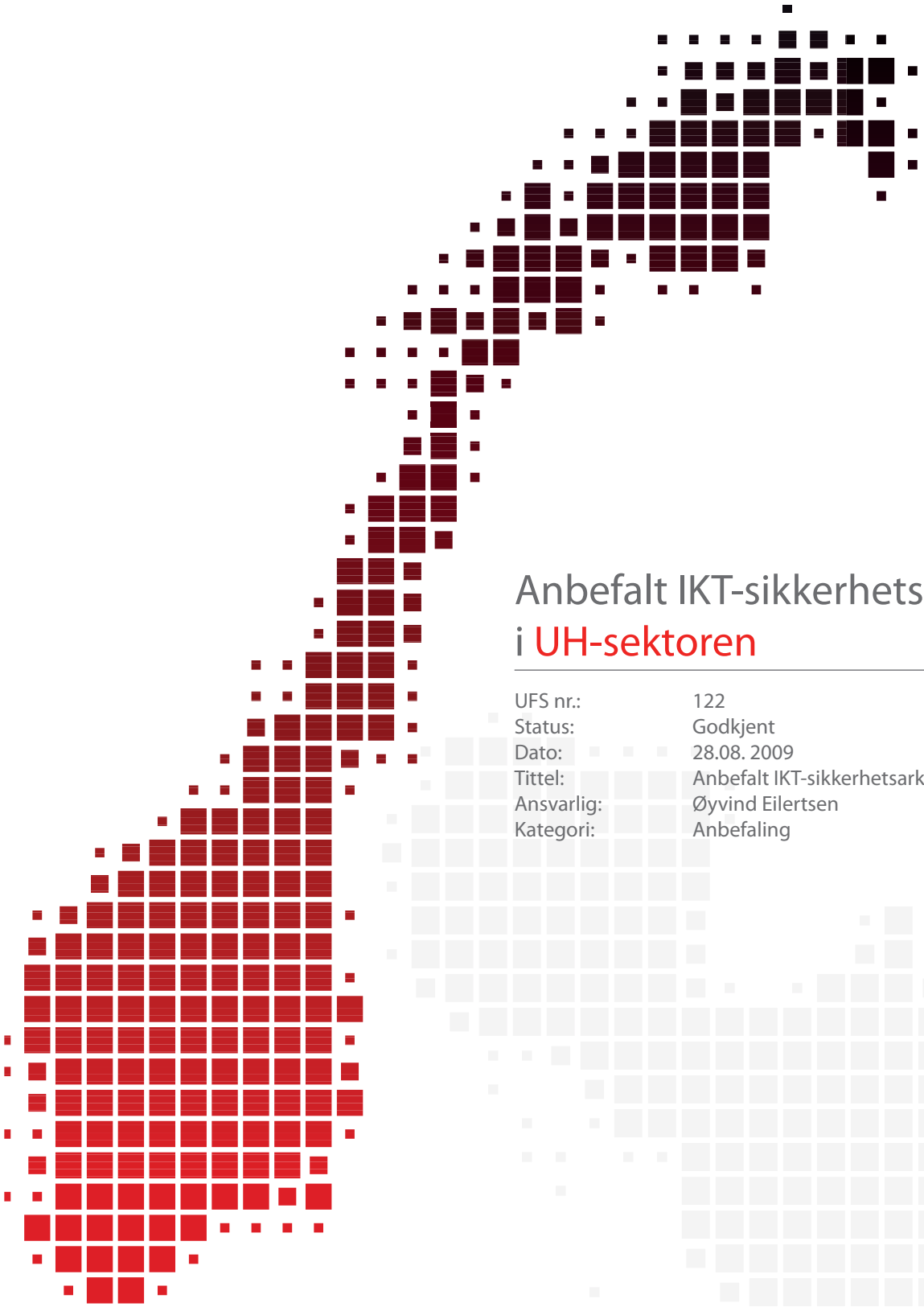
UNINETT Fagspesifikasjon



Anbefalt IKT-sikkerhetsarkitektur i UH-sektoren

UFS nr.:	122
Status:	Godkjent
Dato:	28.08. 2009
Tittel:	Anbefalt IKT-sikkerhetsarkitektur i UH-sektoren
Ansvarlig:	Øyvind Eilertsen
Kategori:	Anbefaling

Sammendrag

Dette dokumentet har til hensikt å være en veileder for hvordan IKT-sikkerhetsarkitekturen i universitets- og høgskolesektoren i Norge bør realiseres. Anbefalingene baserer seg på «beste praksis», risikovurderinger, regulative og forretningsmessige krav, Datatilsynets veiledere, samt langt på vei eksisterende praksis.

