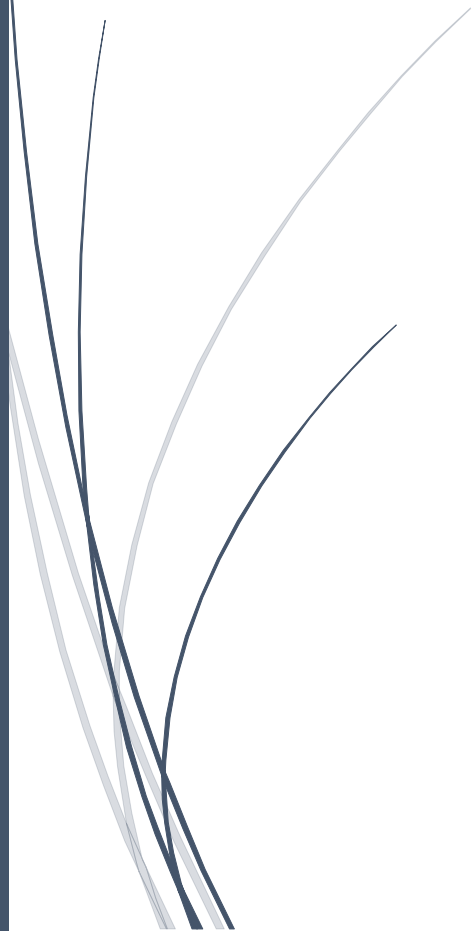
04.12.2018

Informasjonssikkerhet.

Ledelsens gjennomgang 2018



KUNSTHØGSKOLEN I OSLO
OSLO NATIONAL ACADEMY OF THE ARTS

Innledning

Informasjonssikkerhetsarbeidet ved Kunsthøgskolen i Oslo har i 2018 hatt fokus på å tilpasse seg til ny lovgivning (GDPR) som trådte i kraft i juli 2018.

Endringer som dette har medført er:

- Opprettelse av personvernombud.
- Utarbeide/inngå nye databehandleravtaler med tjenestetilbyderne.
- Risikovurdering av flere systemer.
- Utarbeide behandlingsprotokoller for informasjonssystemene
- Utarbeide personvernerklæringer

Kompetansehevende tiltak i 2018:

- Nasjonal sikkerhetsmåned. 200 benyttet e-læringstilbudet hvor rundt halvparten gjennomførte alle modulene. Skolen bør ha ambisjoner om å få flere til å delta og det bør derfor komme føringer fra ledelsen for å gjøre gjennomføringen for de ansatte obligatorisk.

