

Styringssystem for sikkerhet ved UiA

Type dokument	Styringsdokument	
Godkjennes av	Universitetsdirektør Seunn Smith-Tønnessen	21.11.2024
Klassifisering	Åpent	
Gyldighet	Dato for godkjenning, årlig revisjon	13.12.2024
Unntatt offentligheten	Nei	

Innhold

1	Styringssystem for sikkerhet – styrende del	3
1.1	Innledning og hensikt	3
1.2	Formål	3
1.3	Struktur	3
1.4	Virkeområde	3
2	Krav og referanser	3
2.1	Lovkrav	3
2.2	Eksterne krav	4
2.3	Interne krav	4
3	Definisjoner og forkortelser	5
4	Hovedprinsipper for det forebyggende sikkerhetsarbeidet	6
4.1	Innledning	6
4.2	Sikkerhetsmål	6
4.3	Konfidensialitet	6
4.4	Integritet	6
4.5	Tilgjengelighet	6
5	Sikkerhetsorganisasjon, roller, ansvar og myndighet	7
6	Beredskap	9
6.1	Taktisk nivå	9
6.2	Operativt nivå	9
6.3	Strategisk nivå	9
7	Beredskapstelefonen	9
8	Avvikshåndtering	10
9	Rapportering	10
10	Styringssystem for sikkerhet - gjennomførende del	10
10.1	Sikkerhetsområder	10
10.1.1	Krisehåndtering	10

10.1.2	Verdioversikt.....	11
10.1.3	Fysisk sikkerhet	11
10.1.4	Brannvern	Error! Bookmark not defined.
10.1.5	Informasjonssikkerhet og personvern	11
10.1.6	Personellsikkerhet	11
10.1.7	Risikostyring	12
10.1.8	Eksportkontroll	12
10.1.9	Anskaffelser	12
11	Styringssystem for sikkerhet - kontrollerende del	12
11.1	Evaluering prestasjon	13
11.1.1	Overvåking	13
11.1.2	Internrevisjon	13
11.1.3	Ledelsens gjennomgang	13
11.2	Forbedring	13
11.3	Dokumentasjon.....	13
11.3.1	Opplæring og bevisstgjøring	14

1 Styringssystem for sikkerhet – styrende del

1.1 Innledning og hensikt

Universitetet i Agder (UiA) er underlagt sikkerhetsloven. Dette dokumentet er UiAs styringssystem for sikkerhet. Styringssystemet skal oppfylle krav gitt i eller med hjemmel i sikkerhetsloven. Styringssystemet omfatter alle aktiviteter med betydning for forebyggende sikkerhetsarbeid.

Styringssystemet skal være en helhetlig oversikt over alle sikkerhetsområder og skal samordnes med ledelsessystem for informasjonssikkerhet, beredskapsplanverk og virksomhetsstyring for øvrig. Det skal sikre en helhetlig sikkerhetsstyring og vise hvordan UiA organiserer sine sikkerhetsressurser.

Styringssystemet skal gjennomgå årlig, og revideres ved behov. Det er universitetsdirektøren som godkjenner styringssystemet.

1.2 Formål

Formålet med styringssystem for sikkerhet er å sørge for at UiAs sikkerhetsoppgaver utføres i henhold til interne og eksterne krav samt lovkrav. Styringssystem for sikkerhet beskriver de forskjellige sikkerhetsområdene og samvirke mellom disse. Styringssystem for sikkerhet skal sørge for et helhetlig sikkerhetsarbeid på tvers av avdelinger og fakultet.

1.3 Struktur

Styringssystem for sikkerhet består av tre deler:

1. Styrende del
2. Gjennomførende del
3. Kontrollerende del

Den styrende delen beskriver virkeområdet for styringssystemet, sikkerhetsmål, sikkerhetsstrategi og ansvarsfordeling innen alt sikkerhetsarbeid ved UiA.