Målgruppen for dokumentet er IKT-ledere og nettverksansvarlige ved UH-institusjoner.

Innhold

Endringslogg

Versjon	Dato	Kapittel	Endring	Ansvarlig	Godkjent
0.1	2008-04-03		Initell versjon	VF, KH	
0.2	2008-04-24	Alle	Justert	VF, KH	
0.3	2008-06-16	Alle	Justert og lagt til nye kapitler	KH	
0.4	2008-08-12	Alle	Omstrukturering etter workshop 2008-06-26	Prosjekt-gruppen	
0.41	2008-08-22	Alle	Justering av innhold	VF	
0.43	2008-10-23	Alle		GB/ØE	
0.6	2008-11-24	Alle	Oppdatering etter møte 2008-10-31	TL/GB/ØE	
0.7	2008-12-05	Alle	Oppdatering etter møte 2008-11-27	KH/PAE/VF/ GB/TL/ØE	
0.8	2009-02-25	Alle	Oppdatert etter møte 2009-01-06. Intern høring UNINETT AS	ØE	
0.9	2009-05-07	Alle	Oppdatert etter intern høring. Til høring i sektoren	GB/PAE/RS/ TL/ØE	
1.0	2009-08-28	Alle	Oppdatert etter høring i sektoren	GB//RS/TL/ ØE	
1.02	2009-12-03	Alle	Rettet opp trykkfeil	ØE	

Prosjektgruppen har hatt følgende deltakere:
Gunnar Bø, Per-Arne Enstad, Øyvind Eilertsen, Vidar Faltinsen, Morten Knudsen, Torgrim Lauritsen, Rune Sydskjør (alle UNINETT) og Kenneth Høstland (Conferit AS).

1 Formål

Formålet med dette dokumentet er å definere en overordnet arkitektur som kan legge til rette for at virksomhetene i UH-sektoren kan beskytte sin informasjon og sine informasjonssystemer på en formålstjenlig måte. Viktige elementer innen informasjonssikkerhet er

- **Konfidensialitet** (informasjon er bare tilgjengelig for de som skal ha tilgang).
- **Integritet** (informasjon er korrekt og fullstendig).
- **Tilgjengelighet** (informasjon er tilgjengelig innenfor de krav som er satt).

Det er en forutsetning at virksomheten har etablert en informasjonssikkerhetspolicy som spesifiserer overordnede sikkerhetsmål, valg og prioriteringer.

2 Overordnede krav

IKT-sikkerhetsarkitekturen for UH-sektoren skal tilfredsstille følgende overordnede krav:

- Den enkelte institusjon må beskytte sin informasjon i tilstrekkelig grad. Sikkerhets- og risikonivåer skal være *forankret i ledelsen* og basert på vurderinger av *risiko og sårbarhet (ROS-vurderinger)*.
- De tekniske løsningene skal oppfylle institusjonens *policy for informasjonssikkerhet*.
- Det skal tas hensyn til relevante regulative krav og veiledere, slik som personopplysningsloven (1) med forskrift (2), samt Datatilsynets *Veiledning i informasjonssikkerhet for kommuner og fylker («Kommuneveilederen»)* (3).
- Sikkerhetsarkitekturen skal understøtte institusjonens formål og målsetninger, slik som fastlagt i universitetsloven, og institusjonens forhold til tredjeparter.
- De tekniske løsningene skal ha tilstrekkelig kapasitet og motstandsdyktighet mot feilsituasjoner (redundans).
- De tekniske løsningene skal ha tilstrekkelig høy kvalitet.

