Policy for informasjonssikkerhet ved

UNIVERSITETET I AGDER

Dato: 09.05.2011

Versjonskontroll

Versjon	Dato	Endringsbeskrivelse
0.7	2009-11-19	Initiell versjon
0.8	2009-11-26	Etter workshop 2009-11-24
0.81	2010-01-15	Gjennomgang av kap 3.7 ved IT-Avdelingen
0.82	2010-02-01	Arbeidsmøte i forkant av møte i styringsgruppen
0.83	2010-02-09	Arbeidsmøte i forkant av møte i styringsgruppen
0.84	2010-02-11	Arbeidsmøte i styringsgruppen
0.85	2010-02-26	Ferdigstilling av dokument til høringsrunde
1.0	2010-09-08	Dokument godkjent og ferdigstilt

Forfatter og distribusjon

Forfatter	Dato	Rolle
Kenneth Høstland		Ekstern konsulent
Øyvind Eilertsen	2009-11-26	UNINETT GigaCampus
Lars Nesland	2010-01-15	Fungerende prosjektleder UiA
Karen Mortensen	2010-02-01	Prosjektleder UiA
Ove Benestvedt	2010-02-09	Prosjektdeltager UiA
Tord Tjeldnes	2010-02-11	IT-direktør Tord Tjeldnes UiA
Karen Mortensen	2010-02-26	Prosjektleder UiA
Karen Mortensen	2010-09-08	Prosjektleder UiA

Distribusjonsliste	Rolle
	Rektor
	Universitetsdirektør
	Ass. universitetsdirektør
	Driftsdirektør
	Personal- og organisasjonsdirektør
	Økonomidirektør
	Forskningsdirektør
	Studiedirektør
	IT-direktør
	Formidlingsdirektør
	Sikkerhetsleder
	Sentral HMS-koordinator

Gjennomgang og godkjenning

Dato	Navn	Rolle	Initialer
2010-05-07	Administrativt ledermøte	Fellesadm. ledere	
2010-08-27	Fakultetsdirektørmøte	Fakultetsdirektører	
2010-09-01	Tor A. Aagedal	Universitetsdirektør	

Innholdsfortegnelse

1 Policy for informasjonssikkerhet

1.1 Sikkerhetsmål

Universitetet i Agder (UiA) er forpliktet til å ivareta konfidensialitet, integritet og tilgjengelighet for alle fysiske og elektroniske informasjonsverdier i institusjonen for å sikre at regulative, virksomhetsmessige og kontraktsmessige krav blir oppfylt.

De overordnede mål for informasjonssikkerheten i UiA er følgende:

- Sørge for samsvar med gjeldende lover, forskrifter og retningslinjer.
- Ivareta krav til konfidensialitet, integritet og tilgjengelighet for UiAs ansatte, studenter og andre brukere.
- Etablere kontroller for å beskytte UiAs informasjon og informasjonssystemer mot tyveri, misbruk og andre former for skade og tap.
- Motivere ledelse og ansatte til å opprettholde ansvar for, eierskap til, og kunnskap om informasjonssikkerheten, for å minimalisere risikoen for sikkerhetshendelser (avvik).
- Sikre at UiA er i stand til å fortsette sine tjenester også dersom større sikkerhetshendelser skulle inntreffe.
- Sørge for at personvernet ivaretas.
- Sikre tilgjengelighet og pålitelighet i nettverksinfrastruktur og tjenester levert og driftet av UiA.
- Følge metoder fra internasjonale standarder for informasjonssikkerhet.

1.2 Sikkerhetsstrategi

UiAs gjeldende strategiplan og rammeverk for risikostyring er førende for å identifisere, bedømme, evaluere og kontrollere informasjonsrelaterte risikoer.

Informasjonssikkerheten skal ivaretas av *Policy for informasjonssikkerhet*.
Virksomhetsmessig kontinuitet ivaretas gjennom:

- Kontinuitetsplaner
- Backup-prosedyrer
- Forsvar mot skadelig kode
- Forsvar mot ondsinnede aktiviteter
- Tilgangskontroll til systemer og informasjon
- Avvikshåndtering og rapportering.

Informasjonssikkerhet forstås som:

- ***Konfidensialitet:*** sikkerhet for at bare autoriserte personer har tilgang til informasjonen, og at den ikke avsløres til uvedkommende.
- ***Integritet:*** sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, samt et resultat av autoriserte og kontrollerte aktiviteter.
- ***Tilgjengelighet:*** sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig for autoriserte ved behov.

Følgende tabell gir eksempler på tiltak for å ivareta de enkelte elementene for Informasjonssikkerhet:

Konfidensialitet	Klassifisering: Sensitiv – Intern – Åpen (kap 3.3) Utøvelse: • Autentisering – identifisere bruker • Autorisering - tilgangskontroll • Revisjon/logging - sporing (AAA Authentication – Authorization – Accounting/Audit)
Integritet	Versjonshåndtering, saksbehandlingsrutiner
Tilgjengelighet	Klassifisering: Kritikalitet (Høy – Medium – Lav) (kap 3.10) Utøvelse: Redundans, Backup/restore

Et av de mest kritiske aspektene ved UiAs virksomhet er tilgjengelighet og pålitelighet for nett, infrastruktur og tjenester. UiA praktiserer åpenhet og meroffentlighet, men vil i gitte situasjoner prioritere hensynet til konfidensialitet foran hensynet til tilgjengelighet.