Informasjonssystemer/eiere

Systemeier (ansvarlig)	System	Tjenestetilbyder	ROS (Risikovurdering)	Databehandler avtale	Lovverk	Følger lovverk	Klasse: Å(pen),I(ntern),S(ensistiv)
Økonomi	Agresso	Uninett	JA	JA	GDPR/REG	JA	I
	Basware	Uninett	JA	JA	GDPR/REG	JA	I
	SAP	DFØ	JA	JA	GDPR	JA	S
	Reisebestilling	G-Travel	JA	JA	GDPR	JA	I
	iZettle betalingsløsning	iZettle	NEI	NEI	GDPR/REG	NEI	I
HR	Jobbadmin	Jobbnorge.no	NEI	JA	GDPR	NEI	I
Studie	FS	USIT/UNIT	JA	JA	GDPR/HS	JA	S
	Canvas	Canvas	JA	JA	GDPR/HS	JA	I
	Semester Receipt	UNIT	NEI	JA	GDPR/HS	JA	I
	StudentWeb	UNIT	JA	JA	GDPR/HS	JA	I
	SøknadsWeb	UNIT	UNIT bh.ansv	UNIT bh.ansv	GDPR/HS	UNIT bh.ansv	I
	FagpersonWeb	UNIT	NEI	JA	GDPR/HS	NEI	I
	TimeEdit	Evolvera	NEI	NEI	GDPR	NEI	I
Bibliotek	P360	Uninett	JA	JA	GDPR/ARK/OFF	JA	S
	Cristin	UNIT	UNIT bh.ansv	UNIT bh.ansv	GDPR	UNIT bh.ansv	
	Bibsys	Uninett	JA	JA	GDPR	JA	Å
	Bibsys BRAGE			JA	GDPR		Å
	Bibsys ALMA	Uninett		JA	GDPR		Å
Drift	Adgangskontrollsystem	Schneider	JA	NEI	GDPR	NEI	I
	Kameraovervåkning	Tress	JA	NEI	GDPR	NEI	S
Innkjøp	Amesto/Visma	Uninett	NEI	JA	OA	NEI	I
IT	Helpdesk	Metadot	JA	JA	GDPR	JA	I
	Agora	Uninett	JA	JA	GDPR	JA	I
	BaaS (backup)	IPnett/KHIO	JA	JA	GDPR	JA	I
	Office 365	Microsoft	JA	JA	GDPR	JA	I
	Fillagring (Bruker/fellesområde)	KHIO	JA	Ikke relevant	GDPR	JA	I
	Nettverk lokalt	KHIO	JA	Ikke relevant	GDPR	JA	S
	Klienter	KHIO	JA	Ikke relevant	GDPR	JA	S
	Eduroam	KHIO/Uninett	Se ROS nettverk	JA	GDPR	JA	I
	Gjestenett	KHIO/Uninett	Se ROS nettverk	JA	GDPR	JA	I
	Telefoni	Telenor	JA	JA	GDPR	JA	I
	Nettadministrasjon (NAV)	Uninett	JA	JA	GDPR	JA	I
	Logganalyse	Uninett	JA	JA	GDPR	JA	I
	Sikkerhetsanalyse	Uninett	JA	JA	GDPR	JA	I
	Dokumentforvaltning (utskriftsløsning)	KHIO	JA	Ikke relevant	GDPR	JA	S
	Filesender	Uninett	JA	JA	GDPR	JA	I
	BAS	KHIO	JA	Ikke relevant	GDPR	JA	I
	AZURE	Microsoft	JA	JA	GDPR	JA	I
Kommunikasjon	Intranett/nettsider	Idium	NEI	NEI	GDPR	NEI	I
Ballett	Fysioterapeutjournal	ASPIT	JA	JA	HELS	JA	S
Utlånslager	Utlånsregister	?	NEI	NEI	GDPR	NEI	I

Sikkerhetsmål og strategi

Følgende mål for arbeidet med informasjonssikkerhet gjelder ved Kunsthøgskolen i Oslo:

1. *Arbeidet med informasjonssikkerhet skal bidra til høy kvalitet på forvaltningen av all informasjon som benyttes i administrasjon, forskning, undervisning og formidlingsaktiviteten ved Kunsthøgskolen i Oslo.*
2. *Arbeidet med informasjonssikkerhet skal bidra til at Kunsthøgskolen i Oslo ivaretar sine plikter som offentlig forvaltningsorgan og respekterer rettighetene til ansatte, studenter og deltakere i forskningsprosjekter.*

3. *Arbeidet med informasjonssikkerhet skal til enhver tid være i tråd med de krav som stilles i lover og forskrifter som gjelder for Kunsthøgskolen i Oslo, og følge opp de kravene som Kunnskapsdepartementet stiller til informasjonssikkerheten.*
4. *Arbeidet med informasjonssikkerhet skal ivareta grunnleggende personvernhensyn, herunder privatlivets fred, den personlige integriteten og opplysningskvaliteten, ved all elektronisk behandling av personopplysninger.*
5. *Arbeidet med informasjonssikkerhet skal bidra til at alle skal kunne ha tillit til kvaliteten på den informasjonen som kommuniseres og formidles av Kunsthøgskolen i Oslo, uavhengig av hvilke kanaler som benyttes.*
6. *Arbeidet med informasjonssikkerhet skal bidra til at Kunsthøgskolen i Oslo ivaretar sitt omdømme som et profesjonelt og kompetent forvaltningsorgan.*

Følgende strategi for sikkerhetsarbeidet er vedtatt for Kunsthøgskolen i Oslo:

1. *Alt arbeid med informasjonssikkerhet skal basere seg på risikovurderinger. Ingen sikringstiltak, uavhengig av om de er tekniske, organisatoriske, fysiske eller personalmessige, skal gjennomføres uten at risikovurderinger viser at det er behov for tiltakene. Risikovurderinger av IT-systemer og -tjenester, datanettverk og infrastruktur, arbeidsprosesser og fysiske forhold skal gjennomføres hvert annet år. Valg av sikringstiltak skal basere seg på tiltaksoversikten i ISO/IEC 27001: 2013 Annex A, jf. ISO/IEC 27002: 2013.*
2. *Ledelsen ved Kunsthøgskolen i Oslo vil bevilge nødvendige ressurser til opplæring og kompetanseheving for ledere og ansatte som er delegert ansvar for informasjonssikkerheten ved skolen eller som er pålagt å utføre konkrete arbeidsoppgaver. Opplæringen og kompetansehevingen skal i særlig grad fokusere på arbeidsmetodikken i risikostyrt informasjonssikkerhetsarbeid og praktisk bruk av konkrete arbeidsredskaper.*
3. *Ledere på Kunsthøgskolen i Oslo som er delegert ansvaret for informasjonssikkerheten skal sørge for at ressurser bevilges til planlegging, gjennomføring og oppfølging av pålagte arbeidsoppgaver innenfor deres ansvarsområder. Dette inkluderer iverksetting av sikringstiltak som er nødvendige for å oppnå tilfredsstillende informasjonssikkerhet.*
4. *Alle brukere av informasjonsverdiene til Kunsthøgskolen i Oslo skal gis informasjon om rutiner for sikker håndtering av informasjonsverdier og trusler mot informasjonsverdiene. De skal også informeres om avviksmeldingssystemet ved Kunsthøgskolen i Oslo. I tillegg skal de informeres om hensikten med og viktigheten av at avvik/sikkerhetsbrudd rapporteres.*
5. *Fjerndrift av Kunsthøgskolen i Oslo sine informasjonsverdier, for eksempel bruk av nettbaserte tjenester eller andre typer databehandlere, kan bare skje dersom risikoen for sikkerhetsbrudd er innenfor kriteriene for akseptabel risiko, og dersom de nødvendige avtaler er inngått og blir fulgt opp. Utkontraktering (eng.: outsourcing) av drift og forvaltning av informasjon med særskilte*

sikkerhetskrav, for eksempel sensitive personopplysninger eller konfidensielle forskningsdata, kan bare skje etter en spesielt grundig vurdering.

6. *Arbeidet med informasjonssikkerhet ved Kunsthøgskolen i Oslo skal til enhver tid basere seg på anbefalte og anerkjente standarder for styringssystemer for informasjonssikkerhet i offentlig sektor, jf. DIFIs referansekatalog versjon 3.1, punkt 2.16 (tilgjengelig på http://standard.difi.no/forvaltningsstandarder/referansekatalogen-html-versjon).*
7. *UNINETT og Sekretariatet for informasjonssikkerhet i UH-sektoren skal benyttes til rådgiving og bistand når det er nødvendig.*

Sikkerhetsmål og strategi vedtatt av styret dato: 14.06.2016

Sikkerhetsmål	**Sikkerhetsstrategi**	**Konsekvenser**
Det er ikke behov for endringer.	Det er ikke behov for endringer.	Ingen

