Sikkerhetspolicy
for

Versjonskontroll

Versjon	Dato	Endringsbeskrivelse
0.7	25.04.2008	Initiell versjon
0.8	29.05.2008	Etter WS
0.9	12.09.2008	Til møte i Sikkerhetsgruppen ved HVO 12.09.08
1.0	14.10.2008	Ut til høring
1.1	04.12.2008	Godkjent av høgskulestyret
1.2	01.11.2013	Revisjon
1.3	14.01.2014	Revisjon
1.4	04.12.2014	Revisjon, godkjent informasjons-sikkerhetsgruppe

Forfatter og distribusjon

Forfatter	Dato	Rolle
Kenneth Høstland, Uninett Gigacampus	25.04.2008	Ekstern Konsulent
Sikkerhetsgruppa ved HVO	12.09.2008	
Distribusjonsliste		**Rolle**
Jacob Kjøde jr.		Høgskuledirektør
Nina C. Garshol		Personaldirektør
Stig Flåskjer		IT-sjef
Leif Roar Strand		Driftssjef
Peder Magne Sefland		Over.ing. nettverk

Innholdsfortegnelse

1 Ledelsens formål med sikkerhet

Informasjonsteknologi og sikkerhet er vesentlig for at Høgskulen i Volda (HVO) skal kunne yte tjenester for sine ansatte og studenter, og et virksomhetskritisk virkemiddel innen arbeidsprosessene i HVO. 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.

HVOs 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 i samsvar med personopplysningsloven og andre bestemmelser, etter metoder fra internasjonale standarder for informasjonssikkerhet (ISO17799:2005/ 27002).

Dette betyr at HVO skal ha tiltak som sikrer at informasjon og informasjonssystemer er beskyttet mot uønskede hendelser. Som eksempel på dette nevnes menneskelige feil, feil på utstyr, hacker- eller virusangrep, tyveri, strømsvikt og brann.

Sikkerhetspolicy (SP) – dette dokumentet – oppfyller kvalitetshåndbokens føringer for kvalitetsarbeidet i HVO ifht. informasjonssikkerhet. Overtredelse av SP og vedtatte sikkerhetskrav vil være et tillitsbrudd mellom ansatte og HVO. Ved alvorlige overtredelser vil ansettelsesforholdet bli vurdert.

……..
Høgskuledirektør Jacob Kjøde jr.
for Høgskulen i Volda

2 Mål, omfang og definisjoner

2.1 Mål for sikkerhetsarbeid i HVO

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

Konkrete mål for sikkerheten:

- Å ivareta HVO, studentenes og andre brukeres krav til konfidensialitet, integritet og tilgjengelighet
- Å etablere kontroller for å beskytte HVOs informasjon og informasjonssystemer mot tyveri, misbruk og andre former for skade og tap.
- Å sørge for samsvar med gjeldende lover, forskrifter, retningslinjer og være tilnærmet internasjonale standarder for informasjonssikkerhet (ISO 27002 og kontrollområdene i ISO 27001)
- Å etablere ansvar og eierskap for sikkerhet i virksomheten.
- Å motivere ledelse, ansatte og studenter til å opprettholde kunnskap og kompetanse om sikkerhet, slik at frekvens og skadenivå av sikkerhetshendelser kan minimaliseres.
- Å sikre at HVO er i stand til å fortsette sine tjenester, også i fall større sikkerhetshendelser skulle inntreffe.
- Å bidra til at personvernet ivaretas

2.2 Omfang

SP omhandler informasjonssikkerhet, fysisk sikkerhet og personellsikkerhet for hele HVO, og gjelder for alle personer som behandler eller har tilgang til data og/eller informasjon som eies eller forvaltes av HVO.
SP omfatter også alle tilganger til systemer som finnes i HVOs nettverk. SP gjelder for all informasjon i HVO, 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-rom, Nettbrett/smarttelefoner, USB-minnepinne, 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.

3 Prinsipper

3.1 Risikostyring

Risikovurdering

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

3.1.2 Det skal gjennomføres overordnet risikovurdering i forhold til virksomhetens måloppnåelse, og i forhold til IT-system.

3.1.3 Risikovurderingen skal 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 ved bruk av eksterne konsulenter

3.1.4 HVO 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, skal det iverksettes tiltak for å redusere risiko til et akseptabelt nivå.

