Innledning

Alle ansatte og studenter må kjenne til Grunnprinsipper for informasjonssikkerhet. Ledelsessystem for informasjonssikkerhet ved UiA ivaretar de kravene som lovverket og Kunnskapsdepartementet, stiller til arbeidet med informasjonssikkerhet ved UH institusjoner. Derfor er det også avgjørende at all informasjon som UiA forvalter i administrasjon, forskning, undervisning og offentlig formidlingsarbeid er tilfredsstillende sikret mot brudd på:

Konfidensialitet: hindre at uvedkommende får tilgang til sensitiv eller beskyttelsesverdig informasjon.
Integritet: hindre uønsket endring, sletting eller manipulering av informasjon.
Tilgjengelighet: sikre brukere tilgang til informasjon når de har behov for det.

Uønskede hendelser som fører til brudd på **konfidensialitet** kan for eksempel være at taushetsbelagt informasjon offentliggjøres på internettet, mens brudd på **integritet** kan oppstå ved at de samme opplysningene endres på utilsiktede måter av uvedkommende. Uønskede hendelser som fører til brudd på **tilgjengelighet**, kan være at ansatte eller studenter ikke får tak i informasjon de har behov for, fordi datasystemene er ute av drift.

Kort fortalt beskriver Ledelsessystemet hvordan arbeidet med informasjonssikkerhet ved UiA skal foregå.

Hvem skal vite om dette?

Alle som jobber eller studerer ved UiA må kunne grunnprinsippene for informasjonssikkerhet. Det er et felles ansvar å sørge for at vi beskytter informasjonen vår.

Hva står i dokumentene?

Noe av innholdet er ment for ansatte og studenter, noe er ment for ledere, og noe er ment for ansatte med dedikerte sikkerhetsoppgaver.

Ledelsessystemet består av tre deler; styrende, utførende og kontrollerende dokumenter. Til sammen utgjør dette Ledelsessystem for informasjonssikkerhet. Ledelsessystemets første hoveddel inneholder styrende dokumenter. De styrende dokumentene definerer rammene for UiAs arbeid med informasjonssikkerhet, og er noe alle skal være kjent med.

Alle ansatte og studenter skal ha gjort seg kjent med IT-reglementet. Dette er en forutsetning for å kunne ha en brukerkonto ved UiA.

Ansatte og studenter skal overholde lover, regler og retningslinjer som til enhver tid gjelder for informasjonssikkerhet og personvern. Sikkerhetsbrudd og sikkerhetstruende hendelser skal alltid rapporteres. Det samme gjelder dersom det oppdages sikkerhetshull eller sårbarheter. Ansatte skal bistå ved planlegging, gjennomføring eller oppfølging av konkrete sikkerhetsoppgaver dersom de blir bedt om det. Ansatte og studenter skal ha grunnleggende kunnskap om informasjonssikkerhet ref. Ledelsessystem for informasjonssikkerhets – hoveddokument pkt. 5.1.8.

Sikkerhetsbrudd og sikkerhetshendelser

Ved sikkerhetsbrudd og sikkerhetstruende hendelser eller ved mistanke om dette, er samtlige ansatte og studenter pliktig til å melde fra gjennom UiAs Si ifra system. Dersom det er mulig, iverksettes umiddelbare tiltak for å forhindre at den uønskede hendelsen finner sted. Dersom den uønskede hendelsen allerede har funnet sted, vil det bli iverksatt skadereduserende tiltak. Det er helt avgjørende at UiAs Incident Response Team (IRT) får melding så raskt som mulig. For sen eller feil håndtering, kan raskt eskalere til å bli en krise.

Hvem mottar meldingen?

IRT ved UiA koordinerer og håndterer IKT-sikkerhetshendelser og personvernhendelser. Enheten er dedikert til IKT-sikkerhet og IKT-hendelseshåndtering. IRT innehar myndighet til selvstendig å iverksette nødvendige tiltak for å beskytte nettverk og IT-ressurser i forbindelse med IKT-sikkerhetshendelser. IRT er en støtte og samarbeidspartner ved sikkerhetsbrudd/avvik og sikkerhetshendelser.

Mistenkelig e-post

Rapporter mistenkelig e-post! Slike e-poster skal videresendes til spam@uia.no, slik at IRT kan håndtere disse e-postene.