Kriterier for akseptabel risiko

Akseptabel risiko vedtatt dato: 14.06.2016

Nåværende kriterier for akseptabel risiko:	**Endringer:**	**Konsekvens:**
Åpen informasjon: Integriteten og tilgjengeligheten til informasjon som er offentlig tilgjengelig, uavhengig av om dette dreier som forsknings-, undervisnings- eller administrative data, skal prioriteres. Integriteten til informasjonen skal prioriteres foran tilgjengeligheten.	Ingen endring	
Intern informasjon: Konfidensialiteten og integriteten til informasjon som benyttes til intern administrasjon/saksbehandling skal prioriteres. Det aksepteres kun mindre brudd på denne informasjonens konfidensialitet og integritet. Kortere avbrudd i informasjonens tilgjengelighet aksepteres.	Ingen endring.	
Sensitiv informasjon: Konfidensialiteten og integriteten til informasjon som er særlig viktig for institusjonen eller som er underlagt rettslig regulering, for eksempel spesielle typer forskningsdata eller opplysninger om enkeltpersoner (personopplysninger), skal prioriteres høyt. Det aksepteres ikke brudd på konfidensialiteten til sensitive personopplysninger. Det aksepteres ikke brudd på konfidensialiteten og integriteten til særlige sensitive forskningsdata som ikke er godkjent for publisering/offentliggjøring av prosjektansvarlig. Kortere avbrudd i informasjonens tilgjengelighet aksepteres.	Ingen endring.	

Sikkerhetsorganisering

- Styret – Beslutter og stiller krav.
- Direktør – Overordnet ansvar.
- Rektor – Rektor er forskningsansvarlig og har det overordnede ansvaret for informasjonssikkerheten i forskningsprosjekter
- CSO (seksjonssjef virksomhetsstyring) – Utøvende ansvar/ lede arbeidet.
- Informasjonssikkerhetsforum. – Rådgivende for sikkerhetsarbeidet.
- IRT – team (Hendelsesresponsteam bemannet av IT + seksjonssjef virksomhetsstyring) – operativ håndtering av sikkerhetshendelser.
- Seksjon- og avdelingsledere:
    - Seksjonsledere - daglig ansvar for informasjonssikkerhet innenfor sine ansvarsområder, herunder IT-systemer/tjenester som de har eierskapet til.
    - Avdelingsledere - daglig ansvar for informasjonssikkerhet innenfor sine ansvarsområder, herunder IT-systemer/tjenester som de har eierskapet til.
- Teamleder IT - daglig ansvar for informasjonssikkerhet innenfor sine ansvarsområder, herunder IT-systemer/tjenester som de har eierskapet til.
- Teamleder Drift - daglig ansvar for informasjonssikkerhet innenfor sine ansvarsområder, herunder IT-systemer/tjenester som de har eierskapet til.
- Brukere (ansatte, studenter, gjester) - skal overholde de rutiner og retningslinjer som til enhver tid gjelder for sikker håndtering av informasjonsverdier og personopplysninger.
- Personvernombud – håndterer forespørsler/klager om behandling av personopplysninger på Kunsthøgskolen i Oslo

Vurdering av eksisterende organisering:	Kjennskapen til metodikken for sikkerhetsarbeid i seksjonene ikke er tilstrekkelig til å utføre sikkerhetsoppgavene selvstendig. Mye av det praktiske informasjonssikkerhetsarbeidet må derfor midlertidig utføres av IT-enheten. Seksjonene sin rolle vil i disse tilfellene endres til å godkjenne sikkerhetsvurderingene som IT-enheten har gjort basert på samtaler med seksjonene. Informasjonssikkerhetsforumet består av samme årsak midlertidig av seksjonssjef virksomhetsstyring, seksjonssjef service brukerstøtte og infrastruktur og Teamleder IT.
Vurdering av behov for endringer:	Ansvaret for praktisk informasjonssikkerhetsarbeid tilbakeføres til seksjonene etter at tilstrekkelig opplæring er gitt. Funksjonen som midlertidig personvernombud må erstattes av permanent ordning.

Avviksmeldinger

De mest alvorlige avvik i løpet av perioden				
Avvik #	**Hendelses beskrivelse**	**Tiltak**	**Ansvarlig:**	**Frist:**
1	Rutiner/håndtering av varsler oppfylte ikke krav til beskyttelse av personopplysninger.	Endring av rutiner. Innføring av elektronisk skjema for varsling.	CSO (Seksjonssjef virksomhetsstyring)	01.01.2019
2	Filnavn på utskrifter ble lagret lokalt i logg på skriver	Endret skriveroppsett	Teamleder IT	Utført 23.10.2018

