KUNSTHØGSKOLEN I OSLO
OSLO NATIONAL ACADEMY OF THE ARTS

Sikkerhetspolicy for informasjonssikkerhet

15.07.2013

Innholdsfortegnelse

1 Ledelsens formål med informasjonssikkerhet

Informasjonsteknologi og -sikkerhet er vesentlig for at Kunsthøgskolen i Oslo (KHiO) skal kunne yte tjenester for sine ansatte og studenter, og et virksomhetskritisk virkemiddel innen arbeidsprosessene i KHiO. Det stilles derfor strenge krav til at sikkerheten blir tilstrekkelig ivaretatt. Systemer og infrastruktur skal være pålitelige i bruk, samtidig som informasjon skal være korrekt og beskyttet mot uautorisert tilgang.

KHiOs medarbeidere, studenter og andre brukere skal alltid kunne motta korrekt informasjon til riktig tid. Samtidig som at alle skal være trygge på at informasjonen som trenger beskyttelse blir behandlet på korrekt måte. Dette i samsvar med personopplysningsloven og andre bestemmelser, etter metoder fra internasjonale standarder for informasjonssikkerhet (ISO17799/ 27002).

Det betyr at KHiO skal ha tiltak som sikrer at informasjon og informasjonssystemer er beskyttet mot uønskede hendelser. Som eksempel på dette nevnes systemsvikt, lagrings- og utstyrsfeil, hacker- eller virus-angrep, tyveri, strømsvikt og brann.

Dette dokumentet oppfyller kvalitetshåndbokens føringer for kvalitetsarbeidet i KHiO ift informasjonssikkerhet. Brukerne skal derfor forstå kravene i dette dokumentet, og bidra til at fornuftige sikkerhetskontroller er implementert og vedlikeholdt i henhold til KHiO sine retningslinjer og standarder. Overtredelse av denne Policy for informasjonssikkerhet og vedtatte sikkerhetskrav vil være et tillitsbrudd mellom brukeren og KHiO. Alvorlige overtredelser vil kunne medføre sanksjoner.

2 Mål, omfang og definisjoner

2.1 Mål for sikkerhetsarbeid i KHiO

Tilgjengelig og korrekt informasjon, velfungerende informasjonssystemer og sikkerhet generelt er kritisk og svært viktig for KHiO. Hovedmålet med sikkerhetsarbeidet er å sikre informasjon og informasjonssystemer mot misbruk, ødeleggelse og uberettiget innsyn, slik at informasjonsflyten skjer på en informasjonssikker måte. Policy for sikkerhet skal bidra til at KHiO opprettholder en høy tillit hos sine studenter og alle øvrige forbindelser. KHiO skal ha rutiner som bidrar til å forebygge sikkerhetsbrudd.

Konkrete mål for sikkerheten er å:

- Ivareta KHiO, studentene og andre brukeres krav til konfidensialitet, integritet og tilgjengelighet.
- Etablere kontroller for å beskytte KHiOs informasjon og informasjonssystemer mot tyveri, misbruk og andre former for skade og tap.
- Sørge for samsvar med gjeldende lover, forskrifter, retningslinjer og være tilnærmet internasjonale standarder for informasjonssikkerhet (ISO 27002 og kontrollområdene i ISO 27001).
- Etablere ansvar og eierskap for sikkerhet i virksomheten.
- Motivere ledelse, ansatte og studenter til å opprettholde kunnskap og kompetanse om sikkerhet, slik at frekvens og skadenivå av sikkerhetshendelser kan minimaliseres.
- Sikre at KHiO er i stand til å fortsette sine tjenester, også i fall større sikkerhetshendelser skulle inntreffe.
- Bidra til at personvernet ivaretas.

2.2 Omfang

Policy for sikkerhet (dette dokumentet) omhandler *informasjonssikkerhet*, *fysisk sikkerhet* og *personellsikkerhet* for hele KHiO, og gjelder for alle personer som behandler eller har tilgang til data og/eller informasjon som eies eller forvaltes av KHiO.
Policyen omfatter også alle tilganger til systemer som finnes i KHiOs nettverk. Policy for sikkerheten gjelder for all informasjon i KHiO, dette kan inkludere data og informasjon som er:

- papirbasert
- lagret i databaser
- lagret på datamaskiner
- overført på interne og offentlige nettverk
- lagret på flyttbare media som CD/DVD, Smart-telefoner, nettbrett, USB-stick, og andre lignende media
- lagret på fastmonterte media som harddisker og disksystemer

