Godkjent av:	IT-direktør Tore Burheim	**Godkjent dato:**	12.04.2021
Versjon:	1.0	**Arkivsak nr:**	20yy/xxxx

Styringssystem for informasjonssikkerhet og personvern
Del II – Vedlegg 2B –
Retningslinjer for plassering av IT-systemer på UiBs datanett

Innhold:

Versjonshistorikk

Dato	Versjon	Endring	Utført av
yy.05.2020	0.1	Definert som vedlegg	XX
24.03.2021	0.9	Revidert tekst, klar for godkjenning	Magne Bergland, Arild Raftevoll, Sidsel Storebø
26.03.2021	0.95	Endring etter revisjon av IT-direktør	Sidsel Storebø
12.04.2021	1.0	Godkjent på ledermøte	Tore Burheim

1 Begreper

AV	Audiovisuelt utstyr. En samlebetegnelse for lyd- og bildeutstyr, prosjektorer, skjermer, lydanlegg, mm.
DHCP	Dynamic Host Configuration Protocol. Kommunikasjonsprotokoll som brukes i UDP/IP datanettverk. Ved hjelp av en DHCP server er det mulig å automatisk tildele IP-adresser og andre nettverksparametre til tilkoblede klienter.
DHCP-admin	Grensesnittet der man styrer UiB sin DHCP-tjeneste.
Eduroam	Trådløsnett som tilbys ved utdanningsinstitusjoner, der man kan logge på med konto fra den institusjonen man tilhører.
ICMP	Internet Control Message Protocol. En protokoll i IP-protokoll som settes og brukes til å overføre meldinger om feil eller andre hendelser. Kjente bruksområder for ICMP er ping og traceroute.
IOT	Internet of Things; «tingenes internett». Nettverket av identifiserbare gjenstander som er utstyrt med elektronikk, programvare, sensorer og nettverk som gjør gjenstandene i stand til å koble seg til hverandre og utveksle data.
IP	Internet Protocol er den grunnleggende kommunikasjonsprotokollen for internett.
IP-adresse	Internet Protocol address. En unik identifikator eller adresse som tildeles en enhet, for eksempel en PC eller en skriver i et TCP/IP-basert datanettverk.
Klient	Med klient menes datamaskiner, nettbrett eller smarttelefoner ment brukt som sluttbrukerutstyr.
Klientdriftet maskin	Med dette menes at klienten er satt opp og driftet av IT-avdelingen ved UiB ned standard oppsett og prosedyrer.
Offentlige IP-adresser	IP-adresser i nummerserier som er tildelt en organisasjon og som kan presenteres ut mot internett.
Privatnettadresser (RFC 1918)	IP-adresser i forhåndsdefinerte adresseområder som ikke skal presenteres ut mot internett.
SIP	UiBs Styringssystem for informasjonssikkerhet og personvern.
SIP-TLF	(Session Initiation Protocol.) Protokoll for VoIP (Voice over IP; IP-telefoni). Når man ringer til en IP-telefon, er det egentlig til en IP-adresse man ringer. SIP «oversetter» et telefonnummer eller annen adresseinformasjon til en IP-adresse.
System	Infrastruktur/utstyr, applikasjoner, tjenester og løsninger som behandler data i en eller annen form. (def i SIP Del I)

TCP	Transmission Control Protocol. En nettverksprotokoll for forbindelsesorientert, pålitelig overføring av informasjon, og opererer på transportlaget i OSI-modellen for datanett.
Tjener	Datamaskin som leverer tjenester i nettverket, ikke ment som sluttbrukerutstyr.
Tjeneste	Programvare som tilbyr funksjoner over nettverket.
UDP	User Datagram Protocol. En minimal meldingsorientert nettverksprotokoll for forbindelsesløs overføring av informasjon, og opererer på transportlaget i OSI-modellen for datanett.
Wifi	Brukes i dagligtale som betegnelse på trådløse lokale datanettverk innenfor et avgrenset område. Datamaskiner, smarttelefoner og andre trådløse enheter kan koble seg til det trådløse nettet for å få internettilgang.
WPA2-PSK	Wifi med pre shared key, en forhåndsdelt nøkkel som brukes til autentisering.

