom de likevel skjer.

Risikovurderingen må videre sees i sammenheng med etablerte akseptkriterier for risiko (jf. punkt 2.3), og akseptabel risiko må fastsettes før risikovurderingen foretas. Dersom risikoen for at en eller flere uønskede hendelser skjer er større enn det som er definert som akseptabelt, må denne risikoen håndteres ved at forebyggende tiltak iverksettes.

Risikovurderinger skal foretas

- når trusselbildet endres
- før oppstart av behandling av personopplysninger
- ved oppstart av forskningsprosjekter
- ved etablering eller endring av IKT-systemer
- ved organisatoriske endringer som kan påvirke informasjonssikkerheten

Alle risikovurderinger skal dokumenteres. Dersom risikovurderinger avdekker tilfeller som skal følges opp, skal det navngis hvem som har ansvar for å fastsette relevante tiltak og plan for oppfølgning av disse. Risikovurderingen skal leveres til informasjonssikkerhetsrådgiver(ne) som skal benytte disse i ledelsens gjennomgang og sørge for at dokumentene lagres i UiTs arkivsystem.

5 Opplæring

Opplæring skal bidra til å bygge en god sikkerhetskultur ved UiT. Den skal bevisstgjøre ansatte og studenter om betydningen av informasjonssikkerhet og gjøre dem i stand til å etterleve UiTs sikkerhetspolicy i sitt daglige virke. Opplæring i informasjonssikkerhet må derfor tas inn som en naturlig del av opplæringen av studenter og ansatte på alle nivå i organisasjonen. Systemeiere er spesielt ansvarlig for opplæring i sine respektive systemer.

Ledere har et overordnet ansvar for at nødvendig informasjon blir gitt til de ansatte, og at det blir satt av tid og ressurser til opplæring. For å sikre at dette ansvaret blir ivaretatt skal informasjonssikkerhet inngå i UiTs lederopplæring. Videre skal universitetsdirektøren sørge for at informasjonssikkerhet tas opp som tema i egnede lederfora minst en gang i året.

Informasjon om informasjonssikkerhet ved UiT skal være lett tilgjengelig for alle via universitetets nettsider og andre relevante kanaler.

Alle som er tildelt sentrale roller og oppgaver i sikkerhetsarbeidet skal gis spesiell opplæring. Eksterne kurs, seminarer og deltakelse i relevante nettverk er viktig for å sikre utveksling av informasjon og øke kompetansen hos denne gruppen ansatte.

6 Kontroll og oppfølging

6.1 Internrevisjon

Hensikten med internrevisjon er å kontrollere at det vedtatte styringssystemet for informasjonssikkerhet innføres, driftes og vedlikeholdes i alle deler av organisasjonen. Det skal gjennomføres årlig systematisk kontroll av universitetets behandling av informasjon der det er krav til konfidensialitet, integritet og tilgjengelighet. Kontrollen skal identifisere eventuelle avvik og behov for justeringer i selve styringssystemet og/eller i opplæringen. Det skal føres kontroll av de interne retningslinjene og hvorvidt disse er oppdatert i forhold til regler og praksis i virksomheten. Det skal også kontrolleres at de etterlever krav i lov og forskrifter. Den årlige kontrollen skal danne grunnlag for ledelsens gjennomgang.

6.2 Rapportering av avvik

Avvik er brudd på lover, forskrifter eller interne bestemmelser på UiT. Melding av avvik er viktig- både for å kartlegge årsaken til at de skjer, og for å eventuelt iverksette nye sikringstiltak for å unngå liknende avvik i fremtiden. Avvik handler således om kvalitet og forbedring.

Eksempler på avvik:

- Tyveri av datautstyr,
- misbruk av IT-tjenester,
- misbruk av passord,
- dataangrep for eksempel ved virusangrep eller hacking,
- datalekkasje,
- svakheter i IT-systemer eller rutiner på UiT,
- sensitiv informasjon på avveie,
- personopplysninger på avveie,
- uautorisert tilgang til opplysninger.

Fremgangsmåte ved avvik:

1. Den som oppdager et avvik skal rapportere dette via avviksmeldingssystemet.
2. Informasjonssikkerhetsrådgiver(ne) undersøker årsakene til avviket og iverksetter korrigerende tiltak for å lukke avviket.
3. Informasjonssikkerhetsrådgiver(ne) skal føre en samlet oversikt over alle avvik som er meldt inn. Disse skal blant annet inngå i ledelsens gjennomgang og benyttes for læring på tvers i organisasjonen for å hindre gjentakelse.

6.3 Ledelsens gjennomgang

Informasjonssikkerhet er et lederansvar på lik linje med andre sentrale lederoppgaver ved UiT. Det er ledelsen som har det øverste ansvaret for å sikre at UiT ivaretar pålagte krav til informasjonssikkerhet, og som skal passe på at medarbeidere og studenter har tilstrekkelig kjennskap til informasjonssikkerhet. For at ledelsen skal kunne ivareta sine oppgaver, skal det årlig utarbeides en rapport som gjennomgår arbeidet med informasjonssikkerhet.

Informasjonssikkerhetsrådgiver(ne) har ansvar for at denne rapporten blir utarbeidet.

Ledelsens gjennomgang skal omhandle

- resultater fra internrevisjonen
- resultater fra risikovurderinger
- rapporterte avvik og iverksatte tiltak
- eventuelle nødvendige justeringer av styringssystemet

Ledelsen skal etter gjennomgangen ta stilling til

- om ansvars- og oppgavefordelingen er hensiktsmessig
- om det er behov for endringer i styringssystemet
- om det er spesielle ressurs- og opplæringsbehov for kommende år

7 Vedlegg

7.1 Relevant regelverk

7.2 Prosedyrer, instrukser og rutiner

7.2.1 Reglement for brukere av IKT-ressurser ved UiT Norges arktiske universitet
7.2.2 Retningslinjer for behandling av studentopplysninger ved UiT Norges arktiske universitet
7.2.3 Retningslinjer for behandling av personopplysninger i forbindelse med personal og økonomiforvaltningen ved UiT
7.2.4 Retningslinjer for behandling av personopplysningar i forskings- og studentprosjekt ved UiT Norges arktiske universitet
7.2.5 Systemlandskap ved UiT
7.2.6 Klassifikasjon av informasjonsverdier ved UiT
7.2.7 Rutiner for helseforskning for Helsefak og UNN
7.2.8 Prosedyre for bestilling av leverandørkonto og fjerntilgang
7.2.9 Prosedyre for taushetsplikt og taushetserklæring
7.2.10 Prosedyre for fysisk sikring, tilgangskontroll og systemanskaffelser
7.2.11 Rutine for søknad om overføring av personopplysninger fra FS, Paga og System X til andre datasystemer

7.3 Mal for ROS- vurdering (risiko- og sårbarhetsvurdering)

7.4 Mal for databehandleravtale fra Datatilsynet

7.4.1 Mal for databehandleravtale etter helseregisterloven
7.4.2 Mal for databehandleravtale etter personopplysningsloven

7.5 Mal for leverandøravtale