Gjennomførende del, sammen med vedlegg, gir utfyllende opplysninger om oppgaver og aktiviteter som skal gjennomføres i henhold til beskrivelsene i styringssystemet.

Kontrollerende del, sammen med vedlegg, beskriver kontrollerende aktiviteter som skal gjennomføres.

1.4 Virkeområde

Styringssystem for sikkerhet gjelder for hele UiA sin virksomhet og kan i tillegg komme til anvendelse ved bruk av eksterne parter der det er aktuelt. Der det er overlappende fagområder innen sikkerhet skal styringssystemet beskrive rutiner for håndtering av dette. HMS er regulert under egne internkontrollrutiner og er derfor ikke en del av styringssystemet.

2 Krav og referanser

2.1 Lovkrav

Sikkerhetsarbeidet ved UiA er underlagt en rekke krav gitt i hjemmel og lov – med tilhørende forskrifter.

Kravinstans	Hjemmel og krav
Justis- og beredskaps- departementet	Lov om nasjonal sikkerhet (sikkerhetsloven) Forskrift om virksomheters arbeid med forebyggende sikkerhet Lov om behandling av personopplysninger (personopplysningsloven) Beskyttelsesinstruksen Personvernforordning Forvaltningsloven Offentlighetsloven
Kunnskaps- departementet	UH-loven
Utenriksdepartementet	Lov om kontroll med eksport av strategiske varer, tjenester og teknologi mv. (eksportkontrollloven)
Arbeids- og Inkluderings- departementet	Forskrift om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (internkontrollforskriften)
Nærings og fiskeridepartementet	Lov om anskaffelser offentlige
Kultur og likestillingsdepartementet	Arkivlova

2.2 Eksterne krav

Kravinstans	Hjemmel og krav
Kunnskapsdepartementet	Styringsdokument for arbeidet med sikkerhet og beredskap i kunnskapsdepartementets sektor Tildelingsbrev for Universitetet i Agder Virksomhets- og økonomiinstruks for statlige universiteter og høyskoler Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning
Direktoratet for Høyere utdanning og kompetanse	Tilstandsrapport om arbeidet med sikkerhet og beredskap Tilstandsrapport om arbeidet med informasjonssikkerhet

2.3 Interne krav

Dokumentnr. / Arkivreferanse	Dokumentnavn/Krav
18/02891-1	Ledelsessystem for informasjonssikkerhet
	Et helhetlig rammeverk for dokumentasjon av internkontroll
	Retningslinje for internkontroll

3 Definisjoner og forkortelser

CSO/SL	Chief Security Officer/ Sikkerhetsleder
IRT	Incident Response Team. Operativ håndtering i IKT - sikkerhetshendelser
CISO	Chief Information Security Officer
KD	Kunnskapsdepartementet
FOI	Forskning og Innovasjonsavdeling
GNF	Grunnleggende nasjonal funksjon som ved helt eller delvis bortfall vil få konsekvenser for statens evne til å nasjonale sikkerhetsinteresser. KD har utpekt forskning og utvikling som GNF.
Skjermingsverdige Verdier	Informasjon, informasjonssystemer, infrastruktur eller objekt som må sikres. Manglende sikring og/eller avvik på disse kan utgjøre en trussel for nasjonale sikkerhetsinteresser eller grunnleggende nasjonale funksjoner (GNF)
Sikkerhetsklarering	Besluttet av sivil klareringsmyndighet på grunnlag av sikkerhetsmessig skikkethet for tilgang til sikkerhetsgradert informasjon.
Autorisasjon	Godkjenning fra virksomheten (UiA) for tilgang til sikkerhetsgradert informasjon, adgang til skjermingsverdige objekter og/eller infrastruktur.
Sikkerhetsgradert informasjon	Informasjon som i henhold til sikkerhetsloven er gitt et særskilt vern. Sikkerhetsgradert informasjon inndeles i fire kategorier: BEGRENSET, KONFIDENSIELT, HEMMELIG OG STRENGT HEMMELIG.
Forsvarlig sikkerhetsnivå	Grunnlaget for sikringsnivå av verdier. Forsvarlig sikkerhetsnivå må sees i sammenheng med krav gitt i sikkerhetsloven.
Sikkerhetstruende hendelser	Tilsiktede handlinger som direkte eller indirekte truer eller kan true nasjonale og/eller UiAs skjermingsverdige verdier.
Verdioversikt	Oversikt over universitetets immaterielle og fysiske verdier