2.3 Definisjon av informasjonssikkerhet

Informasjonssikkerhet omfatter beskyttelse mot brudd på:

- konfidensialitet; sikkerhet for at kun autoriserte personer har tilgang til sensitiv informasjon, og at den ikke avsløres til uvedkommende
- integritet; sikkerhet for at informasjonen og informasjonsbehandlingen er fullstendig, nøyaktig og gyldig, og et resultat av autoriserte og kontrollerte aktiviteter
- tilgjengelighet; sikkerhet for at en tjeneste oppfyller bestemte krav til stabilitet, slik at aktuell informasjon er tilgjengelig ved behov

Informasjonssikkerhet kan ut fra dette defineres som:
Beskyttelse mot brudd på konfidensialitet, integritet og tilgjengelighet (KIT) for den informasjonen som behandles av informasjonssystemet og beskyttelse av systemene i seg selv.

3 Prinsipper

3.1 Risikostyring

Risikovurdering

3.1.1 Risikovurdering skal identifisere, kvantifisere og prioritere risiko i forhold til kriterier for risikoaversjon som er relevant for virksomheten.

3.1.2 Det skal gjennomføres overordnet risikovurdering i forhold til virksomhetens måloppnåelse, og ift IKT-systemer.

3.1.3 Risikovurderingen oppdateres en gang i året, eller når det skjer endringer i virksomheten som har betydning for sikkerheten eller i forhold til måloppnåelse. Det skal benyttes anerkjente metoder for risikovurdering.

3.1.4 KHiO skal ha en tilnærming til sikkerhet som er basert på risikovurderinger.

Håndtering av risiko

3.1.5 Håndtering av risiko skal foretas i forhold til ledelsesforankrede akseptkriterier.

3.1.6 Risikovurderinger skal godkjennes av virksomhetens ledelse

3.1.7 Ved identifisering av uakseptabel risiko, iverksettes tiltak for å redusere risiko til et akseptabelt nivå.

Relaterte prosedyrer og rammeverk: Ref rutine for risikovurdering, IKT-100.

3.2 Policy for sikkerhet

3.2.1 KHiOs ledelse (høgskoledirektør og rektor) skal sørge for at Policy for sikkerhet, retningslinjer og standarder blir benyttet og fulgt opp.

3.2.2 KHiOs ledelse skal sørge for at det tilrettelegges for alle brukere slik at de får nødvendig opplæring og materiell, slik at brukerne kan beskytte KHiOs informasjon og informasjonssystemer.

3.2.3 Sikkerhetspolicyen skal gjennomgås og oppdateres ved behov på årlig basis.

3.2.4 Alle viktige endringer mht. KHiOs aktivitet, eller andre endringer som vil påvirke dagens trusselbilde, skal føre til en revidering av Policyen og retningslinjer som angår sikkerhet.

3.2.5 Alle sikkerhetshendelser skal rapporteres internt og til myndighetene der det er lovpålagt, og følges opp med tanke på forbedring og læring.

3.3 Sikkerhetsorganisasjon

Virksomhetens sikkerhetsorganisasjon

3.3.1 Ansvaret innefor sikkerhetsområdet er som følger:

- Det overordnede sikkerhetsansvaret ligger hos høgskoledirektøren.
- Økonomisjef er sikkerhetsansvarlig (CSO) for KHiO og ufører sikkerhetsoppgavene på oppdrag fra høgskoledirektøren. Sikkerheten for IT og fysisk infrastruktur er delegert til IT-leder (Security Manager). Ansvar for personellsikkerhet er plassert hos CSO.

- HMS ansvaret ligger til høgskoledirektøren, mens det operasjonelle ansvaret er delegert til CSO. Behandlingsansvarlig de ansattes personopplysninger er CSO, som ivaretar myndighetskontakt ift Datatilsynet.
- Behandlingsansvarlig for studentregisteret er studiesjefen.
- Den ansvarlige for kvalitetsarbeidet er høgskoledirektøren, mens det operasjonelle ansvaret er delegert til studiesjefen.