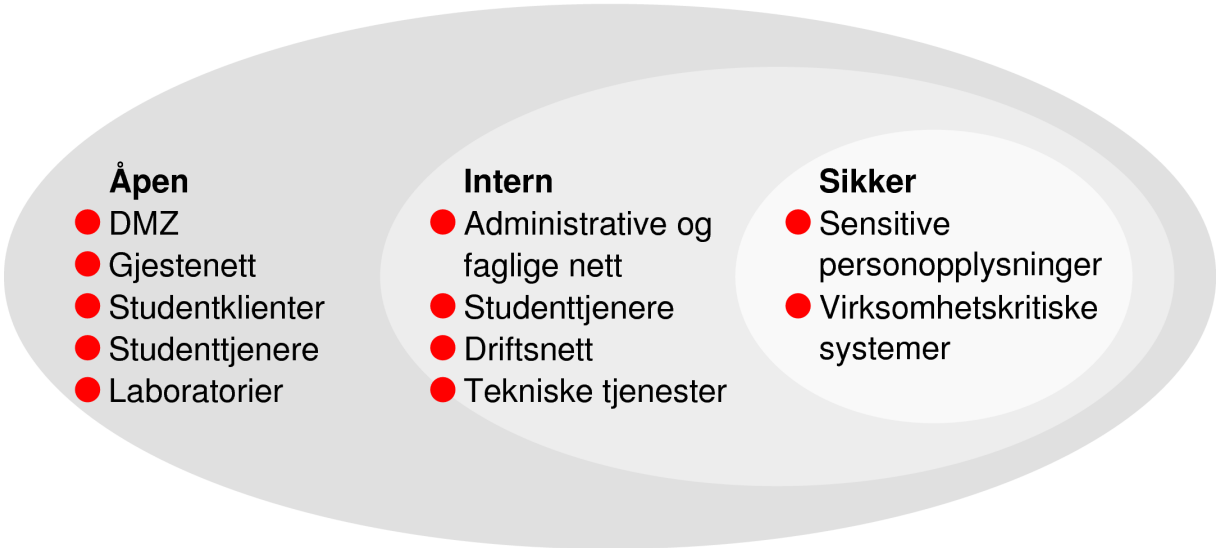
3 Sikkerhetsarkitekturen

Sikkerhetsarkitekturen er basert på følgende prinsipper:

- Nettet skal deles inn i *soner* og *sikkerhetsklasser*.
- Det skal finnes et klart skille mellom *tjenere* og *klienter*.
- Tjenere og klienter skal plasseres i relevante sikkerhetsklasser basert på risiko- og sårbarhetsvurderinger (ROS-vurderinger).
- Tilgangen til tjenestene skal reguleres gjennom bruk av *sikkerhetsbarrierer.*
- Virtuelle tjenere og klienter skal behandles etter de samme prinsipper som andre enheter.

3.1 Inndeling i soner, sikkerhetsklasser og segmenter

- Inndeling i soner og klasser skal være basert på *ROS-vurderinger*.
- *Systemeier* er ansvarlig for klassifisering og plassering av systemet.
- Inndeling i *soner* skal benyttes som et prinsipp for sikkerhetsarkitekturen. En sone definerer et minimums sikkerhetsnivå. Det skal i utgangspunktet benyttes tre soner: *Åpen* sone, *Intern* sone og *Sikker* sone. En institusjon kan velge å implementere flere soner dersom det er hensiktsmessig ifølge ROS-vurderingen.
- En sone har i utgangspunktet ikke tilgang til en sone med høyere sikkerhetsnivå med mindre det er eksplisitt tillatt.
- En sone med høyere sikkerhetsnivå har ikke nødvendigvis tilgang til en sone med lavere sikkerhetsnivå.
- Hver sone vil inneholde ett eller flere *nettverkssegmenter*, jf. Figur 1.
- Nettverkssegmenter innenfor en og samme sone kan ha forskjellige krav til sikkerhet. Segmenter innenfor en sone som har felles krav til sikkerhet kan grupperes i en *sikkerhetsklasse*.
- Nettverkssegmenter i samme sone eller sikkerhetsklasse er ikke nødvendigvis fullt tilgjengelige for hverandre.