4 Hovedprinsipper for det forebyggende sikkerhetsarbeidet

4.1 Innledning

Forebyggende sikkerhetsarbeid ved UiA skal være kunnskaps og risikobasert. Dette innebærer bruk av anerkjente standarder. Nasjonale og lokale risikovurderinger danner sammen med interne sikkerhetsvurderinger utgangspunktet for UiAs egne risikovurderinger og tilhørende risikoreduserende tiltak.

Alle som utarbeider, mottar, eller på annen måte behandler informasjon er pliktige til selv å vurdere om informasjonen er skjermingsverdig. I de tilfellene UiA behandler verdier vurdert som skjermingsverdige i henhold til sikkerhetsloven, skal disse beskyttes med nødvendige og forsvarlige sikringstiltak. Sikringstiltak skal besluttes etter gjennomført risikovurdering.

UiA gjennomfører årlig helhetlig sikkerhetsvurdering hvor alle sikkerhetsområder er representert. Enheter og fagmiljø som er berørte av krav i sikkerhetsloven skal i tillegg gjennomføre risikovurderinger.

4.2 Sikkerhetsmål

Universitetet i Agders behandling av skjermingsverdige verdier skal ha et forsvarlig sikkerhetsnivå, og være i samsvar med regulatoriske, interne og avtalerettslige krav til forebyggende sikkerhet. Gradert og annen skjermingsverdig informasjon skal sikres gjennom tilfredsstillende fysiske, tekniske og organisatoriske tiltak. All sikring av skjermingsverdige verdier skal baseres på risikovurderinger.

UiA skal inkludere samfunnssikkerhet, beredskap, informasjonssikkerhet og personvern i universitetets beslutningsprosesser for å sikre kontinuerlig forbedring i sikkerhetsarbeidet.

Det skal legges til rette for nødvendig sikkerhetsopplæring til ansatte og studenter og gjøre dem i stand til å håndtere og forbygge uønskede hendelser.

4.3 Konfidensialitet

Skjermingsverdige verdier som behandles ved UiA skal være forsvarlig beskyttet mot uautorisert tilgang.

4.4 Integritet

Skjermingsverdige verdier som UiA har ansvaret for skal være forsvarlig beskyttet mot uautoriserte endringer. Verdiene skal ikke kunne endres utilsiktet.

4.5 Tilgjengelighet

Skjermingsverdige verdier som behandles ved UiA skal være tilgjengelige for autoriserte brukere ved behov.