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

3.2 Sikkerhetspolicy

3.2.1 HVOs ledelse (Høgskuledirektør og rektor) skal sørge for at sikkerhetspolicy (SP) – dette dokumentet, retningslinjer og standarder blir benyttet og fulgt opp.

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

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

3.2.4 Alle viktige endringer mht. HVOs aktivitet, eller andre endringer som vil påvirke dagens trusselbilde, skal føre til en revidering av SP 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 *Det overordnede sikkerhetsansvaret ligger hos administrerende direktør.* Personaldirektør er sikkerhetsansvarlig (CSO) for HVO og ufører sikkerhetsoppgavene på oppdrag fra høgskuledirektøren. IT-sikkerhetsansvaret er delegert til IT-sjef. Ansvaret for personalsikkerhet er direkte plassert hos CSO. Sikkerhet er et ansvar som påhviler virksomhetens administrative ledelse.

- HMS-ansvarlig er høgskuledirektør, som har delegert HMS-oppgavene til ledere med personalansvar.

- Behandlingsansvarlig for personopplysninger er høgskuledirektøren.
- Daglig behandlingsansvarlig for de ansattes personopplysninger er personaldirektør, som ivaretar myndighetskontakt ift Datatilsynet.
- Daglig behandlingsansvarlig for studentregisteret er studiedirektør.
- Den ansvarlige for kvalitetsarbeidet er Høgskulestyret, som har delegert koordinatoroppgavene til studiedirektøren.
- Driftssjef er ansvarlig for den fysiske sikkerheten, herunder også fysisk tilgangskontroll.

3.3.2 HVO har opprettet en overordnet HMS-gruppe som består av

- Personaldirektør
- Studiedirektør
- Hovedvernombud
- HMS-rådgiver (sekretær)
- Rep. fra dekan-gruppen
- Informasjonsleder

HMS-gruppen har møte minst 2 ganger pr. semester, eller oftere når det kreves.
Personaldirektør kaller inn til møtene. Referat blir lagt i egen sak i Public360 der bare medlemmer i gruppen har lese-tilgang.

HMS-gruppen skal sørge for revidering av beredskapsplan, gjennomføring av øvelse. Etablere og forankre rutiner for systematisk arbeid med ROS-analyse, og være pådriver for systematisk HMS-arbeid i organisasjonen.

3.3.3 HVO har etablert en IT-sikkerhetsgruppe som består av

- Høgskuledirektør
- Personaldirektør (CSO)
- IT-sjef
- HMS-koordinator / Hovedvernombud
- Driftssjef
- IT-nettverksansvarlig
- Rep. Statsbygg (ved behov)

IT-sikkerhetsgruppen har møte minst en gang pr semester eller oftere når det er påkrevet.
Nettverksansvarlig kaller inn IT-sikkerhetsgruppen. Referat blir lagt i egen sak i Public360 der bare medlemmer i gruppen har lese-tilgang.

IT-sikkerhetsgruppen sitt arbeid er primært informasjonssikkerhet. Dette omfatter IT-system med tilhørende infrastruktur.
Gruppen skal fremme operasjonell sikkerhet i organisasjonen gjennom nødvendig engasjement og tilstrekkelig ressursbruk. Beslutninger samstemmes/koordineres med den faglige ledelse (rektor) i ledermøte.

IT-sikkerhetsgruppen skal ha følgende oppgaver:

- Gjennomgang og godkjenning av retningslinjer for sikkerhet og generelle ansvarsforhold;
- Overvåkning av vesentlige endringer i truslene mot organisasjonens informasjonsaktiva;
- Gjennomgang og overvåkning av sikkerhetshendelser;
- Godkjenning av større initiativ for å styrke sikkerheten.

3.4 Klassifisering og kontroll

3.4.1 All HVOs vesentlige informasjon og eiendeler skal ha en eier. Alt relevant utstyr skal være klassifisert og merket.