Alle brukere av UiAs informasjonssystemer er forpliktet til å følge *Policy for informasjonssikkerhet*. Overtredelse av policyen og vedtatte sikkerhetskrav vil være et tillitsbrudd mellom brukeren og UiA, og vil kunne medføre konsekvenser for ansettelses- eller avtaleforholdet.

……..
Universitetsdirektør Tor A Aagedal

2 Roller og ansvarsområder

2.1 Roller og ansvarsområder

Styret har det overordnete ansvaret for at UiAs verdier forvaltes på en effektiv og betryggende måte i henhold til gjeldende lover, forskrifter og avtaler.

Styret har delegert Universitetsdirektøren det daglige ansvar for informasjonssikkerheten ved UiA.

Eier av sikkerhetspolicy

2.1.1 Universitetsdirektøren er eier av *Policy for informasjonssikkerhet.* Universitetsdirektøren delegerer forvaltningen av *Policy for informasjonssikkerhet* til Sikkerhetsansvarlig (CSO, Chief Security Officer). Alle endringer i policyen skal dokumenteres, og signeres av Sikkerhetsansvarlig.

Sikkerhetsansvarlig

2.1.2 Sikkerhetsansvarlig er hovedansvarlig for informasjonssikkerheten ved UiA. *Assisterende universitetsdirektør* har denne rollen.

Systemeier

2.1.3 Systemeier, i samråd med IT-avdelingen, er ansvarlig for krav til anskaffelse, utvikling og vedlikehold av informasjon og relaterte informasjonssystemer. Alle systemer med tilhørende informasjon, skal ha en definert eier. Systemeieren skal definere hvilke brukere eller brukergrupper som skal ha tilgang til informasjonen og hva som er autorisert bruk av informasjonen. *Hvert informasjonssystem skal beskrives i et eget dokument. Systemeier er ansvarlig for at dokumentet foreligger.*

Systemadministrator

2.1.4 Systemadministratorer er personer som forvalter og administrerer UiAs informasjonssystemer og informasjon som er betrodd universitetet fra andre parter. Hver enkelt type informasjon og systemer kan ha en eller flere dedikerte Systemadministratorer. Disse er ansvarlige for å beskytte informasjonen, inklusive å implementere tilgangskontrollmekanismer for å sikre konfidensialitet, og å ha ansvar for at det tas backup, slik at kritisk informasjon ikke går tapt. Systemadministratorer implementerer, drifter og vedlikeholder dessuten sikkerhetsmekanismer i tråd med policyen. Det skal utarbeides en oversikt over Systemadministratorer for hvert enkelt system.

Superbrukere

2.1.5 Personer med høy kompetanse på et system. Kan ha utvidede rettigheter, men har ikke fulle administratorrettigheter. Kontaktperson for hjelp til bruk av systemet.

Brukere

2.1.6 Brukere er ansvarlige for å gjøre seg kjent med og rette seg etter UiAs IKT-reglement. Spørsmål om håndtering av forskjellig type informasjon skal stilles til Systemeieren for den aktuelle informasjonen, eventuelt til Systemadministrator.

Tredje part

2.1.7 Tredje part (f.eks. Kontraktspartnere og innleide konsulenter) som kan få tilgang til sensitiv informasjon skal skrive under taushetserklæring.

2.2 Sikkerhetsforum

Sikkerhetsansvarlig kan etablere et sikkerhetsforum etter behov, samt ta opp sikkerhetsrelaterte saker med riktig instans.

2.2.1 UiA kan etablere et informasjonssikkerhetsforum. Sikkerhetsforumet skal gi Universitetsdirektøren råd om tiltak som fremmer informasjonssikkerheten i organisasjonen, gjennom nødvendig engasjement og tilstrekkelig ressursbruk. Sikkerhetsforumet skal bl.a. ha følgende oppgaver:

- Gjennomgå og anbefale policy for informasjonssikkerhet med tilhørende dokumenter og generelle ansvarsforhold.
- Overvåke vesentlige endringer i truslene mot organisasjonens informasjonsaktiva.
- Gjennomgå og overvåke innrapporterte sikkerhetshendelser.
- Godkjenne større initiativ for å styrke informasjonssikkerheten.

3 Prinsipper for informasjonssikkerhet ved UiA

3.1 Risikostyring

UiA definerer risiko som kombinasjonen av sannsynligheten for en hendelse og konsekvensen av den.

Risikovurdering

3.1.1 UiA skal ha en tilnærming til sikkerhet som er basert på risikovurderinger.

3.1.2 UiA skal løpende analysere risikoer og vurdere behovet for beskyttelsestiltak. Tiltak skal vurderes med utgangspunkt i UiAs rolle som utdannings- og forskningsinstitusjon og med hensyn til effektivitet, kostnad, og praktisk gjennomførbarhet.

3.1.3 Det skal gjennomføres en årlig overordnet risikovurdering av informasjonssystemene.

3.1.4 Risikovurderingene skal identifisere, kvantifisere og prioritere risiko i forhold til relevante kriterier for akseptabel risiko.

3.1.5 Det skal gjennomføres risikovurderinger ved endringer som har betydning for informasjonssikkerheten. Det skal benyttes anerkjente metoder for risikovurdering.