Figur 1: Eksempel på inndeling i soner og nettverkssegmenter

3.2 Sikkerhetsbarrierer

En *sikkerhetsbarriere* er en samling av premisser som må tilfredsstilles for å få tilgang til ressurser i en gitt sone eller sikkerhetsklasse. Sikkerhetsbarrieren kan bestå av ett eller flere av følgende elementer (listen er ikke uttømmende):

- brannmur/brannmurfunksjonalitet i ruter
- pakkefilter

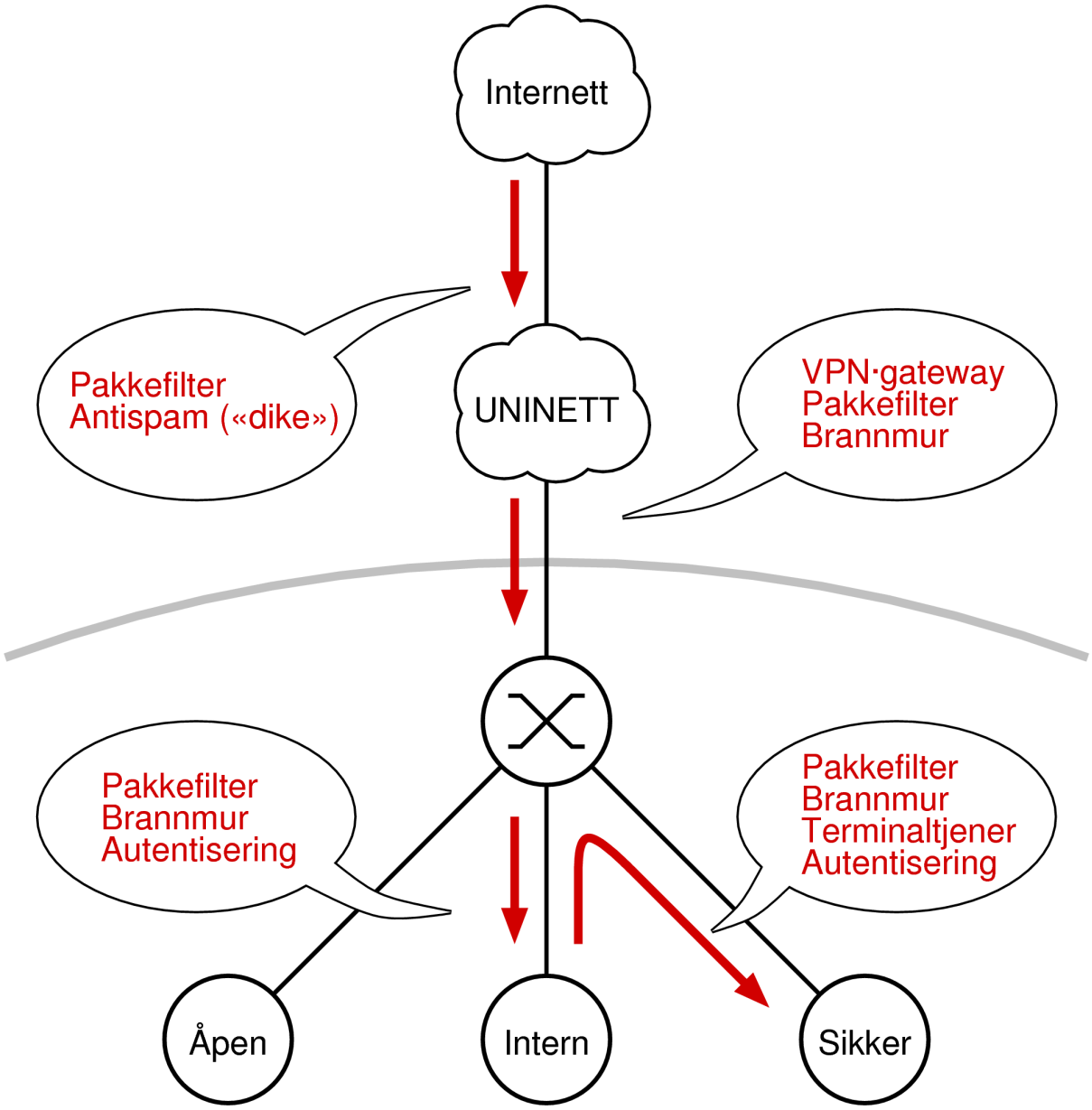
- applikasjonsportnere, slik som proxyer og terminaltjenere
- autentiseringsløsninger
- VPN-løsninger/SSL-gateway
- krav til klienter
- krav til tjenere