3.4.2 All vesentlig informasjon, inkludert informasjon som mottas fra tredjepart skal klassifiseres.

3.4.3

3.4.4 All vesentlig informasjon, inkludert informasjon som mottas fra tredjepart skal klassifiseres i en av følgende kategorier for konfidensialitet:

- **Unntatt offentlighet**
  Informasjon av meget sensitiv art, og hvor uautorisert tilgang (også innenfor virksomheten) kan medføre betydelig skade for enkeltpersoner, virksomheten eller dennes interesser. Fortrolig informasjon er Personopplysninger og sensitiv informasjon i forhold til forretningsvirksomheten. Slik informasjon skal sikres i "Røde" områder, ref. kap 3.x
- **Intern**
  Informasjon som kan skade virksomheten eller være upassende at tredjepart får kjennskap til. Systemeier avgjør lagrings- og delingsmåte.
- **Offentlig**
  All annen informasjon er åpen. Kun offentlig informasjon kan lagres i skytjenester. Jmf IKT-188 - Retningslinjer for bruk av skytjenester

3.4.5 HVO skal gjennomføre risikoanalyser for å kunne klassifisere informasjon ut fra hvor virksomhetskritisk den er.

3.4.6 Brukere som forvalter informasjon på HVOs vegne, skal behandle denne i henhold til klassifiseringen. Opplæring vil bli gitt.

3.4.7 Output fra systemer der informasjonens klassifikasjonsnivå er fortrolig, skal merkes med konfidensialitetsnivå og eierskap.

For klassifisering *innen fysisk sikkerhet, se kapittel 3.6*

3.5 Personellsikkerhet

Før ansettelse gjelder følgende:

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

3.5.2 Sjekk av bakgrunnen til alle som blir ansatt i stillinger ved HVO skal foretas iht. relevante lover og regulativer, samt forretningsmessige krav.

3.5.3 Taushetserklæringer skal signeres av alle ansatte, vikarer, innleide eller andre som kan få kjennskap til informasjon i HVO som har behov for beskyttelse, ref. IKT-006 (for eksterne)

3.5.4 IT reglement skal benyttes og signeres i alle ansettelsesforhold og ved tredjeparts systemtilganger, ref. «IKT-005 IT Reglement».

I ansettesforholdet gjelder følgende:

3.5.5 IT-reglementet referer til HVOs krav til informasjonssikkerhet, og den ansatte har ansvar for å gjøre seg kjent med og oppfylle disse.

3.5.6 Alle ansatte og tredjepartsbrukere skal få tilstrekkelig opplæring og oppdatering i SP og relevante retningslinjer og prosedyrer. Det vil være varierende grad av krav til opplæring.

3.5.7 Brudd på SP og sikkerhetsretningslinjer vil normalt medføre sanksjoner overfor den ansatte. Sanksjonene vil variere avhengig av overtredelsens art og vedkommendes aktsomhet, og vil følge de retningslinjer som er utarbeidet for dette, ref. «IKT-003 Retningslinjer for Disiplinær reaksjoner».

3.5.8 HVOs informasjon, informasjonssystemer og andre verdier som f.eks. telefoni, skal kun benyttes til de formål de er bestemt for. Nødvendig privat bruk tillates.

3.5.9 Bruk av virksomhetens IT-infrastruktur i egen næringsvirksomhet er under ingen omstendigheter tillatt.

Avslutning eller endring av ansettelse

3.5.10 Ansvar for terminering eller endring av ansettelsesforhold skal være klart definert.

3.5.11 Alle ansatte og innleid personell skal levere inn alle HVOs eierandeler i deres besittelse ved opphør av ansettelse eller arbeidskontrakt.

3.5.12 Tilgangsrettighetene til ansatte og innleide skal termineres ved avslutting av arbeidskontrakt. Tilgang til e-post kan forlenges etter særskilt avtale mellom leder og IT-kontoret. Avtalen legges i personalmappe.

3.6 Fysisk og miljømessig sikkerhet

Sikkerhetsområder

3.6.1 HVO skal benytte sikre soner 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.	Utanfor åpningstid, regulert med adgangskontroll-systemet.
Gul	Noen tekniske rom, f.eks. koblingsrom, printerrom, rom hvor det eksempelvis i arbeidstiden vil forefinnes skjermverdig/intern informasjon. Kontorlokaler, møterom, noen arkiver.	Utskrifter skal foretas vha. ”Follow me”-funksjonaltet.
Rød	Avgrensede områder hvor spesiell autorisasjon kreves, datarom/-serverom/arkiver med fortrolig informasjon og lignende.	Adgangskort.

Områdene skal avmerkes i bygningsplansjer.