5 Sikkerhetsorganisasjon, roller, ansvar og myndighet

STILLING/ROLLE	ANSVAR SOMRÅDE OG MYNDIGHET
Universitetsstyret	Styret har det overordnede ansvaret for at UiA drives i overensstemmelse med de lover, forskrifter og regler som gjelder. Styret vedtar styringssystem for sikkerhet del 1.
Universitetsdirektør	Virksomhetens øverste administrative leder og har overordnet ansvar for sikkerhet ved UiA. • Orienterer styret ved behov • Fordeling av roller og myndighet i sikkerhetsarbeidet • Utøver overordnet ansvar for all behandling av personopplysninger • Strategisk kriseleder ved hendelser • Oppfølging av internkontroll • Skal iverksette nødvendige tiltak.
Dekan og avdelingsdirektører	Skal overholde krav stilt gjennom lov, forskrift og UiAs styringssystem for sikkerhet. Dekan skal også orientere fakultetsstyret ved behov.
Fakultetsdirektører og avdelingsdirektører	Skal avsette tilstrekkelige ressurser for ivaretagelse av sikkerhet, beredskap og personvern innen sitt ansvarsområde. Har også ansvar for at ansatte, studenter og gjester er informert om rutiner og retningslinjer og deltar på nødvendig opplæring. • Skal sørge for at hendelser og avvik følges opp i tråd med UiAs interne retningslinjer. • Gjennomføre sårbarhetssamtaler der det er behov for dette i henhold til sikkerhetsloven. • Ansvar for behandling av personopplysninger i egen enhet.
Sikkerhetsleder/CSO	Sikkerhetsleder har delegert oppgaver og myndighet til å utøve daglig sikkerhetsledelse, inkludert administrasjon av sikkerhetsklareringer og autorisasjon. Vedkommende rapporterer til universitetsdirektøren i alle saker som omhandler UiAs sikkerhet. Sikkerhetsleder skal holde et oppdatert bilde av verdier, trusler og sårbarheter ved UiA, og utarbeide og legger frem ledelsens gjennomgang innenfor sikkerhetsområdet i samarbeid med CISO. I tillegg koordinerer sikkerhetsleder krisehåndtering og hendelser med krisepotensiale. Sikkerhetsleder følger egen <u>stillingsinstruks</u> som fastsettes av universitetsdirektøren.
Informasjonssikkerhetsleder/ CISO	Informasjonssikkerhetslederen rapporterer til universitetsdirektøren i saker som omhandler UiAs informasjonssikkerhet. Informasjonssikkerhetsleder skal holde et oppdatert bilde av verdier, trusler og sårbarheter innenfor informasjonssikkerhet ved UiA, og utarbeider og legger frem ledelsens gjennomgang innenfor informasjonssikkerhet i samarbeid med CSO.

	Informasjonssikkerhetslederen deltar i hendelseshåndtering og oppfølging der informasjonssikkerhet påvirkes, og skal følge opp hendelser og avvik på overordnet nivå innen informasjonssikkerhet samt påse at enhetene lukker disse. Informasjonssikkerhetsleder følger egen <u>stillingsinstruks</u> som fastsettes av universitetsdirektøren.
XX – skal besluttet av universitetsdirektør	Leder ressursgruppe rådgivende eksportkontroll og ansvarlig internasjonalt samarbeid.
Økonomi- og Campusdirektør	Ansvarlig for fysiske sikringstiltak og beskyttelse av fysiske verdier. Delegerer oppgaver og myndighet innen området i egen avdeling. Ansvarlig for at UiAs plikter som leietaker innenfor brannvern følges opp i henhold til lovverk, forskrifter og interne retningslinjer.
PO-direktør	Ansvarlig for UiAs HMS og avvikssystem. Dette innebærer blant annet beredskapstelefon, HMS koordinator og pårørendetelefon.
IT-direktør	Er ansvarlig for at alle ansatte og studenter ved UiA har tilgang til tjenester og materiell slik at brukerne kan beskytte UiAs IT-infrastruktur, informasjon og informasjonssystemene. Er ansvarlig for at IRT og Rådgivende Ingeniør Elektro, RIE, besatt og har nødvendig opplæring og ressurser.
Utdanningsdirektør	Ansvarlig for at lover, forskrifter og interne overordnede retningslinjer innen studentsikkerhet følges opp. Eier interne sikkerhetsrutiner som gjelder på tvers i matrisen. Delegerer oppgaver og myndighet i egen avdeling.
Internkontroll	Internkontrollfunksjonen skal å bistå ledelsen med å koordinere, utvikle og vedlikeholde internkontrollsystemet. Har sammen med CSO, CISO og HMS-koordinator ansvar for oppfølging av rapporter til myndigheter som omhandler HMS. Internkontroll rapporterer til universitetsdirektør.
Personvernombud	Personvernombudet er en uavhengig rolle og er sentral i UiA sin etterlevelse av personvernlovgivningen. Ombudet gir råd til ledelsen og andre ved UiA og skal kontrollere etterlevelsen av regelverket. I tillegg er personvernombudet kontaktpunkt for de registrerte og Datatilsynet.
Studentombud	Studentombudet er en uavhengig bistandsperson som skal gi studentene råd og hjelp til studentene i deres studiesituasjon. Studentombudet kan bistå og gi råd til studenter i forbindelse med varsel om kritikkverdige forhold knyttet til studiesituasjonen ved UiA.
Alle ansatte	Pliker å gjøre seg kjent med aktuelle lover og forskrifter innen sikkerhet, beredskap og personvern. Pliker også å delta på sikkerhetsopplæring. Skal bidra til å forhindre og rapportere avvik når disse oppstår