Avvik med konsekvenser for personvernet

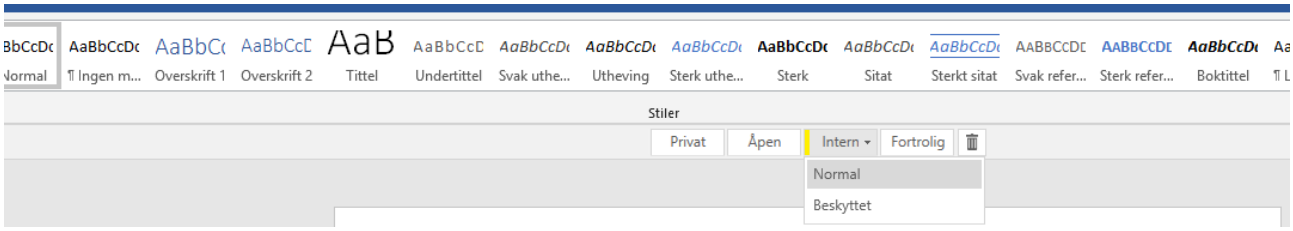
Samtlige avvik som har en konsekvens for personvernet, skal meldes som et sikkerhetsbrudd umiddelbart via Si ifra systemet. Det er krav til at UiA varsler Datatilsynet innen 72 timer etter at avvik er blitt kjent. Derfor er det helt avgjørende at IRT kan starte håndteringen av avviket og vurdere om avviket må meldes til Datatilsynet. IRT har egne rutiner for å håndtere avvik knyttet til personvern.

Klassifisering og håndtering av informasjon

All informasjon skal klassifiseres. Den som utsteder informasjon skal på forhånd vurdere konsekvensene (skadepotensialet) dersom uvedkommende får tilgang til informasjonen, og på bakgrunn av dette sette en klassifisering. Les mer om sikker lagring på Innaskjærs. Office 365 er beskyttet med to-trinns autentisering, les mer om dette her.

Klassifiseringsløsningen UiA har etablert i Office 365, er konstruert slik at du aktivt må velge klassifiseringene Intern/beskyttet eller Fortrolig. Da vil dokumentet krypteres og få nødvendig tilgangsstyring.
For at dokumentet skal bli beskyttet på korrekt måte, er det en forutsetning at klassifiseringsløsningen som er satt opp for UiA i Office 365 benyttes.

Det er ikke bygget inn ekstra beskyttelse i klassifiseringene åpen og intern/normal. Valg av lagringsområde må derfor vurderes ut fra hvem som skal ha tilgang til informasjonen.



Det er ikke tillatt å behandle eller lagre strengt fortrolig informasjon i Office 365 eller universitetets IT-systemer. Unntak for behandling av denne type informasjon er UiAs arkivsystem og Tjenester for sensitive data 2.0 (TSD 2.0). IT-avdelingen skal konsulteres før strengt fortrolig informasjon behandles.

To-trinns autentisering må alltid benyttes for tilgang til fortrolig og streng fortrolig informasjon.

Alle ansatte plikter å sette seg inn i retningslinjene som gjelder for klassifisering av informasjon (gjennomførende dokument). Det samme gleder studenter som behandler personopplysninger eller sensitive data i prosjekter/oppgaver. Bruk klassifiseringsplakaten, dersom du er usikker.

Kriterier for akseptabel risiko

Arbeidet med informasjonssikkerhet skal sørge for at informasjonsverdiene ved UiA til enhver tid er tilfredsstillende sikret mot brudd på konfidensialitet, integritet og tilgjengelighet. For å oppnå tilfredsstillende informasjonssikkerhet skal arbeidet basere seg på følgende kriterier for akseptabel risiko:

Åpen informasjon: Integritet til informasjonen skal vektlegges foran hensynet til tilgjengelighet. Kortere avbrudd i informasjonens tilgjengelighet aksepteres. Dette omfatter for eksempel informasjon som skal være offentlig tilgjengelig, uavhengig av om dette dreier som forsknings-, undervisnings- eller administrativ informasjon.

Intern informasjon: Det aksepteres kun mindre brudd på denne informasjonens konfidensialitet og integritet. Kortere avbrudd i informasjonens tilgjengelighet aksepteres. Dette omfatter for eksempel ikke-sensitive personopplysninger[1], karakterer, store studentarbeider, ikke-sensitive forskningsdata og -arbeider som ikke er godkjent for publisering/offentliggjøring, upubliserte artikkel- eller bokmanus, utkast til strategier/planer eller ikke publiserte forslag til forskningsprosjekter.

Det aksepteres ikke brudd på konfidensialitet og integritet på informasjon som er unntatt offentlighet, taushetsbelagt eller personopplysninger innhentet i forskningsøyemed. Kortere avbrudd i informasjonens tilgjengelighet aksepteres.

Det aksepteres ikke brudd på konfidensialitet og integritet til eksamensoppgaver (tekster/forslag) og eksamensbesvarelser. Det samme gjelder uferdige eller innleverte studentoppgaver (bachelor/master) og avhandlinger (p.hd.) som ikke skal eller ikke er godkjent for publisering/offentliggjøring. Korte avbrudd i informasjonens tilgjengelighet aksepteres, dersom dette ikke vanskeliggjør eksamensgjennomføring eller innlevering og sensurering av eksamensbesvarelser, studentoppgaver eller p.hd. -avhandlinger.

Fortrolig: Det aksepteres ikke brudd på konfidensialitet og integritet til informasjon gradert fortrolig. Kortere avbrudd i informasjonens tilgjengelighet aksepteres. Dette omfatter informasjon som vil kunne forårsake skade for UiA, offentlige interesser, enkeltindivider eller samarbeidspartnere ved at informasjonen blir kjent for uvedkommende, for eksempel enkelte arbeidsdokumenter, risiko- og sårbarhetsvurderinger, dokumenterte sikringstiltak, enkelte strategidokumenter, sensitive

[1] I EUs personvernsforordning artikkel 4 defineres personopplysninger som enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator.

personopplysninger[2], fortrolige forskningsdata og -arbeider og informasjon om personer som har adressesperre kode 7 (fortrolig adresse).