3.3.2 KHiO har etablert et sikkerhetsforum

Sikkerhetsforumet skal ha følgende oppgaver:

- Gjennomgå og godkjenne retningslinjer for sikkerhet og generelle ansvarsforhold,
- overvåke vesentlige endringer i truslene mot organisasjonens informasjonsaktiva,
- gjennomgå og overvåke sikkerhetshendelser,
- godkjenne større initiativ for å styrke sikkerheten,
- Én av lederne skal være ansvarlig for alle sikkerhetsrelaterte aktiviteter (CSO).
- KHiO vil jevnlig bli revidert gjennom internkontroll og ekstern IT-revisor.

3.4 Klassifisering og kontroll

3.4.1 KHiO eier all vesentlig informasjon og informasjonsmateriell på KHIOs informasjonssystemer. Relevant utstyr skal være klassifisert og merket.

3.4.2 Vesentlig informasjon, inkludert fra tredjepart, skal klassifiseres

3.4.3 Informasjon som nevnt i pkt 3.4.2 skal klassifiseres i en av tre følgende kategorier for konfidensialitet:

Fortrolig
Informasjon av meget sensitiv art, og hvor uautorisert tilgang (også internt) kan medføre betydelig skade for enkeltpersoner, virksomheten eller disses interesser. Fortrolig informasjon er sensitiv informasjon i forhold til forretningsvirksomheten og personopplysninger. Slik informasjon skal sikres i ”Røde” områder, ref. kap 3.6

Intern
Informasjon som kan skade virksomheten eller være upassende at tredjepart får kjennskap til. Systemeier avgjør lagrings- og delingsmåte.

Åpen
Annen informasjon er åpen.

3.4.4 KHiO skal gjennomføre risikoanalyser for å kunne klassifisere informasjon ut fra virksomhetskritiskhet.

3.4.5 Det skal være utarbeidet rutine for gjennomføring av klassifisering og risikoanalyser

3.4.6 Brukere som forvalter informasjon på KHiOs vegne skal behandle denne i henhold til klassifiseringen.

3.4.7 Fortrolige dokumenter skal være tydelig merket.

For klassifisering *innen fysisk sikkerhet, se kapittel 3.6*

3.5 Personellsikkerhet

Ved ansettelse

3.5.1 Sikkerhetsansvar- og roller for relevant personell, både ansatte og innleide, skal beskrives.

3.5.2 Sjekk av bakgrunnen til alle kandidater til stillinger i KHiO skal foretas ihht relevante lover og regulative krav og forretningsmessige krav.

3.5.3 Taushetserklæring signeres av arbeidstakere, oppdragstakere eller andre som kan få kjennskap til fortrolig og/eller intern informasjon. Ref IKT 006

3.5.4 Informasjonsdisiplin-erklæring signeres i alle ansettelsesforhold og ved tredjeparts systemtilganger.

For ansatte gjelder

3.5.5 Informasjonsdisiplin-erklæring referer til KHiOs krav til informasjonssikkerhet, og den ansattes ansvar for å oppfylle disse. Ref IKT-005

3.5.6 Datadisiplinerklæringen skal gjennomgås med ansatte jevnlig (f eks ved medarbeidersamtale).

3.5.7 Alle ansatte og tredjeparts brukere skal få tilstrekkelig opplæring og oppdatering i Policy for informasjonssikkerhet og relevante retningslinjer og prosedyrer. Det vil være varierende grad av krav til opplæring.

3.5.8 Brudd på Policy for informasjonssikkerhet og -retningslinjer vil normalt medføre sanksjoner. Sanksjonene vil variere avhengig av overtredelsens art, vedkommendes aktsomhet og vil følge de retningslinjer som er utarbeidet. Ref IKT-003

3.5.9 KHiOs informasjon, informasjonssystemer og andre verdier (f eks telefon), skal kun benyttes til de formål de er bestemt for. Nødvendig privat bruk tillates etter avtale med nærmeste leder.

3.5.10 Bruk av virksomhetens IKT-infrastruktur i egen næringsvirksomhet er ikke tillatt.

Avslutning eller endring av ansettelse

3.5.11 Ansvar for terminering eller endring av ansettelsesforhold skal være klart definert i egen rutine med relevant rundeskjema.

3.5.12 KHiO eier all IKT-utstyr som skolen har gitt til ansatte/studenter og disse skal leveres inn ved opphør av behov for bruk.