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 ut fra tabellen i pkt. 3.6.1, inkl. relevant sporbarhet/logging. (kjør ROS, der et tiltak iverksettes iht. risikobildet).

3.6.4 Sikkerhetsansvarlig for fysisk sikkerhet (Driftssjef) skal sikre at arbeide i sikre områder overvåkes.

3.6.5 Rød sone skal være forsvarlig sikret mot miljøskader forårsaket av brann, vann, støv og tilsvarende påvirkning.

3.6.6 Alle medarbeidere er ansvarlig for at dører og vinduer med adgang til/fra bygninger skal lukkes og låses ved arbeidsdagens slutt. Vaktselskap skal benyttes for å følge opp denne retningslinjen.

3.6.7 Besøkende som skal ha tilgang til rød sone må registreres i resepsjonen, og de skal bære synlige gjestekort når de ferdes i virksomheten og utskrives når de forlater området.

3.6.8 Adgangskort kan gis til håndverkere, teknikere og andre mot at det leveres ID kort og fullstendig utfylt skjema «IKT-006 Ansvars og taushetserklæring konsulent.ekstern»

Sikring av utstyr

3.6.9 IT-utstyr klassifisert som «Høy» skal plasseres eller beskyttes slik at det reduserer risikoen for miljømessige trusler (brann, oversvømmelse, temperatursvingninger, fukt etc.).

3.6.10 Tilgang til informasjon klassifisert som «Fortrolig» på bærbare maskiner skal passordbeskyttes og krypteres

3.6.11 Bærbart utstyr skal håndteres som håndbagasje under reiser.

3.6.12 Utstyr kan kun fjernes fra virksomheten ved behov og etter godkjenning fra overordnede.

3.6.13 Områder klassifisert som «Rød» skal sikres med relevant brannslukningsutstyr med relevant varsling. Det skal jevnlig gjennomføres brannøvelser. Lokaler som rommer en betydelig mengde IT systemer, skal sikres med relevant kjøling.

3.6.14 Alle forretningskritiske systemer (klassifisert som HØY) skal beskyttes med nød-strøm for kontrollert nedkjøring av systemene.

3.7 Kommunikasjon og driftsadministrasjon

Operasjonelle prosedyrer og ansvarsområder

3.7.1 All installasjon av IT-utstyr inklusive programvare på HVOs IT-systemer skal testes og godkjennes av IT-kontoret før installasjon.

3.7.2 IT-kontoret skal sikre at alle systemer er dokumentert etter virksomhetens standard.

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

3.7.4 IT-kontoret skal sikre at det foreligger en nødprosedyre for å minimalisere effekten av feilslåtte endringer.

3.7.5 Dokumentasjon av driftsprosedyrer skal utføres etter enhver vesentlig endring.

3.7.6 I produksjon skal man planlegge 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 muligheten for uautorisert eller uforutsett misbruk av virksomhetens verdier.

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

Ekstern serviceleverandør

3.7.9 Virksomheten skal regelmessig overvåke serviceleverandørene, gjennomgå de avtalte rapporter og logginger, samt utføre revisjoner for å sikre at avtalene overholdes og sikkerhetshendelser og problemer håndteres betryggende.
(dette gjelder USIT, UNINETT FAS, SSØ oa)

Systemplanlegging og aksept/godkjenning

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

3.7.11 IT-systemenes skal dimensjoneres etter kapasitetskrav. Belastning skal overvåkes slik at oppgradering og tilpasning kan finne sted løpende. Dette gjelder særlig for virksomhetskritiske systemer.

Beskyttelse mot skadelig kode

3.7.12 Datautstyr skal sikres mot virus og annen ondsinnet og skadelig kode. IT-sjef må sørge for at slik sikring er tilgjengelig for brukere, og at den er implementert på standard infrastruktur.

Sikkerhetskopiering

3.7.13 IT-kontoret skal sørge for at det tas sikkerhetskopi og at testing av denne skjer regelmessig, samt oppbevaring av alle forretningskritiske data på virksomhetens IT-systemer.

3.7.14 Sikkerhetskopier skal oppbevares på 2 lokasjoner.

Nettverksstyring

3.7.15 IT-kontoret skal sikre virksomhetens nettverk

3.7.16 Det skal føres oversikt over alt IT-utstyr som kobles opp i HVOs nettverk (ikke for studentnettet), samt mobile enheter.