6 Beredskap

UiA har en tredelt beredskapsorganisering med fastsatte roller og mandat. Beredskapsorganisasjonen trer i kraft når uønskede hendelser inntreffer som krever en midlertidig organisering for å ivareta UiAs kjerneverdier. Organisering av beredskapsarbeidet, fullmakter og mandat i kriser, er beskrevet i UiAs beredskapsplanverk.

6.1 Taktisk nivå

Taktisk nivå består av alle fakulteter og avdeling for lærerutdanning og ledes av fakultetsdirektører (fakultet) og avdelingsdirektør (lærerutdanning). Taktisk nivå har ansvar for hendelseshåndtering av uønskede hendelser innenfor eget ansvarsområde. Dekan deltar i all hendelseshåndtering og overtar ansvar når fakultetsdirektør/avdelingsdirektør ikke er tilgjengelig.

Taktisk nivå består i tillegg av IRT (Incident Response Team), førstelinjetjenesten UiA-hjelp og Pårørendetelefon.

6.2 Operativt nivå

Operativt nivå ledes av CSO og rapporterer direkte til leder av strategisk nivå (Universitetsdirektør) i alle hendelser som håndteres som kriser, eller hendelser med krisepotensiale. Operativt nivå består ellers av faste medlemmer fra følgende administrative avdelinger;

- Personal- og Organisasjonsavdelingen
- Utdanningsavdelingen
- IT-avdelingen
- Kommunikasjonsavdelingen
- Økonomi og campusavdelingen

6.3 Strategisk nivå

Strategisk nivå har fem faste medlemmer/roller: Universitetsdirektør, Rektor, Kommunikasjonsdirektør, Personal- og Organisasjonsdirektør og Utdanningsdirektør. I tillegg til de faste medlemmene skal det være minimum en loggfører.

Universitetsdirektøren utpeker stedfortreder i sin rolle som også deltar.

7 Beredskapstelefonen

UiA har en beredskapstelefon hvor en gruppe ansatte går i turnus for mottak av beredskapshenvendelser. Beredskapstelefonen er for håndtering av større avvik, og ikke bygningsmessige feil og mangler som håndteres av driftstelefonen. Den som har vakt på

beredskapstelefonen skal gjøre førsteinnsats i hendelseshåndtering av potensielle kriser. Dette omhandler mobilisering, aktivering og bruk av beredskapsplanverket.

8 Avvikshåndtering

UiA har etablert avviksrapportering via sin «Si fra sider» der sikkerhetsbrudd også rapporteres. Det er etablert egne rutiner der en arbeidsgruppe håndterer og videreformidler innmeldte avvik. I tilfeller der det vurderes risiko for personsikkerhet, studieprogresjon eller omdømme skal CSO varsles. Sikkerhetsleder koordinerer sikkerhetsbrudd på tvers av fagområder.

Rutine for avvikshåndtering er en del av styringssystemets utførende del. Avvikssystemet ansatte eies av personal- og organisasjonsdirektøren.