3.5.13 Tilgangsrettigheter termineres ved bortfall av behov for systemtilgang.

Ref Personalrutine/ IKT 320

3.6 Fysisk og miljømessig sikkerhet

Sikkerhetsområder

3.6.1 Sikre 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	Alt er i utgangspunktet tilgjengelig. Studentområder og kantine.	Må passere skranke for en overordnet validering.
Gul	Noen tekniske rom, slik som printerrom, rom hvor det eksempelvis i arbeidstiden vil forefinnes skjermverdig / intern informasjon. Kontorlokaler, møterom, noen arkiver.	Utskrift skal benyttes med ”Follow me”-funksjonalitet der det skrives ut fortrolig informasjon.
Rød	Avgrensede områder hvor spesiell autorisasjon kreves, datarom/serverom/arkiver og koplingsrom med fortrolig informasjon og lignende.	Adgangskort og relevant nivå av nøkkelsikkerhet.

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

3.6.2 Systemeier er ansvarlig for godkjenning av medarbeidere med adgang til sikre områder.

3.6.3 Alle virksomhetens lokaler skal sikres med tilstrekkelige sikringssystemer iht klassifisering, ref. tabell ovenfor, inkl. relevant sporbarhet/logging. (kjør ROS, der et tiltak, slik som overvåkning, etc. settes iht risikobildet).

3.6.4 Sikkerhetsansvarlig sikrer at arbeid utført av tredjepart i sikre områder er relevant overvåket.

3.6.5 Ansatte og studenter skal kunne tilkjennegi sin identitet og bære personlige adgangskort når de er i virksomheten. ID kortene er personlige, og må ikke overdras til tredjepart eller kolleger.

3.6.6 Røde områder skal være forsvarlig sikret mot miljøskader forårsaket av brann, vann, eksplosjon, vibrasjoner mv.

3.6.7 Alle skall-dører og vinduer skal låses og stenges ved arbeidsdagens slutt. Vaktselskap kontrollerer og sikrer eiendommene etter arbeidstidens slutt.

3.6.8 Besøkende innenfor rød sone skal skje sammen med autorisert personell.

3.6.9 Adgangskort kan gis til håndverkere, teknikere og andre mot verifikasjon.

Sikring av utstyr

3.6.10 IKT-utstyr klassifisert som ”Høy” skal plasseres eller beskyttes slik at det reduserer risikoen for miljømessige trusler (brann, oversvømmelse, temperatursvingninger, fukt etc.).

3.6.11 Tilgang til informasjon klassifisert som ”Fortrolig” på bærbare maskiner skal passordbeskyttes.

3.6.12 Bærbart utstyr skal håndteres som håndbagasje under reiser.

3.6.13 Utstyr kan kun tilkoples, flyttes eller tas ut av lokalene etter godkjenning fra IT-avdelingen

3.6.14 Områder klassifisert som ”Rød” skal sikres med relevant branslukkingsutstyr med relevant varsling. Det skal jevnlig gjennomføres brannøvelser

3.6.15 IT–systemer utstyres med relevant kjøling.

3.6.16 Forretningskritiske systemer (klassifisert som HØY) beskyttes med nødstrømsaggregat med kapasitet til minst 4 timers uavbrutt drift (settes gjennom ROS analyse).

3.7 Kommunikasjon og driftsadministrasjon

Operasjonelle prosedyrer og ansvarsområder

3.7.1 Installasjon av IT-utstyr inklusive programvare skal godkjennes av IT-avdelingen før installasjon.

3.7.2 IT avdelingen sikrer dokumentasjon av systemer etter virksomhetens standard.

3.7.3 Endringer gjennomføres kun når det er forretnings- og sikkerhetsmessig velbegrunnet.

3.7.4 IT avdelingen har ansvaret for at det foreligger en nødprosedyre for å minimalisere effekten av feilslåtte endringer.

3.7.5 Dokumentasjon av driftsprosedyrer skal utføres etter vesentlig endring. Driftsprosedyrer er dokumentert i egne prosedyrer (ref Dokumentoversikten).

3.7.6 Før produksjon skal det planlegges for å forhindre at feil oppstår, i tillegg til å ha rutiner for overvåking og håndtering av uforutsette problemer.

3.7.7 Oppgaver og ansvar skal separeres på en slik måte at det reduserer muligheter for uautorisert- eller uforusett misbruk av virksomhetens verdier.