Håndtering av datamedier

3.7.17 Håndtering av flyttbare datamedia (som USB-minnepinne, CD-/DVD-er, eksterne harddisker o.l.) i de ansattes utstyr skal sikres iht. klassifikasjon. Det påhviler den enkelte ansatte at dette gjennomføres.

3.7.18 Media skal avhendes på sikker måte når det ikke er behov for disse lenger.

Utveksling av informasjon

3.7.19 Det skal være etablert prosedyrer og kontroller for å beskytte all type av utveksling av informasjon med tredjepart eller forflytting av informasjon utenfor virksomheten, ref. data- og taushetserklæringene.

3.7.20 Ekstern serviceleverandør skal underlegges HVOs retningslinjer for utveksling av informasjon.

Bruk av kryptografiske teknikker

3.7.21 Lagring og overføring av fortrolige opplysninger (ref. kategorier for konfidensialitet i pkt. 3.4.3) skal krypteres eller beskyttes på annen måte.

Elektroniske forretningsytelser

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

3.7.23 IT-kontoret skal sikre at offentlig tilgjengelig informasjon, for eksempel på virksomhetens web-tjenester, er tilstrekkelig beskyttet mot uautoriserte tilganger.

Overvåkning av systemtilgang og bruk

3.7.24 Tilgang og bruk av systemer klassifisert som «Høy» skal logges og overvåkes for å kunne identifisere potensielt misbruk av systemer eller informasjon.

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

3.7.26 IT-kontoret med samarbeidspartner(-e) skal registrere vesentlige forstyrrelser og uregelmessigheter i driften av systemene, samt mulige årsaker til feil.

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

3.7.28 IT-kontoret med samarbeidspartner(-e) skal logge sikkerhetshendelser på alle virksomhetens vesentlige systemer.

3.7.29 IT-kontoret med samarbeidspartner(-e) skal sikre at systemenes klokker jevnlig synkroniseres til korrekt tid.

3.8 Tilgangskontroll

Forretningsmessige krav

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

3.8.2 Tilgangspolicyen skal inneholde retningslinjer for endringsfrekvens, passordregler (minimumslengde, type karakterer som kan/skal benyttes etc.) og hvor passordet kan lagres.

Brukeradministrering- og ansvar

3.8.3 All system og systemaksess skal – som et minimum – autentiseres ved hjelp av personlige brukeridentiteter og passord.

3.8.4 Alle brukere skal ha unike brukeridentiteter og passord.

3.8.5 Brukere er ansvarlige for enhver bruk av personlige brukeridentiteter og passord. Brukere skal holde brukeridentiteter og passord konfidensielle, og ikke røpe disse hvis ikke dette spesifikt autoriseres av sikkerhetsansvarlig.

Tilgangskontroll/Autorisasjon

3.8.6 Tilgang til alle informasjonssystemer skal være autorisert av nærmeste leder og tilgangsrettigheter, inkludert tilhørende aksessrettigheter (privilegier), skal lagres i «aksesslister». Autorisasjoner gis på bakgrunn av «need-to-know»-prinsippet, og reguleres av hvilken stilling den enkelte har eller hvilken rolle vedkommende har.
Aksesslister skal beskrive roller & ansvar med tilhørende tilgangsrettigheter med basis i følgende klassifisering.

HVO har følgende roller/klasser:

- Ansatte
- Studenter
- Publikum
- Samarbeidspartnere
- Kunder

Kontroll med nettverkstilgang

3.8.7 IT-kontoret har ansvaret for at brukernes nettverkstilgang skjer i overensstemmelse med retningslinjene for tilgang.

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

Mobilt utstyr og fjernarbeidsplasser

3.8.9 Hjemmekontor er tillatt dersom SP og IT-reglement er underskrevet og overholdt.

3.8.10 Mobile enheter skal sikres med tilstrekkelige sikkerhetsmekanismer mot fiendtlig kode ol.

3.8.11 Fjerntilgang til virksomhetens nettverk skal kun skje gjennom sikkerhetsløsninger godkjent av IT avdelingen.

3.8.12 Fortrolig informasjon skal krypteres når det oppbevares eller transporteres på bærbare medier, slik som USB-minnepinne, Nettbrett, Mobiltelefoner, CD-er, DVD-er e.l.