I tillegg kommer ansvarliggjøring av brukere ved hjelp av administrative tiltak, herunder policy, prosedyrer og lignende.

3.3 Anvendelse av sonene

Følgende anvendelse av sonene anbefales:

Sikker sone	Kritiske systemer, dvs. systemer som håndterer sensitive personopplysninger iht. personopplysningslovens § 2.8 og/eller virksomhetskritisk informasjon
Intern sone	Virksomhetsinterne nettverkssegmenter som brukes av ansatte og andre som er tilknyttet institusjonen. Virksomhetsinterne segmenter skal ikke kunne nås direkte fra maskiner utenfor institusjonen.
Åpen sone	Alt annet, for eksempel studentsoner, gjestenett, DMZ og private maskiner.



Figur 2: Implementasjon av soner og sikkerhetsbarrierer

3.4 Krav til dedikerte tjenere

Åpen sone:
Krav om god systemadministrasjon, slik som patching og stopp av unødvendige tjenester. For tjenester lokalisert i demilitarisert sone (DMZ) er det ytterligere krav til tjenere, slik som herding og sentral logging. Sentral logging anbefales generelt for alle dedikerte tjenere.

Intern sone:
Samme som åpen sone.

Sikker sone:
I tillegg til samme krav som intern sone skal ytterligere tiltak vurderes, slik som integritetssjekk, innbruddsdeteksjon, kryptering av trafikk, herding og sentral logging.

3.5 Krav til klienter

I alle soner skal klienter skilles fra dedikerte tjenere, dvs. at klienter og tjenere skal befinne seg i forskjellige nettverkssegmenter.

Åpen sone:
Institusjonen avgjør hvilke krav som skal stilles til klienter.

Intern sone:
- Klienter skal være sentralt administrert, dvs. at bare systemansvarlige har administratorrettigheter, ikke vanlige brukere.
- Klienter skal følge institusjonens standarder for operativsystem.
- Klientbeskyttelse, slik som antivirusprogramvare mv., skal ha nyeste revisjonsnivå.
- Ingen private klienter, dvs. klienter som ikke eies eller disponeres av institusjonen, skal være lokalisert i intern sone.

Sikker sone:
- Ingen klienter skal være lokalisert i sikker sone.
- Klienter som skal ha tilgang til tjenester i sikker sone kan bare komme fra intern sone. Disse skal dermed være administrerte klienter, ha siste revisjonsnivå av klientbeskyttelse og ikke være private klienter.
- Fjerntilgang må som minimum tilfredsstille Datatilsynets krav slik de er formulert i «Kommuneveilederen» (3).

4 Autentisering og tilgangskontroll

Med *tilgangskontroll* forstås en sikkerhetsbarriere en klient må passere for å få tilgang til ressurser i en spesifikk sone og sikkerhetsklasse.
Som overordnete prinsipper gjelder følgende:
- Tilgang skal gis bare etter behov
- Det skal foreligge tilstrekkelige mekanismer for logging og sporbarhet.

For behandling av personopplysninger er logging med historikk på minimum 3 måneder et krav i henhold til personopplysningsforskriften § 2-16. Det samme gjelder andre hendelser med betydning for IKT-sikkerheten.

Åpen sone:
- På trådløst nett skal tilgangskontrollen i utgangspunktet implementeres ved bruk av eduroam.
- Det må finnes en særskilt ordning for gjester som ikke inngår i eduroam-samarbeidet.
- Eduroam med tilhørende gjesteløsning eller tilsvarende sikker autentisering skal også benyttes i trådbasert åpen sone, for eksempel i auditorier og på møterom.