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

Systemplanlegging og aksept/godkjenning

3.7.9 Det tas hensyn til IT-sikkerhetskrav når nye IT-systemer designes, testes, implementeres og oppgraderes, samt ved systemendringer. Det utarbeides rutine for endringshåndtering og systemutvikling/vedlikehold

3.7.10 IT-systemenes dimensjonering avpasses etter kapasitetskrav. Belastning overvåkes slik at oppgradering og tilpasning kan finne sted løpende. Dette gjelder særlig for virksomhetskritiske systemer.

Beskyttelse mot skadelig kode

3.7.11 Datautstyr sikres mot virus og annen ondsinnet og/eller skadelig kode. IT-ansvarlig sørger for sikringen.

Sikkerhetskopiering

3.7.12 IT-avdelingen er ansvarlig for regelmessig sikkerhetskopiering og testing og oppbevaring av alle data på virksomhetens IT-systemer.

3.7.13 Studentene er selv ansvarlig for å ta backup av egne data.

3.7.14 Sikkerhetskopier oppbevares eksternt eller i egen relevant sikret brannsone.

Nettverksstyring

3.7.15 IT-avdelingen har det overordnede ansvaret for å beskytte virksomhetens nettverk.

3.7.16 *Det føres oversikt over alt IKT-utstyr som kobles opp i KHiO nettverk (ikke for studentnettet), samt mobile enheter.*

Håndtering av datamedier

3.7.17 Håndtering av flyttbare datamedia (som taper, USB-stick, disketter og utskrifter) sikres iht klassifikasjon. Det påhviler den enkelte ansatt at dette gjennomføres.

3.7.18 Media avhendes på sikker måte ved kassasjon mv. (Ref IKT 117)

Utveksling av informasjon

3.7.19 Det etableres prosedyrer og kontroller for å beskytte utveksling av informasjon med tredjepart eller forflytting av informasjon.

3.7.20 Ekstern serviceleverandør underlegges retningslinjene.

Bruk av kryptografiske teknikker

3.7.21 Lagring og overføring av fortrolige opplysninger (ref. Klassemodell i kap 3.4.3) krypteres eller beskyttes på annen måte.

Elektroniske forretningsytelser

3.7.22 Informasjon involvert i elektronisk handel over offentlige nettverk beskyttes mot svindel, kontraktsmessige uoverensstemmelser, uautorisert adgang og endringer.

3.7.23 Informasjonsavdelingen har ansvar for at offentlig tilgjengelig informasjon, f eks på virksomhetens Web-tjenester, er tilstrekkelig beskyttet mot uautoriserte tilganger.

Overvåkning av systemtilgang og bruk

3.7.24 Tilgang og bruk av systemer logges og overvåkes for å kunne identifisere potensielt misbruk.

3.7.25 Bruk og beslutninger skal være sporbare til en spesifikk entitet (f eks person eller enkeltsystem).

3.7.26 IT avdelingen med samarbeidspartnere registrerer vesentlige forstyrrelser og uregelmessigheter i driften av systemene, samt mulig årsak til feil.

3.7.27 IT-systemer og nettverk overvåkes i tilstrekkelig grad ift kapasitet, oppetid og kvalitet for pålitelig drift og tilgjengelighet.

3.7.28 IT avdelingen med samarbeidspartnere logger sikkerhetshendelser i alle vesentlige systemer

3.7.29 IT avdelingen med samarbeidspartnere sikrer at systemenes klokker jevnlig synkroniseres til korrekt tid.

3.7.30 IT-avdelingen skal igangsette nødvendig tiltak for å redusere risikoen for hærverk/tveri av relevant IT-utstyr

3.8 Tilgangskontroll

Forretningsmessige krav

3.8.1 Det skal finnes en skriftlig tilgangs- og passordpolitikk som er basert på forretnings- og sikkerhetsmessige krav og behov. Tilgangspolitikken revideres regelmessig.

3.8.2 Tilgangspolitikken inneholder retningslinjer for endringsfrekvens, passordregler (minimumslengde, type karakterer som kan/skal benyttes mv) og hvor passordet kan lagres.

Brukeradministrering- og ansvar

3.8.3 System og systemaksess autentiseres minimum ved hjelp av personlige brukeridenter og passord.

3.8.4 Brukere skal ha unike kombinasjoner av brukeridenter og passord.

3.8.5 Brukere er ansvarlige for enhver bruk av brukeridenter og passord. Brukere holder brukeridenter og passord konfidensielle, og røper bare disse hvis det er spesifikt autorisert av Security Manager. (Ref IKT-103)

Tilgangskontroll/Autorisasjon

3.8.6 Tilgang til informasjonssystemer skal være autorisert av nærmeste leder og tilgangsrettigheter, inkludert tilhørende aksessrettigheter (privilegier) som lagres i ”aksesslister”. Autorisasjoner gis på bakgrunn av ”Need to know”-prinsippet, og reguleres av type rolle/stilling.