3.1.6 Sikkerhetsansvarlig er ansvarlig for at risikostyringsprosessene ved UiA blir koordinert iht. *Policy for informasjonssikkerhet.*

3.1.7 Systemeier er ansvarlig for at risikovurderinger blir gjennomført.

Håndtering av risiko

3.1.8 Håndtering av risiko skal foretas i forhold til kriterier som UiAs ledelse har definert.

- IKT-100B Retningslinjer for risikovurdering personvern
- ROS-analyse

3.1.9 Risikovurderinger skal godkjennes av Sikkerhetsansvarlig.

3.1.10 Dersom en risikovurdering avdekker uakseptabel risiko, skal det settes i verk tiltak for å redusere risikoen til et akseptabelt nivå.

3.2 Implementering og endring

3.2.1 Universitetsdirektøren skal sørge for at *Policy for informasjonssikkerhet*, samt retningslinjer og standarder, blir benyttet og fulgt opp.

3.2.2 Universitetsdirektøren skal sørge for at det blir lagt til rette for at alle brukere får nødvendig opplæring og materiell, slik at brukerne kan beskytte UiAs informasjon og informasjonssystemer.

3.2.3 *Policy for informasjonssikkerhet* skal gjennomgås og oppdateres minimum en gang årlig eller ved behov.

3.3 Klassifisering og kontroll med informasjon og eiendeler

3.3.1 Informasjon og infrastruktur skal klassifiseres med hensyn til sikkerhetsnivå og tilgangsbegrensning.

3.3.2 Informasjonen skal klassifiseres i en av tre følgende kategorier for konfidensialitet:

Sensitiv
Informasjon av sensitiv art hvor uautorisert tilgang (også internt) kan medføre betydelig skade for enkeltpersoner, universitetet eller deres interesser. Sensitiv informasjon er her synonymt med sensitive personopplysninger som definert i personopplysningsloven, men kan også gjelde informasjon som kommer under forvaltningslovens «Unntatt Offentlighet» eller informasjon som UiA selv definerer som sensitiv. Slik informasjon skal sikres i «røde» soner, ref. kapittel 3.5.

Intern
Informasjon som kan skade UiA eller være upassende at tredjepart får kjennskap til. Systemeier avgjør hvem som skal ha tilgang og hvordan tilgangen skal implementeres.

Åpen
Annen informasjon er åpen.

3.3.3 UiA skal gjennomføre risikoanalyser for å kunne klassifisere informasjon ut fra hvor kritisk den er for virksomheten (*kritikalitet– kan utløse krav til tilgjengelighet*).

3.3.4 Det skal være utarbeidet rutiner for gjennomføring av informasjonsklassifisering og risikoanalyser.

3.3.5 Brukere som forvalter informasjon på UiAs vegne skal behandle denne i henhold til klassifiseringen.

3.3.6 Sensitive dokumenter skal være tydelig merket.

3.3.7 Klassifisering av utstyr i forhold til kritikalitet er behandlet i kapittel 3.10.

3.3.8 Det skal foreligge en plan for hvordan vesentlig dokumentasjon som er lagret elektronisk skal tas vare på over tid.

3.3.9 Informasjon som er vesentlig for virksomheten skal være uavhengig av hvilke systemer informasjonen er skapt eller behandlet i.

3.4 Informasjonssikkerhet knyttet til brukere av UiAs tjenester

Ved ansettelse

3.4.1 Sikkerhetsansvar og -roller for relevant personell, både ansatte og innleide, skal beskrives av nærmeste overordnede.

3.4.2 Det skal foretas sjekk av bakgrunnen til alle som innstilles til stillinger ved UiA iht. relevante lover og regler. Ansvarlig for dette er nærmeste overordnede.

3.4.3 Taushetserklæring skal signeres av arbeidstakere, oppdragstakere eller andre som kan få kjennskap til sensitiv og/eller intern informasjon.

3.4.4 IKT-reglementet skal aksepteres i alle ansettelsesforhold og ved systemtilganger for tredjepart.

For brukere gjelder

3.4.5 IKT-reglementet refererer til UiAs krav til informasjonssikkerhet og brukernes ansvar for å oppfylle disse.

3.4.6 IKT-reglementet skal gjennomgås jevnlig med alle brukere og ved alle nyansettelser.

3.4.7 Alle ansatte og tredjepartsbrukere skal få tilstrekkelig opplæring og oppdatering i *Policy for informasjonssikkerhet* og relevante retningslinjer og prosedyrer. Kravet til opplæring vil variere.

3.4.8 Brudd på policy for informasjonssikkerhet og tilhørende retningslinjer vil normalt medføre sanksjoner i henhold til IT-reglementet. For ansatte henvises også til tjenestemannsloven.

3.4.9 UiAs informasjon, informasjonssystemer og andre verdier (for eksempel telefon) skal kun benyttes til de formål de er bestemt for. Nødvendig privat bruk tillates.

3.4.10 Bruk av UiAs IKT-infrastruktur i egen næringsvirksomhet er ikke tillatt, med mindre det er særskilt godkjent av Universitetsdirektøren.

Avslutning eller endring av ansettelse

3.4.11 Ansvar for avslutting eller endring av ansettelsesforhold skal være klart definert i en egen rutine med relevant rundeskjema.

3.4.12 UiAs eiendeler skal leveres inn ved opphør av tjenestelig behov for bruk av eiendelene.

3.4.13 UiA skal endre eller stenge tilgangsrettigheter ved opphør av ansettelse eller endring av arbeidsforhold. Det skal finnes rutiner for å håndtere seniorforhold og alumni.