9 Rapportering

Ledelsens gjennomgang (LG) er et møte som ledes av virksomhetens administrative leder og der alle øvrige ledere som påvirker eller kan påvirkes av sikkerhetsstyringssystemet deltar. Det skal informeres om siste års forebyggende sikkerhetsarbeid, blant annet fra håndtering av uønskede hendelser, resultater fra revisjoner samt informasjon om endringer (interne og eksterne) som kan påvirke det forebyggende sikkerhetsarbeidet.

Styret informeres årlig med sikkerhetsstatus i årlig HMS rapport.

Overordnet risikobilde for UiA vil bli presentert for styret i egen gjennomgang.

10 Styringssystem for sikkerhet - gjennomførende del

Alle ansatte og studenter ved UiA har plikter og ansvar relatert til sikkerhet og beredskap. Dette innebærer blant annet å bidra i det forbyggende arbeidet, som å sette seg inn i gjeldende instruksjer og sikkerhetsrutiner, og å rapportere avvik og hendelser.

For å nå sikkerhetsmålene skal operativt sikkerhetsarbeid ved UiA være balansert og risikojustert, systematisk og inngå som en helhetlig del av virksomhetsstyringen.

10.1 Sikkerhetsområder

10.1.1 Krisehåndtering

Beredskap ved UiA handler om å gjennomføre planlagte tiltak og øvelser for å kunne håndtere uønskede hendelse dersom noe skjer. Formålet med UiAs plan for beredskap og krisehåndtering er å gi en overordnet beskrivelse av det systematiske forbyggende beredskapsarbeidet ved UiA, samt tydeliggjøre organisering, roller og ansvar i en krise eller i en uønsket situasjon.

Organisering av beredskapsarbeidet, fullmakter og mandat i kriser, er beskrevet i UiAs Beredskapsplan.

UiA har en tredelt beredskapsorganisering med fastsatte roller og mandat. Beredskapsorganisasjonen trer i kraft når uønskede hendelser inntreffer som krever en midlertidig organisering for å ivareta UiAs studenter, ansatte, tilknyttede personer og øvrige verdier.

10.1.2 Verdioversikt

Oversikt og vurdering av verdien av UiAs informasjon, utstyr og ressurser skal bidra til å oppnå tilstrekkelig kjennskap til, og sikring av disse. For å beskytte UiAs verdier og nasjonale sikkerhetsinteresser, og etterleve lovkrav, er det etablert egne retningslinjer for verdikartlegging, klassifisering, merking, behandling, arkivering og gradering av informasjon, utstyr og ressurser. Informasjon skal i størst mulig grad være åpen og tilgjengelig for ansatte, studenter og personer tilknyttet UiA så lenge det ikke strider mot lovkrav og hensynet til sikkerhet og beredskap.

10.1.3 Fysisk sikkerhet

Fysisk sikkerhet ved bygninger og arealer handler om å forebygge uønskede hendelser og regulere hvem som har tilgang til hvilke områder ved UiA. Det skal benyttes en risikobasert tilnærming for ivaretagelse av fysisk sikkerhet basert på UiAs vedtatte risikoaksept nivå. En risikobasert tilnærming innebærer at det skal gjennomføres risikovurderinger i planlegging, oppføring og endring av UiAs bygninger, eiendommer og områder.

Risikovurderinger skal blant annet foretas ved:

- planlegging og oppføring av nye bygninger
- omdisponering eller endring/ombygging av hele eller deler av eksisterende bygninger
- inngåelse av leiekontrakter

Ved utleie skal UiA være særlig oppmerksom på skjermingsverdige objekter/infrastruktur i det utleide arealet/bygget som skal benyttes av leietaker og hvilke forpliktelser UiA i så fall påtar seg med tanke på sikring.

Universitetet i Agder har retningslinjer for fysisk sikkerhet og brannvern som er basert på nasjonale lovkrav. Kravene til fysisk sikkerhet finnes i brannvernloven, sikkerhetsloven, arbeidsmiljøloven og internkontrollforskriften.

UiA har egne retningslinjer og rutiner som er nødvendig for håndtering av fysisk sikkerhet, eksempelvis adgangskontroll.