Aksesslister beskriver roller og ansvar med tilhørende tilgangsrettigheter med basis i følgende klassifisering.

KHiO har følgende roller/klasser:

- Intern (styret, ledere, administrativtansatte, fagligansatte)
- Ekstern (samarbeidsparterne, gjestelærere, teknikere ol.)
- Studenter
- Publikum

Kontroll med nettverkstilgang

3.8.7 IT avdelingen har ansvaret for at brukernes nettverkstilgang skjer i overensstemmelse med retningslinjene for tilgang (Ref IKT-103)

3.8.8 Brukere skal kun ha tilgang til de tjenester de er autorisert for.

Mobilt utstyr og fjernarbeidsplasser

3.8.9 Arbeid utenfor KHiOs lokaler på KHiOs utstyr er tillatt dersom sikkerherhetspolicy og datadisiplinerklæring underskrives og overholdes.

3.8.10 Mobile enheter sikres med tilstrekkelige sikkerhetsmekanismer.

3.8.11 Fjerntilgang til virksomhetens nettverk skal kun skje gjennom sikkerhetsløsninger godkjent av IT-avdelingen, (ref IKT-113)

3.8.12 Fortrolig informasjon krypteres når det oppbevares på bærbare medier, slik som USB-stick, smarttelefoner, CDer, DVDer eller minnekort ol.

3.8.13 Tilgang til privilegerte kontoer og fortrolige områder skal begrenses.

3.8.14 Brukere skal hindres i å tilegne seg informasjon de ikke skal ha tilgang til.

3.9 Systemutvikling og vedlikehold

Sikkerhetskrav til informasjonssystemer

3.9.1 Definisjon av forretningsmessige krav til nye systemer eller videreutvikling av systemer skal inneholde sikkerhetsmessige krav.

Kryptografiske kontroller

3.9.2 Retningslinjer for administrasjon og bruk av kryptografiske kontroller for beskyttelse av informasjon, skal utvikles og implementeres.

Sikkerhet i systemfiler

3.9.3 Endringer i produksjonsmiljø skal følge gjeldende rutiner.

3.9.4 Implementering av endringer skal kontrolleres - gjennom bruk av formelle prosedyrer for endringskontroll - for å minimalisere mulighetene for skade på informasjon eller informasjonssystemer.

Sikkerhet i utvikling og vedlikehold

3.9.5 De systemer som utvikles og/ tilpasses for ev av KHiO, skal ha klare krav til sikkerhet, inkludert validering av data, sikring av koden før produksjonssetting, og eventuell bruk av kryptografi. Endringer i produksjonsmiljø skal følge gjeldende rutiner, (ref relevante driftsrutiner)

3.9.6 Programvare gjennomtestes og aksepteres formelt av eier/brukere og driftsansvarlig før programvaren overføres til produksjonsmiljøet.

Risikovurdering

3.9.7 Før ny programvare (klassifisert som Høy), eller større endringer av ditto systemer settes i produksjon, gjennomføres en sårbarhets- og risikovurdering. IKT-100

3.10 Hendelseshåndtering

Ansvar for rapportering

3.10.1 Leder og medarbeider er ansvarlig for å rapportere brudd og mulige brudd på sikkerheten. Rapporteringen går linjevei, eventuelt direkte til CSO.

Måling

3.10.2 Det skal være mulig å definere kostnader ved sikkerhetshendelser. CSO er ansvarlig for dette.

3.10.3 Det utarbeides rutiner for avvikshåndtering og rapportering. Rutinen skal inneholde krav til tiltak for å forhindre gjentagelser samt skadereduksjon.

Bevissikring

3.10.4 Security Manager skal være kjent med enkle rutiner for bevissikring ved mistanke til sikkerhetshendelser

3.11 Kontinuitetsplanlegging

Kontinuitetsplan

3.11.1 Det skal utarbeides kontinuitetsplan som dekker kritiske/viktige informasjonssystemer og infrastruktur.

3.11.2 Kontinuitetsplaner utarbeides på bakgrunn av risiko og sårbarhetsanalyser som tar utgangspunkt i forretningsrisiko.