3.5 Informasjonssikkerhet knyttet til fysiske forhold

Sikkerhetsområder

3.5.1 For å sikre konfidensialitet skal sikre fysiske soner benyttes for å beskytte områder som inneholder IKT-utstyr og informasjon som krever beskyttelse. Sikre soner skal beskyttes med hensiktsmessige adgangskontroller for å sikre at kun autorisert personell får adgang.

Følgende soneinndeling skal benyttes:

Sikringsnivå	Område	Sikring
Grønn (Åpen)	Alle har i utgangspunktet tilgang. Studentområder og kantine.	Ingen adgangskontroll. Interne og sensitive opplysninger skal ikke skrives ut i denne sonen.
Gul (Intern)	Områder hvor det i arbeidstiden kan forefinnes intern informasjon. Kontorlokaler, møterom, noen arkiver, noen tekniske rom slik som koblingsrom, skriverrom.	Adgangskontroll utenom arbeidstid. Nøkkelkort/nøkkel. Adgangskontroll i arbeidstid avgjøres av Sikkerhetsansvarlig. Alle utskrifter skal beskyttes med «Follow me»-funksjonalitet.
Rød (Sensitiv)	Avgrensede områder som krever spesiell autorisasjon. Datarom, serverrom, arkiver o.l. med sensitiv informasjon.	Adgangskontroll: Nøkkelkort/nøkkel Alle utskrifter skal beskyttes med «Follow me»-funksjonalitet.

Sonene skal avmerkes i bygningsplansjer eller eksplisitt beskrives i eget dokument.

3.5.2 Sikkerhetsansvarlig er ansvarlig for godkjenning av fysisk tilgang i henhold til klassifisering/soneinndeling.

3.5.3 Alle UiAs lokaler skal sikres iht klassifisering med tilstrekkelige sikringssystemer, inkludert relevant sporbarhet/logging. Se tabell ovenfor.

3.5.4 Sikkerhetsansvarlig har ansvar for at arbeid utført av tredjepart i sikre soner er relevant overvåket og dokumentert.

3.5.5 Alle ansatte skal kunne tilkjennegi sin identitet og bære personlige adgangskort når de befinner seg i gule og røde soner. ID-kortene er personlige, og må ikke overdras til kolleger eller tredjepart.

3.5.6 Røde soner skal være forsvarlig sikret mot miljøskader forårsaket av brann, vann, vibrasjoner mv.

3.5.7 Alle skalldører og -vinduer skal stenges og låses ved arbeidsdagens slutt. Den siste som forlater et område er ansvarlig for sikring, inkludert å slå på alarm.

3.5.8 Adgangskort kan gis til håndverkere, teknikere og andre mot at det fremvises ID-kort.

3.5.9 Besøkende i rød sone skal registreres inn og ut, og de skal bære synlige gjestekort eller personlige adgangskort.

3.5.10 Besøk i rød sone skal ledsages eller overvåkes, f.eks. med kamera.

Sikring av utstyr

3.5.11 For å sikre tilgjengelighet/oppetid skal IKT-utstyr klassifisert som «høy» (se kapittel 3.10.5) plasseres eller beskyttes slik at det reduserer risikoen for miljømessige trusler (brann, oversvømmelse, temperatursvingninger, mv.) i henhold til klassifisering. Utstyr skal klassifiseres med basis i ROS-vurderinger.

3.5.12 Informasjon klassifisert som «sensitiv» som er lagret på bærbart datautstyr skal passordbeskyttes og krypteres.

3.5.13 Bærbart datautstyr skal håndteres som håndbagasje under reiser.

3.6 Driftsadministrasjon av IKT

Prosedyrer og ansvarsområder

3.6.1 Installasjon av IKT-utstyr skal godkjennes av IT-avdelingen før installasjon.

3.6.2 Installasjon av programvare på IKT-utstyr skal så langt det er mulig godkjennes av IT-avdelingen før installasjon.

3.6.3 IT-avdelingen skal sikre dokumentasjon av IKT-systemer etter UiA sin standard.

3.6.4 Endringer i IKT-systemer skal bare gjennomføres dersom det er virksomhetsmessig og sikkerhetsmessig velbegrunnet. Endringer godkjennes iht ITIL i Change Advisory Board (CAB).

3.6.5 IT-avdelingen skal sørge for at det foreligger en nødprosedyre for å minimalisere effekten av feilslåtte endringer i IKT-systemer.

3.6.6 Driftsoppgaver skal være skriftlig dokumentert i egne prosedyrer. Dokumentasjon av driftsprosedyrer skal oppdateres etter alle vesentlige endringer.

3.6.7 Oppgaver og ansvar skal separeres på en slik måte at det reduserer muligheten for uautorisert eller uforutsett misbruk av UiAs eiendeler/systemer.

3.6.8 Utvikling, test og vedlikehold skal separeres for å redusere risikoen for uautorisert tilgang eller uautoriserte endringer og feilsituasjoner.