3.8.13 Tilgang til privilegerte kontoer og fortrolige områder skal begrenses.

3.8.14 Brukere skal ikke forsøke 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.

Korrekt virkemåte i applikasjoner

3.9.2 Data input til og output fra applikasjoner skal valideres for å sikre at disse data er korrekte og relevante.

3.9.3 Påliteligheten og integriteten til meldinger skal defineres og relevante tiltak implementeres.

Kryptografiske kontroller

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

Sikkerhet i systemfiler

3.9.5 Alle endringer i produksjonsmiljø skal følge gjeldende rutiner.

3.9.6 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

3.9.7 HVO driver ikke selv med egenutvikling av systemer, men de systemer som utvikles for HVO, skal ha klare krav til sikkerhet, inkludert validering av data, sikring av koden før produksjonssetting, og eventuell bruk av

kryptografi.

3.9.8 All programvare skal være gjennomtestet og formelt akseptert av eier/brukere og driftsansvarlig før programvaren overføres til produksjonsmiljøet

Risikovurdering

3.9.9 Før ny programvare klassifisert som Høy, eller større endringer i slike systemer settes i produksjon skal det gjennomføres en sårbarhets- og risikovurdering. IKT-100

3.10 Hendelseshåndtering

Ansvar for rapportering

3.10.1 Enhver leder og medarbeider er ansvarlig for å rapportere brudd og mulige brudd på IT-reglement og/eller sikkerhetspolicy. Rapporteringen går linjevei, eventuelt direkte til Sikkerhetssjef (CSO).

Måling

3.10.2 Det skal være mulig å definere kostnader ved sikkerhetshendelser. Sikkerhetssjef er ansvarlig for at dette blir gjort ved behov.

3.10.3 Det er utarbeidet rutiner for avvikshåndtering og rapportering.

Bevissikring

3.10.4 Alle ansatte skal være kjent med hvem som skal kontaktes ved mistanke om sikkerhetshendelser. IT-kontoret bør vurdere hva som skal gjøres.

3.11 Kontinuitetsplanlegging

Kontinuitetsplan

3.11.1 Det skal være utarbeidet kontinuitetsplan som dekker alle viktige og kritiske informasjonssystemer og infrastruktur.

3.11.2 Kontinuitetsplan(er) skal være utarbeidet på bakgrunn av risiko og sårbarhetsanalyser som tar utgangspunkt i forretningsrisiko.

3.11.3 Planen(ene) skal være avstemt med HVOs øvrige beredskap og planverk.

3.11.4 Kontinuitetsplanen skal testes periodisk for å sikre at den er dekkende, og sikre at ledelse og ansatte forstår hvordan denne skal gjennomføres.

3.11.5 Produksjonssystemer og andre systemer klassifisert som "Høy", skal ha reserveløsninger. Tabellen settes etter at ROS /BIA er gjennomført.

Verdi	Tilgjengelighet	Beskrivelse
3 - Høy	<8 time	Systemet kan være utilgjengelig opp til 8 timer
2, Med	24 timer	Systemet kan være utilgjengelig opp til ett døgn
1 - Lav	3 dager	Systemet kan være utilgjengelig opp til 3 dager

3.12 Samsvar

Samsvar med juridiske krav

3.12.1 HVO skal følge 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 og veiledere
- Tjenestemannsloven
- Regnskapsloven
- Lov om universiteter og høyskoler
- Offentlighetsloven
- E-signaturloven

Andre eksterne referanser

- Kommuneveilederen
- HTA,
- SPH

Samsvar med sikkerhetspolicy

3.12.2 Alle ansatte er pålagt å forholde seg i overensstemmelse med SP og sikkerhetsretningslinjer. Oppfølging av dette er linje ledelsens ansvar.

3.12.3 Alle ansatte skal være klar over at bevis fra sikkerhetshendelser skal tas vare på (lagres) og kan overleveres myndighetene

Kontroll og revisjon

3.12.4 Revisjonskrav og revisjonshandlinger skal 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.

Høgskuledirektør har det overordnede ansvar for sikkerheten i virksomheten.

Sikkerhetspolitikk - Eier

4.1.1 Høgskuledirektør er sikkerhetspolitikkens (dette dokumentet) eier.
Høgskuledirektør delegerer sikkerhetspolitikk 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 personaldirektør, og hovedansvarlig for informasjonssikkerhet i virksomheten.