Strengt fortrolig:
Det aksepteres ikke brudd på konfidensialitet eller integritet til informasjon gradert strengt fortrolig. Kortere avbrudd i informasjonens tilgjengelighet aksepteres. Dette omfatter informasjon som vil kunne forårsake betydelig skade for UiA, offentlige interesser, enkeltindivider eller samarbeidspartnere at informasjonen blir kjent for uvedkommende, for eksempel strengt fortrolige forskningsdata, særlige sensitive personopplysninger og informasjon om personer som har adressesperre kode 6 (strengt fortrolig adresse).

Personvern

I EUs personvernsforordning artikkel 5 defineres ivaretakelse av personopplysningenes konfidensialitet og integritet som grunnprinsipp ved behandling av personopplysninger. Videre kreves dokumentasjon av sikringstiltakene. Hovedreglene om informasjonssikkerhet finnes i forordningens artikkel 32. Mer informasjon om personvern ved UiA finner du på Innaskjærs.

Krav til systemer, tjenester og applikasjoner

UiA benytter seg av en rekke systemer og tjenester fra eksterne aktører. Derfor er det avgjørende at de systemer og tjenester UiA benytter, imøtekommer gitte krav i lov og forskrift. Rutine for anskaffelse av system og tjeneste skal alltid etterleves.

Nødvendig informasjon om dette finnes på Innaskjærs.

Alle systemer skal ha en systemeier og en systemadministrator. Systemeier er alltid enhetsdirektør, mens systemadministratorrollen delegeres til en ansatt i enheten. Systemeier har ansvar for tjenesten, og er den som skal signere databehandleravtalene. Systemadministrator er ansvarlig for å gjennomføre det utøvende arbeidet med informasjonssikkerhet og personvern i systemet/tjenesten.

Systemintegrasjoner er ofte kompliserte og krever kompetanse og deltagelse av mange grupperinger:

- noe skal utvikles
- det skal på plass en databehandleravtale
- løsningen skal risikovurderes
- løsningen skal ha stabil drift
- være redundant og skalerbar
- rettigheter skal delegeres
- dokumentasjon skal produseres
- tjenesteportefølje skal oppdateres med planverk og budsjett

[2] I EUs personvernsforordning artikkel 9 og betrakting 75 defineres særlige kategorier av personopplysninger (sensitive personopplysninger) når behandlingen gjelder personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion eller overbevisning, fagforeningsmedlemskap, og behandling av genetiske- og biometriske opplysninger, helseopplysninger, seksuelle forhold eller straffedommer og straffbare forhold.

Det stilles i tillegg krav til tilfredsstillende informasjonssikkerhet og personvern ved bruk/anskaffelse/utvikling av systemer og tjenester. Dette innebærer at det må gjennomføres en risikovurdering før et system eller tjeneste kan anskaffes eller tas i bruk. Dette er uavhengig om dette er en gratis- eller betalingstjeneste. En databehandleravtale må også inngås med leverandøren, dersom personopplysninger finnes/behandles i systemet/tjenesten. I tillegg stilles det krav gitt i lov og forskrift for offentlige anskaffelser.

Det er avgjørende at UiA har en helhetlig systemoversikt, slik at tilfredsstillende informasjonssikkerhet kan oppnås.

Det skal sikres at viktige vurderinger i forbindelse med bruk, anskaffelse eller utvikling av nye systemer/tjenester dokumenteres.

Register nytt system, tjeneste eller applikasjon her

Spesielt om overføring av opplysninger til utlandet

EUs personvernforordning gjelder for EØS-området. Det inkluderer alle EU-land, Island, Liechtenstein og Norge. Når personopplysninger overføres til et land som er etablert utenfor EØS-området, og som ikke er underlagt personvernforordningen, gjelder spesielle krav for overføring slik at beskyttelsesnivået som gjelder i EØS-området ikke undergraves. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/overfore/

NB! Etter at EU-domstolen vedtok Schrems-II dommen, er overføringer til USA særdeles problematiske. Resultatet av dette, er at det kan være vanskelig å finne et lovlig overføringsgrunnlag for å ta i bruk nye systemer som overfører data til USA, eller andre tredjestater som ikke er godkjente. Dette gjelder også for underleverandører som leverandøren benytter. Med overføring menes også fjernaksess, et eksempel på dette er support ol. **Personvernombudet skal alltid kontaktes før en tar i bruk et system eller tjeneste som overfører opplysninger til USA eller andre tredjestater.** Dette for å sikre at UiA opptrer innenfor lovverket.

Har du spørsmål knyttet til informasjonssikkerhet og personvern, finner du informasjon på informasjonssikkerhetssidene på Innaskjærs.