Intern sone:

- Alt utstyr som kobles på nett skal autentiseres, f.eks. ved bruk av 802.1X.
- Alle brukere skal i utgangspunktet autentiseres mot en sentral brukerdatabase.
- Systemer som ikke støtter sentral autentisering må beskyttes spesielt.

Sikker sone:

- Brukere som skal til sikker sone fra intern sone, må re-autentiseres/utfordres på nytt gjennom en applikasjonsportner.
- Dersom fjerntilgang, slik som fra hjemmekontor, til sikker sone skal være tillatt, skal minst kravene i «Veiledning i informasjonssikkerhet for kommuner og fylker», kapittel 18, være oppfylt.

5 Tjenestene og systemene i det sonedelte nettet

Systemeier for en gitt tjeneste har ansvaret for å avgjøre hvilken sone tjenesten skal plasseres i og hvilken beskyttelse den skal ha. For eksempel er det ikke IT-avdelingens oppgave å bestemme om et system skal plasseres i sikker sone. Systemeier og IT-avdeling må samarbeide om å definere plassering og beskyttelse.

5.1 Åpen sone

Åpen sone inneholder tjenester som skal eksponeres mot verden, bl.a. nettverkssegmentene DMZ (demilitarisert sone), gjestenett og laboratorier, samt studentenes nettverkssegmenter. Følgende inndeling anbefales for de enkelte segmentene i åpen sone:

5.1.1 DMZ

DMZ (demilitarisert sone) er et nettverkssegment som benyttes til å isolere tjenester som er eksponert mot omverdenen, og som trenger spesiell beskyttelse. DMZ kan bl.a. Inneholde følgende tjenester:

- Eksterne websider, portal o.l.
- Inngående e-postmottak fra eksterne nett
- webmailtjener
- ekstern navnetjener (DNS; også kalt *autoritativ* eller *publiserende* navnetjener)
- VPN-tjeneste for ansatte.

5.1.2 Gjestenett

Gjestenett er et nettverkssegment i institusjonen som er ment for gjester, for eksempel kunder, leverandører og ansatte ved andre undervisningsinstitusjoner. Institusjonens egne ansatte kan også benytte gjestenettet for enkel tilgang til Internet. Av hensyn til sporbarhet bør det være et krav at alle brukere på gjestenettet er autentisert.
I forhold til institusjonens øvrige nettverk og soner er gjestenettet å betrakte som Internet.

Institusjonen kan velge å tilby trådløst eller trådbundet gjestenett, for eksempel i møterom eller auditorier. Brukere som ønsker tilknytning må akseptere institusjonens vilkår for bruk. Institusjonen avgjør om det i tillegg skal stilles bestemte krav til klientutstyret som benyttes.

5.1.3 Studenttjenester

Dette nettverkssegmentet inneholder tjenester som institusjonen tilbyr til studentene for bruk i studiene. Eksempler på slike tjenester er:

- Interne e-posttjenester for studenter
- filtjener(e) for hjemme- og webområder for studenter
- skrivertjenere.

5.1.4 Laboratorier

Alt relevant laboratorieutstyr, såfremt dette *ikke* inneholder personopplysninger eller andre virksomhetskritiske systemer eller informasjon.

5.1.5 Studenteide klienter

Dette segmentet inneholder klienter for brukere som er registrert som studenter på institusjonen. Disse klientene har typisk tilgang til segmentet som inneholder studentsystemer.

5.2 Intern sone

Intern sone inneholder bl.a. segmentene fagnett, tekniske tjenester, administrative systemer og driftsnett, samt klienter som kan aksessere tjenestene i sikker sone. Dersom institusjonen tillater fjerntilgang til intern sone, må det i tillegg finnes utstyr som håndterer og administrerer slik tilgang.

Virksomhetsinterne tjenester som *ikke* inneholder sensitive personopplysninger hører hjemme i denne sonen. Et forslag til plassering i nettsegmenter for noen relevante tjenester følger under. Listen er ikke uttømmende.