10.1.4 Informasjonssikkerhet og personvern

Informasjonssikkerhet handler om å sikre informasjonsbehandling, som foregår i samspill mellom mennesker, prosesser og teknologi. Personvern er individets rett til privatliv og kontroll over egne personopplysninger. Kunnskapsdepartementet har fastsatt policy for informasjonssikkerhet og personvern i høyere utdanning og forskning (regjeringen.no), som beskriver krav til forsvarlig informasjonsbehandling, IT-sikkerhet og personvern. Dette danner grunnlaget for UiAs policyer, retningslinjer, prosedyrer og rutiner og sikkerhetsarbeid innen informasjonssikkerhet og personvern.

10.1.5 Personellsikkerhet

Personellsikkerhet er tiltak, handlinger og vurderinger for å hindre at personer utgjør en sikkerhetsrisiko der sikkerhetsloven brytes. Det er sikkerhetsleder/CSO som på mandat fra universitetsdirektøren ivaretar daglig oppfølging av sikkerhetslovens kapittel 8. Det er utarbeidet egne rutiner for arbeidet med sikkerhetsklarering og autorisasjon.

10.1.6 Risikostyring

Det forebyggende sikkerhetsarbeidet ved UiA skal være risikobasert. Dette innebærer at risikoanalyser og vurderinger utføres etter anerkjente standarder. Nasjonale og lokale risiko- og trusselvurderinger danner sammen med interne sikkerhetsvurderinger utgangspunktet for UiAs egne risikovurderinger og tilhørende risikoreduserende tiltak.

- Overordnet risikobilde skal gjennomgås hvert år og legges frem for ledelse og styret årlig. Overordnet ROS er basert på trusselvurderinger, sikkerhetssituasjon i samfunnet og underliggende ROS fra fakultet og avdelinger ved UiA.
- Ved større endringer i omgivelsene eller ved alvorlige hendelser skal det vurderes om ROS må gjennomgås og oppdateres utenom gitt frekvens.
- ROS ved fakultet og avdeling for lærerutdanning skal gjennomgås hvert fjerde år, eller ved behov. Eksempler på hendelser som medfører behov for ny gjennomgang av risikovurdering er nye aktiviteter, nye/endringer i lokaler, nye maskiner og/eller produkter m.m.
- Informasjonssikkerhets-ROS gjennomføres annethvert år av systemeier. CISO er ansvarlig for oppdatering av rutiner og oppfølging av årshjul og ROS – informasjonssikkerhet.
- Systemeiere har ansvar for ROS-vurderinger av sine system i henhold til gjeldende Policy.

10.1.7 Eksportkontroll

Eksportkontroll (regjeringen.no) handler om å ikke dele eksportregulert sensitiv kunnskap og flerbruksteknologi med land utenfor Norge, uten lisens.

10.1.8 Anskaffelser

Alle offentlige virksomheter skal gjennomføre offentlige anskaffelser i henhold til lov og forskrift. Sikkerhetsloven har bestemmelser som retter seg mot sikkerhetsgradert informasjon, objekter eller infrastruktur. I tillegg omfattes også anskaffelse av skjermingsverdige ugraderte informasjonssystemer av bestemmelser i sikkerhetsloven.

UiA er underlagt sikkerhetsloven og har skjermingsverdige verdier, såkalt grunnleggende nasjonale funksjoner (GNF) relatert til forskning og utvikling, og må derfor også vurdere om bortfall av en anskaffelse vil gå ut over evnen til å levere disse funksjonene.

UiA skal også vurdere om innkjøp og avhending av utstyr og systemer som benyttes i forskning og i utøvelse av internasjonalt kunnskapssamarbeid, faller inn under eksportkontrollens reguleringer og krav til lisens.