3.11.3 Planen(ene) avstemmes med KHiOs øvrige beredskap og katastrofeplanverk.

3.11.4 Kontinuitetsplanen testes periodisk for å sikre at den er dekkende, og sikre at ledelse og ansatte forstår gjennomføringen.

3.11.5 Produksjonssystemer og andre systemer klassifisert som ”Høy”, skal ha reserveløsninger.

3.12 Samsvar

Samsvar med juridiske krav

3.12.1 KHiO følger gjeldende lovverk, samt andre eksterne retningslinjer slik som:

- Lov om Arbeidervern og arbeidsmiljø og forskrifter til denne
- Lov om Helse, Miljø og Sikkerhet
- Lov om personopplysninger m.m.
- Datatilsynets krav
- Tjenestemannsloven
- Regnskapsloven
- Lov om universiteter og høyskoler
- Offentlighetsloven

Andre eksterne referanser

- Kommuneveilederen

3.12.2 Ansatte er pålagt å forholde seg i overensstemmelse med Policy for informasjonssikkerhet og retningslinjer. Oppfølging av at dette er linjeledelsens ansvar

3.12.3 Ansatte skal være klare over at bevis fra sikkerhetshendelser tas vare på (lagres) og overleveres

Kontroll og revisjon

3.12.4 Revisjonskrav og revisjonshandlinger planlegges og avtales med de involverte for å minimere risikoen for forstyrrelser av virksomhetens forretningsaktiviteter.

3.12.5 De personene som utfører revisjonen, skal være uavhengige av det reviderte området.

4 Roller og ansvarsområder

4.1 Roller og ansvarsområder

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

Høgskoledirektøren har det overordnede ansvar for sikkerheten i virksomheten.

Sikkerhetspolitikk - Eier

4.1.1 *Høgskoledirektøren er sikkerhetspolitikkens (dette dokumentet) eier. Høgskoledirektøren delegerer sikkerhetspolitisk dokumentasjon og signaturrettigheter til sikkerhetsansvarlig (CSO). Alle endringer i dokumentet skal dokumenteres og signeres av sikkerhetsansvarlig.*

Sikkerhetsansvarlig

4.1.2 Sikkerhetsansvarlig (CSO, Chief Security Officer) er hovedansvarlig for Informasjonssikkerhet i virksomheten. Økonomisjefen har denne rollen (ref pkt 3.3.1).

Systemansvarlige

4.1.3 Systemansvarlige er ansvarlig for spesifikke områder av IT i virksomheten. Systemansvarlige er personer som forvalter virksomhetens informasjonssystemer eller informasjon som er betrodd virksomheten fra andre parter. Hver enkelt type informasjon og systemer kan ha en eller flere dedikerte systemansvarlige. Disse er ansvarlige for å beskytte informasjonen, inklusive å implementere aksesskontrollmekanismer for å sikre konfidensialitet, og å foreta backup slik at kritisk informasjon ikke går tapt. De implementerer, drifter og vedlikeholder dessuten sikkerhetsmekanismer i tråd med intensjonen.

Avdelingsledere

4.1.4 Avdelingsledere er ansvarlige for krav til anskaffelse, utvikling og vedlikehold av informasjon og relaterte informasjonssystemer, i samråd med IT avdelingen. Alle typer informasjon skal ha en definert eier. For hver type informasjon skal eierne klassifisere informasjonen, definere hvilke brukere (brukergrupper) som skal ha tilgang til denne, og definere hva som er autorisert bruk av informasjonen.

Konsulenter og kontraktspartnere

4.1.5 Skal skrive under taushetserklæring ved innsyn i fortrolige forhold.

Brukere

4.1.6 Med brukere forstås ansatte, deltidsengasjerte, timelærere, studenter og andre som gis tilgang til skolens interne datasystemer og lokaler. Brukere er ansvarlige for å gjøre seg kjent med, og rette seg etter virksomhetens politikk, prosedyrer og standarder innenfor informasjonssikkerhet. Spørsmål om håndtering av forskjellig type informasjon skal stilles til den aktuelle informasjonens eier, eventuelt systemansvarlig.