Eksterne leverandører

3.6.9 For alle avtaler som angår utkontrakterte IKT-systemer skal det foreligge en SLA-avtale (Service Level Agreement) med den eksterne leverandøren. Avtalen skal inneholde:

- beskrivelse av avtalt sikkerhetsnivå
- krav til informasjonssikkerhet, herunder konfidensialitet, integritet og tilgjengelighet
- krav til fortløpende rapportering av avvik fra leverandør
- beskrivelse av hvordan UiA kan etterprøve at leverandørene oppfyller avtalene
- beskrivelse av UiAs rett til revisjon
- beskrivelse av økonomiske konsekvenser ved brudd på avtale
- dersom systemet inneholder sensitiv informasjon må der også foreligge garanti for at informasjon er beskyttet i henhold til norsk lov

Systemplanlegging og aksept/godkjenning (nye systemer)

3.6.10 Det skal tas hensyn til informasjonssikkerhetskrav ved design, testing, implementasjon og oppgradering av nye IKT-systemer, samt ved systemendringer. Det skal utarbeides rutiner for endringshåndtering og systemutvikling/vedlikehold.

3.6.11 IKT-systemene skal dimensjoneres i henhold til kapasitetskrav. Belastningen skal overvåkes slik at oppgradering og tilpasning kan gjøres fortløpende. Dette gjelder særlig for virksomhetskritiske systemer.

Beskyttelse mot skadelig kode

3.6.12 Datautstyr skal sikres mot virus og annen ondsinnet og/eller skadelig programvare. It-avdelingen forvalter denne sikringen.

Sikkerhetskopiering

3.6.13 IT-avdelingen er ansvarlig for regelmessig sikkerhetskopiering og testing av denne, samt oppbevaring av data på UiAs IKT-systemer iht. klassifisering.

3.6.14 Sikkerhetskopier skal oppbevares eksternt eller i egen relevant sikret sone.

Nettverksstyring

3.6.15 IT-avdelingen har ansvaret for å beskytte UiAs interne nettverk på vegne av Sikkerhetsansvarlig.

3.6.16 Det skal være kontroll på utstyr som er koblet opp i UiAs kablede datanettverk. Sentrale komponenter skal føres i en inventarkontroll før de settes i nettverket.

3.6.17 Det skal føres oversikt over tilgang og bruk av UiA sitt nett ihht klassifisering.

Håndtering av lagringsmedier

3.6.18 Håndtering av flyttbare lagringsmedier, slik som taper, minnepinner, disketter og utskrifter, skal sikres iht. klassifikasjon. Den enkelte ansatte er ansvarlig for at dette blir gjennomført.

3.6.19 Lagringsmedier i alt utstyr som avhendes skal destrueres på en forsvarlig måte.

Utveksling av informasjon

3.6.20 Det skal etableres prosedyrer og kontroller for å beskytte utveksling av informasjon med tredjepart. Det skal stilles krav til at eksterne leverandører skal følge disse prosedyrene.

3.6.21 UiA har, på visse vilkår, rett til innsyn i ansattes og studenters personlige e-post og område i UiAs datanettverk, jfr. personopplysningsforskriftens kapittel 9. Ved eventuelt innsyn skal studenter og ansatte varsles i henhold til forskriftens § 9-3.

Bruk av kryptering

3.6.22 Lagring og overføring av sensitiv informasjon (se klassemodellen i kapittel 3.3) skal krypteres eller beskyttes på annen måte.

Elektronisk utveksling av informasjon

3.6.23 Informasjon som utveksles over offentlige nettverk i forbindelse med elektronisk handel skal beskyttes mot svindel, kontraktsmessige uoverensstemmelser, uautorisert tilgang og endringer.

3.6.24 IT-avdelingen skal sørge for at offentlig tilgjengelig informasjon, f.eks. på UiAs webtjenester, er tilstrekkelig beskyttet mot uautorisert tilgang.

Overvåkning av systemtilgang og bruk

3.6.25 Tilgang og bruk av IKT-systemer skal logges og overvåkes for å kunne identifisere misbruk.

3.6.26 Bruk og endringer skal være sporbare til en spesifikk entitet, f.eks. person eller enkeltsystem.

3.6.27 IT-avdelingen (med samarbeidspartner(e)) skal registrere vesentlige forstyrrelser og uregelmessigheter i driften av systemene, samt mulige årsaker til feil. Alvorlige feil rapporteres til sikkerhetsansvarlig.

3.6.28 Kapasitet, oppetid og kvalitet på IKT-systemer og datanettverk skal overvåkes i tilstrekkelig grad for pålitelig drift og tilgjengelighet.

3.6.29 IT-avdelingen (med samarbeidspartner(e)) skal logge sikkerhetshendelser i alle vesentlige systemer i henhold til klassifisering.

3.6.30 IT-avdelingen (med samarbeidspartner(e)) skal sikre at systemklokkene jevnlig synkroniseres til korrekt tid.

3.6.31 For informasjonssystemer som behandler personopplysninger, skal all autorisert bruk og forsøk på uautorisert bruk logges. Loggene skal lagres i minst 3 måneder.

3.7 Tilgangskontroll

Virksomhetsmessige krav

3.7.1 Det skal finnes en skriftlig tilgangs- og passordpolicy som er basert på virksomhets- og sikkerhetsmessige krav og behov. Tilgangspolicyen skal revideres regelmessig.

3.7.2 Tilgangspolicyen skal inneholde retningslinjer for passord (endringsfrekvens, minimumslengde, type karakterer som kan/skal benyttes mv.) og hvordan passordet kan lagres.

Brukeradministrasjon og -ansvar

3.7.3 System og systemtilgang skal minimum autentiseres ved hjelp av personlige brukeridentiteter og passord.

3.7.4 Brukerne skal ha unike kombinasjoner av brukeridentiteter og passord.

3.7.5 Brukerne er ansvarlige for enhver bruk av brukeridentiteter og passord. Brukerne skal holde passord konfidensielle, og skal ikke røpe disse uten at det er spesifikt autorisert av Sikkerhetsansvarlig.