Det pålegges også UiA å gjennomføre risikovurderinger, følge opp tiltak, etablere jevnlig leverandørkartlegging der det påses at leverandører fyller avtalte sikkerhetskrav,

11 Styringssystem for sikkerhet - kontrollerende del

Formålet med kontrollaktiviteter er å kunne vurdere i hvilken grad de etablerte tiltakene er tilstrekkelige og effektive for å sikre etterlevelse av relevant regelverk og overordnede føringer. Gjennom de kontrollerende aktivitetene vil det avdekkes forbedringsområder knyttet til eksisterende tiltak og nye tiltak kan bli identifisert og iverksatt.

UiA sine kontrollaktiviteter innenfor sikkerhet består av faste aktiviteter som gjennomføres i henhold til årshjul, årsplaner eller når sikkerhetssituasjonen krever det.

11.1 Evaluering av prestasjon

Det skal jevnlig gjøres en evaluering av sikkerhet og beredskap og identifiseres forbedringsområder innen ulike ansvarsområder i henhold til kravene i dette styringssystem for sikkerhet.

11.1.1 Overvåking

Sikkerhetsmål skal overvåkes, måles, analyseres og evalueres. Ved behov skal tiltak besluttes og iverksettes.

11.1.2 Internrevisjon

UiA skal ved behov gjennomføre internrevisjon av styringssystem for sikkerhet. Internrevisjon er en uavhengig, objektiv bekreftelses- og rådgivningsfunksjon som har til hensikt å tilføre merverdi og forbedre styringssystemets drift.

11.1.3 Ledelsens gjennomgang

Ledelsens Gjennomgang (LG) et møte der ledelsen går igjennom en konsentrert presentasjon av den viktigste informasjonen om styringssystemet med den hensikt å ta videre valg og beslutninger for å sikre effektiviteten av styringssystemet. LG skal gjennomføres minimum en gang årlig og oftere ved behov.

11.2 Forbedring

UiA skal jevnlig forbedre egnethet, tilstrekkelighet, og virkning av styringssystemet. Dette vil si å identifisere, dokumentere og gjennomføre tiltak for å forbedre sikkerhet og beredskap. Dette innebærer blant annet å jobbe med kontinuering forbedring ut fra evaluering av øvelser, læring fra hendelser og situasjoner og håndtering av avvik.

11.3 Dokumentasjon

Styringssystem for sikkerhet skal dokumenteres og dokumentasjon skal gjennomgås og oppdateres ved behov

Rammeverket for dokumentasjon skal være likt for alle internkontrollområdene ved.

Dokumentasjonen inneholder ulike nivåer med følgende dokumentasjonstyper, ansvar og innhold:

	NIVÅ	DOKUMENTASJONSTYPE	ANSVAR	INNHold
EKSTERNT	Styrende	Lover, forskrifter, tildelingsbrev o.l	Myndighet og overordnet departement	HVA skal gjøres
	Styrende	Policyer og retningslinjer	Virksomhetsledelsen	HVA skal gjøres av HVEM
INTERNT	Gjennomførende	Rutiner, prosedyrer, instruksjoner og dokumentasjon av andre tiltak	Ledere på ulike nivå ut fra ansvarsområde	HVORDEN og NÅR skal noe gjøres
	Kontrollerende	Logger, referat, rapporter, notat o.l. om utførte oppgaver, revisjon, beslutninger mv.	Utførere (alle ansatte ut fra ansvar)	HVA er utført eller besluttet iht. ovennevnt

Figur 1 Fra UiAs rammeverk for dokumentasjon av internkontroll.

11.4 Opplæring

Opplæring skal bidra til å bygge en god sikkerhetskultur ved UiA. Den skal bevisstgjøre ansatte og studenter om betydningen av informasjonssikkerhet og gjøre dem i stand til å etterleve UiAs sikkerhetspolicy i sitt daglige virke. Opplæring i sikkerhet generelt og informasjonssikkerhet må derfor tas inn som en naturlig del av opplæringen av på alle nivå i organisasjonen.

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 sikkerhet inngå i UiAs lederopplæring.

Informasjon om sikkerhet ved UiA 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.