5 Styrende dokumenter for sikkerhetsarbeidet

5.1 Formål med styrende dokumenter

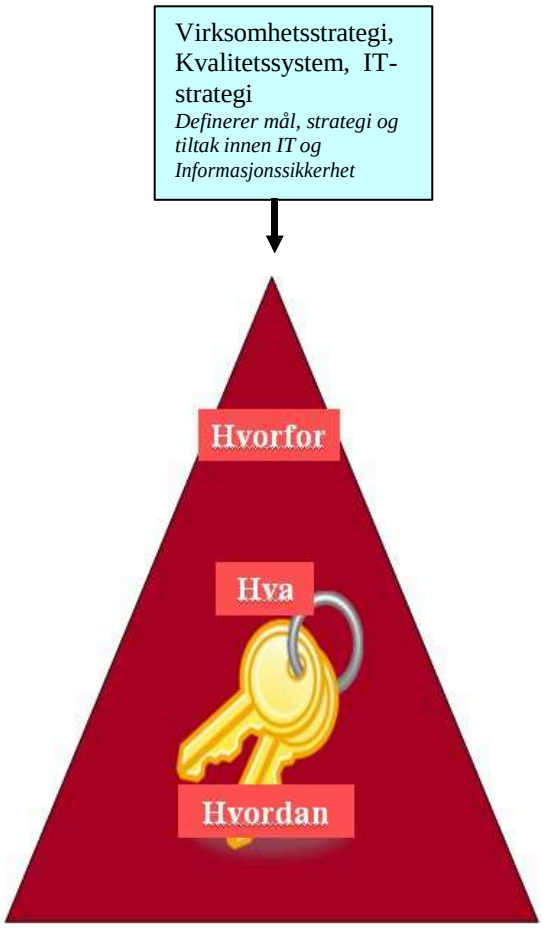
Styrende dokumenter for Informasjonssikkerhet skal bidra til å oppnå et balansert nivå på tiltak i forhold til den risiko og de rammebetingelser KHiO står overfor.

Det skal eksistere dokumenterte krav og retningslinjer knyttet til informasjonssikkerhet basert på oppdaterte risikoanalyser. De øvrige systemer og infrastruktur skal være dekket av gode basiskontroller innen informasjonssikkerhet som til en hver tid skal etterleves.

5.2 Dokumentstruktur

5.2.1 KHiO har organisert dokumentstrukturen for beskrivelse av sin sikkerhetsarkitektur i 3 nivåer

Den etablerte struktur for styrende dokumenter for IT-sikkerhetsarbeidet er som følger:



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.

Overordnede retningslinjer/Prinsipper for Informasjonssikkerhet. Her defineres ***hva*** som må gjøres for å etterleve den etablerte policy.

Standarder og prosedyrer for Informasjonssikkerhet med detaljerte retningslinjer for ***hvordan*** disse standardene skal implementeres. Dette bør etter hvert etableres for alle sentrale plattformer

6 Referanser

6.1 Eksterne referanser

Referanser

6.1.1 *NS-ISO/IEC 17799 Informasjonsteknologi – Administrasjon av informasjonssikkerhet (ISO/IEC 17799:2005*

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

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

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

6.1.5 *Kryptering: http://www.datatilsynet.no/templates/article___889.aspx*

6.1.6 *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

6.1.7 *Arkivloven : http://www.lovdata.no/all/nl-19921204-126.html*

6.1.8 *Åndsverkssloven : http://www.lovdata.no/all/nl-19610512-002.html*

6.1.9 *Regnskapsloven : http://www.lovdata.no/all/nl-19980717-056.html*

6.1.10 *OECDs retningslinjer - for sikkerhet i informasjonssystemer og nettverk - Mot en sikkerhetskultur. Nærings og Handelsdepartementet: http://odin.dep.no/archive/nhdbilder/01/06/OECDr072.pdf*

6.1.11 *Tjenestemannsloven : http://www.lovdata.no/all/nl-19830304-003.html*

6.1.12 Lov om Universiteter og høyskoler

6.2 Interne referanser

Referanser

6.2.1 *Virksomhetsstrategien*

6.2.2 *Kvalitetshåndboken*

6.2.3 Katastrofe/beredskapsplan

6.2.4 *IT strategi*

6.2.5 Kontinuitetsplan IT

6.2.6 *ROS-analyser (fil-server/safe)*

6.2.7 *Personalhåndbok (inkl HMS føringer)*

6.2.8 *IT driftshåndbok (alle driftsrutinene) (fil-server/safe)*