Sikkerhetsrevisjon

Som en del av riksrevisjonens årlige revisjon gjennomført oktober 2018

Revisjon fra riksrevisjonen:
• Databehandleravtaler i tråd med GDPR for Basware, Agresso og SAP overlevert til riksrevisjonen. • Rolleoversikt for tilganger overlevert riksrevisjonen • Rutiner for systematisk revisjon av tilgangsrettigheter overlevert riksrevisjonen • Passordpolicy overlevert riksrevisjonen

Status på risikovurderinger

Gjennomgang av risikovurderinger:	**Kommentar:**
Oppsummering av hovedfunn fra risikovurderinger:	Behov for sterkere autentisering på flere tjenester. Risikoen er stor for vellykket kompromittering av Studentweb og G-travel ved bruk av phishing som metode. Dårlig kontroll med tilganger på fellesområdene på grunn av uklart eierskap til informasjonen. Stor risiko for at informasjon kan mistes ved tap av klienter. Stor risiko for at fortrolig informasjon på papirformat blir akkumulert / håndtert usikkert. Manglende rutiner/utstyr for makulering. Stor risiko for brudd på GDPR ved kameraovervåkning. Stor risiko i forbindelse med håndtering av adgangskort.
Hvem har gjennomført risikovurderinger?	De fleste seksjonene har gjennomført/fått hjelp til å gjennomføre en eller flere risikovurderinger.

Hva er risikovurdert?	Ca 80% av informasjonssystemene er vurdert. En del av risikovurderingene er nå eldre enn 2 år og må revideres. Kvaliteten på vurderingene må også heves. Dette følges opp ved neste ledelsens gjennomgang

Status på risikohåndtering

Status på risikohåndtering:	Seksjonene har ikke i tilstrekkelig grad kommet fram til tiltak for å redusere avdekket risiko.
Vurdering av risikohåndteringsprosessen:	Ikke tilfredsstillende. Systemeierne må i større grad ta eierskap for risikohåndteringsarbeidet og aktivt gjøre risikoreduserende tiltak basert på funn fra risikovurderingene.
Tiltak:	Ledelsen må vurdere behov for ytterligere bemanning og kompetanseheving innenfor informasjonssikkerhetsarbeidet. Ansvarlig for aktiviteten er direktør. Systemeiere reviderer ROS for sine systemer, lager tiltaksplan og rapporterer på dette innen 01.10.2019 Det må settes av ressurser til å implementere sikrere pålogging til G-travel. Det vil påløpe kostnader for tjenesten i drift (SMS-kostnader ved pålogging) Ansvarlig for aktiviteten er seksjonssjef virksomhetsstyring Det må sørges for sikrere autentisering mot Studentweb. Ansvarlig for aktiviteten er seksjonssjefer virksomhetsstyring og studier forskning og formidling. Det må utarbeides/kunngjøres rutiner for håndtering av fortrolig informasjon på papirformat. Tilgjengelighet til makuleringsutstyr må forbedres. Bytte ut offline låssystem. Ansvarlig for aktiviteten er seksjonssjef for service brukerstøtte og infrastruktur.

	Konsekvensutredning (DPIA), ny skilting og gjennomgang av kameraovervåkning. Ansvarlig for aktiviteten er seksjonssjef for service brukerstøtte og infrastruktur.
Oppfølging:	Tiltakene vil bli fulgt opp ved neste gjennomgang for ledelsen.

Ressurs- og kompetansebehov

Ressurs- og kompetansebehov:
På bakgrunn av det som er gjennomgått i årets LG, må fremtidig behov for opplæring/kompetanseheving vurderes. Vurderingene bør særlig gå på de som har operative roller i sikkerhetsorganisasjonen. Ressursbehov for implementering av sterkere autentisering mot 2 tjenester som har uakseptabel risiko vil i hovedsak være interne ressurser. I begrenset grad vil det være behov for eksterne ressurser som det er inndekning for i budsjett for 2019. Det må avsettes midler til utskifting av offline låssystem.

Referat

Sikkerhetsansvarlig skriver referat fra ledelsens gjennomgang.

I referatet skal det tydelig fremgå de avgjørelser og tiltak som er besluttet. Direktør skal undertegne referatet fra ledelsens gjennomgang.