Systemeier

4.1.3 Systemeiere er ansvarlig for spesifikke områder av IT i virksomheten.
Systemeiere er personer som forvalter virksomhetens informasjonssystemer eller informasjon som er betrodd virksomheten fra andre parter. Hver enkelt type informasjon og systemer skal ha en eller flere dedikerte eiere. Disse er ansvarlige for å beskytte informasjonen, dette inkluderer å implementere aksesskontrollmekanismer for å sikre konfidensialitet, og å foreta backup slik at kritisk informasjon ikke går tapt. De skal også implementere, drifte og vedlikeholde sikkerhetsmekanismer som definert av avdelingsledere og CSO.

Avdelingsledere

4.1.4 Avdelingsledere er systemansvarlige og er ansvarlige for krav til anskaffelse, utvikling og vedlikehold av informasjon og relaterte informasjonssystemer, i samråd med IT.
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 Ansatte er ansvarlige for å gjøre seg kjent med, og rette seg etter virksomhetens sikkerhetspolitikk (dette dokumentet), Taushetserklæring og ”Datadisiplinerklæringen”. Spørsmål om håndtering av forskjellig type informasjon skal stilles til den aktuelle informasjonens eier, eventuelt systemansvarlige.

Studenter

4.1.7 Studenter 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 driftsansvarlig. Gjestestudenter har de samme plikter og ansvar som ordinære studenter

Publikum

4.1.8 Publikum er slike som inviteres til konserter og lignende, og har ikke noe sikkerhetsansvar utover det som er definert under tilgang til gjestenett/trådløst nett ol.

Samarbeidspartnere

4.1.9 Samarbeidspartnere 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 driftsansvarlig.

Kunder

4.1.10 Kunder 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 driftsansvarlig.

5 Styrende dokumenter for sikkerhetsarbeidet

5.1 Formål med styrende dokumenter

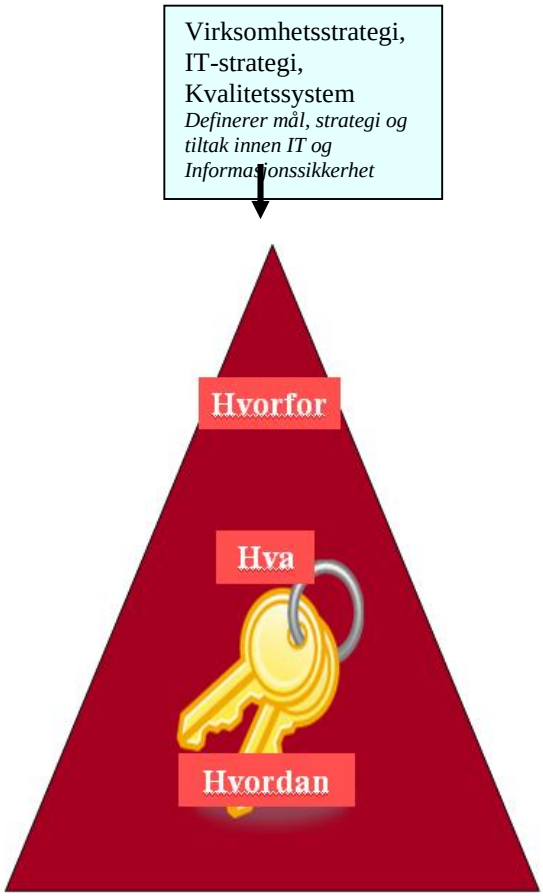
Styrende dokumenter for informasjonssikkerhet skal bidra til å oppnå et balansert nivå på tiltak i forhold til den risiko og de rammebetingelser HVO står ovenfor.

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 enhver tid skal etterleves.

5.2 Dokumentstruktur

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

Den etablerte struktur for styrende dokumenter for 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

Referanser

5.3 Eksterne referanser

Referanser

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

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

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

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

5.3.5 *Kryptering: http://www.datatilsynet.no/templates/article____889.aspx*

5.3.6 *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

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

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

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

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

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

5.3.12 Lov om Universiteter og høyskoler

5.3.13 Esignaturloven

5.4 Interne referanser

Referanser

5.4.1 *Virksomhetsstrategien planer*

5.4.2 *HMS-håndbok*