Tilgangskontroll/Autorisasjon

3.7.6 Tilgang til informasjonssystemer skal være autorisert av nærmeste leder iht. systemeiers direktiver. Dette skal inkludere tilgangsrettigheter, inkludert tilhørende privilegier, som lagres i «aksesslister». Autorisasjoner skal bare gis etter «need to know»-prinsippet, og reguleres av type rolle/stilling.

3.7.7 Nærmeste leder skal melde fra til Systemadministrator om oppretting og endringer i tilgang iht. Systemeiers direktiver.

Kontroll med nettverkstilgang

3.7.8 IT-avdelingen har ansvaret for at brukernes nettverkstilgang er i overensstemmelse med retningslinjene for tilgang.

3.7.9 Brukere skal bare ha tilgang til de tjenester de er autorisert for.

Mobilt utstyr og fjernarbeidsplasser

3.7.10 For å aksessere UiAs datanettverk og informasjon fra ekstern lokasjon må man ha lest og signert UiAs IKT-reglement.

3.7.11 Mobile enheter skal sikres med tilstrekkelige sikkerhetsmekanismer.

3.7.12 Fjerntilgang til UiAs nettverk skal kun skje gjennom sikkerhetsløsninger som er godkjent av IT-avdelingen.

3.7.13 Sensitiv informasjon skal krypteres dersom den blir oppbevart på bærbare medier, slik som minnepinner, PDA-er, DVD-er og mobiltelefoner.

3.7.14 Tilgangen til privilegerte kontoer og sensitive områder skal begrenses.

3.8 Systemutvikling og vedlikehold

Sikkerhetskrav til informasjonssystemer

3.8.1 Definisjoner av virksomhetsmessige krav til nye systemer eller videreutvikling av systemer skal inneholde sikkerhetsmessige krav.

Korrekt virkemåte i informasjonssystemer

3.8.2 Data inn og ut av felles informasjonssystemer skal valideres for å sikre korrekthet og relevans.

Kryptografiske kontroller

3.8.3 Det skal foreligge retningslinjer for administrasjon og bruk av kryptering for beskyttelse av informasjon.

Sikkerhet i systemfiler

3.8.4 Implementering av endringer i produksjonsmiljø skal kontrolleres gjennom bruk av formelle prosedyrer for endringskontroll, for å minimalisere sannsynligheten for skade på informasjon eller informasjonssystemer.

Sikkerhet i utvikling og vedlikehold

3.8.5 De systemer som utvikles for eller av UiA skal ha klare krav til sikkerhet, inkludert validering av data, sikring av koden før produksjonssetting, og eventuell bruk av kryptering.

3.8.6 All programvare skal gjennomtestes og aksepteres formelt av systemeier og IT-avdelingen før programvaren overføres til produksjonsmiljøet.

Risikovurdering

3.8.7 Før større endringer i systemer med risikoklassifisering «høy» settes i produksjon, skal det gjennomføres en risiko- og sårbarhetsvurdering (ROS).

3.9 Håndtering av sikkerhetshendelser og avvik

Ansvar for rapportering

3.9.1 Alle sikkerhetsbrudd, samt bruk av informasjonssystemer i strid med fastlagte rutiner, skal behandles som avvik.

3.9.2 Alle ansatte er ansvarlig for å rapportere brudd og mulige brudd på sikkerheten. Rapporteringen skal gå tjenestevei eller direkte til Sikkerhetsansvarlig.

Bevissikring

3.9.3 It-avdelingen skal være kjent med enkle rutiner for bevissikring ved mistanke om IKT-sikkerhetshendelser.

3.10 Kontinuitetsplanlegging

For å sikre at systemer er tilgjengelige og operative.

Kontinuitetsplan

3.10.1 Det skal utarbeides en kontinuitets- og beredskapsplan (KBP) som dekker kritiske og viktige informasjonssystemer og infrastruktur.

3.10.2 Kontinuitetsplanen(e) skal utarbeides på bakgrunn av risiko- og sårbarhetsanalyser som tar utgangspunkt i virksomhetsrisiko.

3.10.3 Kontinuitetsplanen(e) skal avstemmes med UiAs øvrige beredskap og planverk.

3.10.4 Kontinuitetsplanen(e) skal testes periodisk for å sikre at de(n) er dekkende, og sikre at ledelse og ansatte forstår gjennomføringen.

3.10.5 Produksjonssystemer og andre systemer klassifisert som «høy» skal ha reserveløsninger. Tabellen under skal fylles ut etter at ROS-vurdering og/eller Business Impact Analysis (BIA) er gjennomført.

Kritikalitet	Maksimal nedetid	Beskrivelse
3 - Høy	< 4 timer	Systemet kan være utilgjengelig opp til 4 timer
2 - Medium	24 timer	Systemet kan være utilgjengelig opp til ett døgn
1 - Lav	3 dager	Systemet kan være utilgjengelig opp til 3 dager

3.11 Samsvar

Samsvar med juridiske krav

3.11.1 UiA skal følge gjeldende lovverk, samt andre eksterne retningslinjer, slik som (ikke avgrenset til):

- Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven)
- Forskrift i forhold til om systematisk helse-, miljø-, og sikkerhetsarbeid i virksomheter (internkontrollforskriften)
- Lov om behandling av personopplysninger (personopplysningsloven)
- Lov om statens tjenestemenn m.m. (tjenestemannsloven)
- Lov om årsregnskap mv. (regnskapsloven)
- Lov om universiteter og høyskoler (universitetsloven)
- Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)
- Lov om elektronisk signatur (esignaturloven)
- Lov om arkiv (arkivlova) m/forskrifter
- Forskrift om brannforebyggende tiltak og tilsyn

Andre eksterne referanser

- Hovedtariffavtalen i Staten
- Statens Personalhåndbok
- Datatilsynets krav
- Datatilsynets «Veileder i informasjonssikkerhet for kommuner og fylker».