5.2.1 Basistjenester

Systemadministrative tjenester, bl.a.

- systemtjenester som DHCP, NTP, SIP og rekursiv DNS
- brukerdatabaser, domenekontrollere (AD)
- studenttjenester
- interne e-posttjenester
- filtjener for hjemmeområder for ansatte
- institusjonens interne websider
- kalendersystem
- klientadministrasjonssystemer som SMS, SUS, antivirus og lisenser
- skrivertjenere

5.2.2 Tekniske tjenester

Tjenester som teknisk drift på institusjonen er avhengig av, bl.a.

- Sentral driftskontroll (SD-anlegg), bygningsstyring
- Styringssystem for AV-utstyr
- Utstyr for videoovervåkning

5.2.3 Administrative systemer

Terminalserverløsning for tilgang til tjenester i sikker sone og systemer som hovedsakelig benyttes av studieadministrasjonen, bl.a.

- Arkiv- og sakssystemer
- studieadministrative systemer
- administrative tjenere som ikke blir plassert i sikker sone, f.eks. økonomisystem. ROS-vurderinger avgjør om slike tjenere skal plasseres i intern eller sikker sone.
- Timeregistreringsverktøy

5.2.4 Driftsnett

Dette segmentet inneholder overvåkningstjenere for nettverk og tjenester samt nettelektronikk, for eksempel svitsjer og basestasjoner.

5.3 Sikker sone

Alle tjenester og systemer som inneholder sensitive personopplysninger og alle virksomhetskritiske systemer plasseres i sikker sone.

5.3.1 Sensitive personopplysninger

Alle tjenester og systemer som inneholder sensitive personopplysninger i henhold til personopplysningslovens § 2-8, slik som

- ulike pasientjournalsystemer
- administrative systemer som inneholder sensitive personopplysninger
- opptak fra videoovervåkningsutstyr.

5.3.2 Virksomhetskritiske systemer

Alle tjenester som er virksomhetskritiske eller inneholder virksomhetskritiske opplysninger, slik som

- låsesystemer
- tilgangskontroll
- forskningsmateriale/oppdragsforskning
- sikkerhetskopiering
- annen informasjon med betydning for informasjonssikkerheten, etter ROS-vurdering.

6 Definisjoner og referanser

6.1 Definisjoner

Systemeier
Den person i institutsjonen som har det overordnede ansvar for at systemet blir brukt i henhold til gjeldende avtaler, lover og regler. Systemeier er ansvarlig for å definere og regulere tilgang til data i systemet og er ansvarlig for at virksomheten har tilstrekkelig brukerstøtte, rutinebeskrivelser og kontrollrutiner for bruken av systemet.

Personopplysninger
Opplysninger og vurderinger som kan knyttes til en person.

Sensitive personopplysninger
Opplysninger om

- rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,
- at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
- helseforhold,
- seksuelle forhold,
- medlemskap i fagforeninger.

6.2 Referanser

(1) *Lov om personopplysninger (personopplysningsloven).* http://www.lovdata.no/all/hl-20000414-031.html

(2) *Forskrift om behandling av personopplysninger (personopplysningsforskriften).* http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20001215-1265.html

(3) Datatilsynet: *Veiledning i informasjonssikkerhet for kommuner og fylker («Kommuneveilederen»).* http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/tv202_2005_1.pdf

(4) *ISO/IEC 27001:2005 Information security – Security techniques – Information security management systems – Requirements.*

(5) *ISO/IEC 27002:2005 Information security – Security techniques – Code of practice for information security management.*

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

(7) Datatilsynet: *Risikovurdering av informasjonssystem.* http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/Risikovurdering_TV-506_02.pdf

(8) Senter for statlig økonomistyring: *Risikostyring i staten – Håndtering av risiko i mål- og resultatstyringen.* http://www.sfso.no/upload/forvaltning_og_analyse/risikostyring/NY_Metodedokument_06012006.pdf

Ved spørsmål omkring denne eller andre UFSer – kontakt campus@uninett.no
Andre UFSer er tilgjengelige på www.uninett.no/ufs