Samsvar med sikkerhetspolicy

3.11.2 Alle ansatte skal forholde seg i overensstemmelse med *Policy for informasjonssikkerhet* og retningslinjer. Oppfølging av dette er linjeledelsens ansvar. Studenter skal forholde seg til IKT-reglementet.

3.11.3 Ansatte og studenter skal være klare over at bevis fra sikkerhetshendelser kan bli tatt vare på (lagret) og overleveres etter rettslig krav.

Kontroll og revisjon

3.11.4 Gjennomføring av revisjoner skal planlegges og avtales med de involverte for å minimalisere risikoen for at UiAs aktiviteter blir forstyrret.

4 Styrende dokumenter for sikkerhetsarbeidet

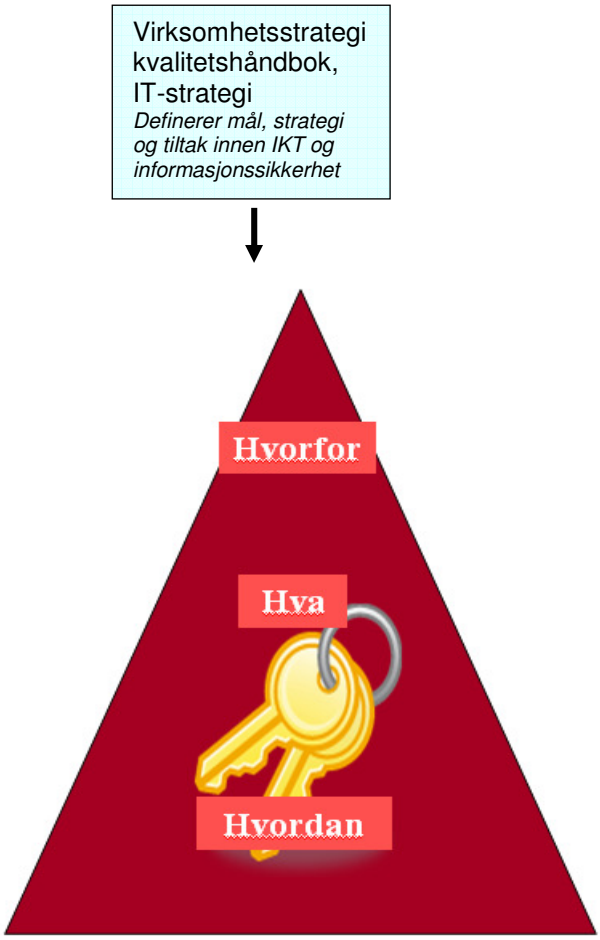
4.1 Formålet med styrende dokumenter

Styrende dokumenter for informasjonssikkerhet skal bidra til å oppnå et balansert nivå på tiltakene i forhold til den risiko og de rammebetingelser UiA står overfor.

Det skal eksistere dokumenterte krav og retningslinjer for informasjonssikkerhet basert på oppdaterte risikoanalyser. Systemer og infrastruktur skal være dekket av gode basiskontroller innen informasjonssikkerhet som til enhver tid skal etterleves.

4.2 Dokumentstruktur

4.2.1 UiA har organisert dokumentstrukturen for beskrivelse av sin sikkerhetsarkitektur i 3 nivåer. Strukturen for styrende dokumenter for informasjonssikkerhetsarbeidet er som følger:



Nivå 1: Sikkerhetspolicy
definerer mål, hensikt, ansvar og overordnede krav. I tillegg gir denne en oversikt over de etablerte styrende dokumenter knyttet til informasjonssikkerhet og *hvorfor* dette er viktig. Dette er *styrende* dokumentasjon.

Nivå 2: Overordnede retningslinjer og prinsipper
for informasjonssikkerhet. Her defineres *hva* som må gjøres for å etterleve den etablerte policy.
Dette er *styrende* dokumentasjon.

Nivå 3: Standarder og prosedyrer
for informasjonssikkerhet. Inneholder detaljerte retningslinjer for *hvordan* disse retningslinjer og prinsipper (nivå 2) skal implementeres. Dette bør etter hvert etableres for alle sentrale informasjons-systemer. Dette er *gjennomførende* og *kontrollerende* dokumentasjon.

5 Definisjoner

ROS-vurdering: *Risiko- og sårbarhetsvurdering*. En analyse av konsekvenser ved feil (risiko) og sannsynlighet for feil (sårbarhet). Systemeier har ansvar for at det foreligger en ROS-vurdering for det aktuelle systemet.

Kontinuitets- og beredskapsplan: Plan med konkrete tiltak for å sikre tilgjengelighet til det aktuelle informasjonssystemet.

BIA: *Business Impact Analysis* – Analyse av hvor stor konsekvens en feil vil kunne gi.

Fra personopplysningsloven § 2:

Personopplysning
Opplysninger og vurderinger som kan knyttes til en enkeltperson

Sensitive personopplysninger
Opplysninger om

a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,
b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
c) helseforhold,
d) seksuelle forhold,
e) medlemskap i fagforeninger.

Fra norsk utgave av ISO/IEC 27002 (NS-ISO 17799:2001):

Hva er informasjonssikkerhet?
Informasjon er et aktivum som, i likhet med andre viktige virksomhetsaktiva, har verdi for en organisasjon og derfor må vernes på forsvarlig måte. Informasjonssikkerhet beskytter informasjon mot en lang rekke trusler med det formål å sikre driftskontinuitet, redusere skader og maksimere utbyttet av investeringer og forretningsmuligheter.

Informasjon kan eksistere i mange former. Den kan trykkes eller skrives på papir, lagres elektronisk, overføres via post eller elektroniske media, vises på film eller formidles muntlig. Uansett hvilken form informasjonen har eller hvilket middel den formidles gjennom og lagres på, bør den alltid beskyttes på forsvarlig måte.

Informasjonssikkerhet omfatter her beskyttelse av:
a) konfidensialitet: at informasjon bare er tilgjengelig for dem som har autorisert tilgang til den;
b) integritet: nøyaktig og fullstendig informasjon og behandlingsprosesser;
c) tilgjengelighet: at autoriserte brukere har tilgang til informasjon og tilhørende tjenester når de trenger dem;
Informasjonssikkerhet oppnås ved å iverksette passende kontrolltiltak, som kan være politikk, rutiner, prosedyrer, organisasjonsstrukturer og programvarefunksjoner. Disse tiltakene må etableres for å sikre at organisasjonens spesielle sikkerhetsmål oppfylles.

6 Referanser

6.1 Interne referanser

Versjon	Dato	Kommentar	Ansvarlig
		IKT-reglement for UiA	
		Strategiplan for UiA	
		Kvalitetssikringssystem for UiA	
		IKT-strategi for UiA	
		Risikovurderinger	
		Personalreglement	
		Personalpolicy	
		Retningslinjer for avhending av IKT-utstyr	
		Taushetserklæring	
		Funksjonsbeskrivelse CSO	
		Andre relevante IKT-relaterte dokumenter	

6.2 Eksterne referanser

[1] *ISO/IEC 27001: 2005 Information security – Security techniques – Information security management systems – Requirements*

[2] *ISO/IEC 27002: 2005 Information security – Security techniques – Code of practice for information security management.*

[3] *ISO/IEC 27005: 2008 Information security – Security techniques – Information security risk management.*

[4] *Lov om personopplysninger: http://www.lovdata.no/all/hl-20000414-031.html*

[5] *Lov om arkiv (arkivlova): http://www.lovdata.no/all/nl-19921204-126.html*

[6] *Lov om årsregnskap m.v. (regnskapsloven): http://www.lovdata.no/all/nl-19980717-056.html*

[7] *Lov om statens tjenestemenn m.m. (tjenestemannsloven): http://www.lovdata.no/all/nl-19830304-003.html*

[8] *Lov om universiteter og høyskoler (universitetsloven): http://www.lovdata.no/all/hl-20050401-015.html*

[9] *Lov om elektronisk signatur (esignaturloven): http://www.lovdata.no/all/hl-20010615-081.html*

[10] *Lov om opphavsrett til åndsverk m.v. (åndsverkloven): http://www.lovdata.no/all/nl-19610512-002.html*

[11] *"Kommuneveiledningen" (Veiledning i informasjonssikkerhet for kommuner og fylker"): http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/tv202_2005_1.pdf*

[12] *Datatilsynet: Veileder for bruk av tynne klienter: http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/Veileder_tynneklienter.pdf*

[13] Datatilsynet*: Kryptering: http://www.datatilsynet.no/templates/article____889.aspx*

[14] Datatilsynet*: Risikovurdering: http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/Risikovurdering_TV-506_02.pdf http://www.sfso.no/upload/forvaltning_og_analyse/risikostyring/NY_Metodedokument_06012006.pdf*

[15] *OECDs retningslinjer - for sikkerhet i informasjonssystemer og nettverk - Mot en sikkerhetskultur. http://www.oecd.org/dataoecd/16/5/15584616.pdf*

[16] Nasjonal Sikkerhetsmyndighet (NSM)*: Veiledning i risiko- og sårbarhetsanalyse (ROS). http://www.nsm.stat.no/Documents/Veiledninger/ROS_2004_veiledning.pdf*

[17] Senter for statlig økonomistyring*: Risikostyring i staten – Håndtering av risiko i mål- og resultatstyringen http://www.sfso.no/upload/forvaltning_og_analyse/risikostyring/NY_Metodedokument_06012006.pdf*

[18] *UFS 107: Krav til strømforsyning av IKT-rom. Fagspesifikasjon fra UNINETT. https://ow.feide.no/_media/gigacampus:ufs103.pdf*

[19] *UFS 108: Krav til ventilasjon og kjøling i IKT-rom. Fagspesifikasjon fra UNINETT. https://ow.feide.no/_media/gigacampus:ufs108.pdf*

[20] *UFS 122: Anbefalt IKT-infrastruktur i UH-sektoren. Fagspesifikasjon fra UNINETT. https://ow.feide.no/_media/gigacampus:ufs:ufs_122_v1.0.pdf*