2 Formål og virkeområde

Dette dokumentet beskriver hvilke IT-systemer som kan settes opp i et UiB-nettverk, trådløst eller trådfast. UiB-nettverk omfatter i denne sammenhengen alle datanett eid av UiB, inkludert, men ikke begrenset til nett med IP-adresser eid av UiB, samt nett der UiB er juridisk ansvarlig, som for eksempel Norwegian Research and Education Cloud (nrec.no).

Retningslinjene gjelder for alle IT-systemer. Med dette menes datamaskiner, utstyr, enheter og annen infrastruktur som er koblet til nettverket.

UiB har et fysisk datanett som er signalbærer for ulike logiske datanett. Datanett omtalt i resten av disse retningslinjene refererer til disse logiske datanettene.

3 Grunnleggende krav

I alle tilfeller der systemer ønskes koblet til UiBs datanett, skal det vurderes i hvilket datanett det er hensiktsmessig og sikkert at systemet plasseres. Systemet skal klassifiseres mot IT-avdelingens ulike klasser av nettverk (se punkt 4).

- Systemer på nettverk er her forstått som systemer/enheter som lytter på TCP/UDP-porter og svarer på innkommende trafikk (ut over bare ICMP). Dette utelukker vanlig konfigurerte PC-er o.l. som ikke tilbyr tjenester til andre maskiner.
- Systemer som ønskes koblet til nettverket skal forhåndsgodkjennes av IT-direktøren i henhold til UiBs føre-var-prinsipp for IT-sikkerhet (SIP Del I pkt 4.4 og 4.6) etter en definert prosedyre og nødvendig dokumentasjon.
- Systemer som skal stå på UiBs datanett og ha offentlige IP-adresser, er underlagt kravene om sikker drift og forvaltning i henhold til bestemmelsene i Styringssystemet for informasjonssikkerhet og personvern (SIP Del II, pkt. 2.3, 2.4 og 2.5).

- Utstyr og tjenester som ønskes koblet til nettverket skal forhåndsgodkjennes av IT-direktøren i henhold til UiBs føre-var-prinsipp for IT-sikkerhet (SIP Del I pkt 4.4 og 4.6) etter en definert prosedyre og nødvendig dokumentasjon
- Systemer skal være plassert på et nettverk som passer til de aktuelle oppgavene.
- IT-avdelingen skal ha rett til utvidet tilgang («root»/«admin») til alle enheter og systemer på nettverket.
- Systemer som står på åpne nettverk skal
    - Kun kjøre programvare som oppdateres fortløpende med alle publiserte sikkerhetspatcher.
    - Ha gyldig lisens på all installert programvare.
- Systemer som krever innlogging skal settes opp med tofaktor autentisering eller bedre. Systemer der dette teknisk ikke er mulig (eks IoT-utstyr, spesialutstyr) skal sikres og skjermes særskilt slik at de er tilsvarende beskyttet.
- IT-avdelingen samler grunnleggende informasjon om enheter i nettverket og kan teste systemene for drift og i sikkerhetsøyemed.

4 Krav til ulike datanett og deres bruksområde

UiB har ulike datanett tilpasset ulikt bruk og behov for sikkerhet og beskyttelse. De ulike nettene stiller krav til driftsregime for systemer og tiltak for reduksjon av sårbarhet både på nett og systemer. Målet er at en feil eller sårbarhet på ett system ikke skal utfordre andre systemer på UiB. Alle systemer, både klienter og tjenermaskiner, skal være plassert på et nettverk som passer til maskinens oppgaver.

De ulike datanettene har en funksjonsbeskrivelse. Om systemet som skal på nett passer inn i en av kategoriene, skal det plasseres deretter. Listen over ulike nettverk kan endres over tid ut fra behov, teknologi og driftsrutiner.

Alle systemer på nett skal ha en spesifisert systemeier som skal ivareta sitt ansvar ihht. øvrige bestemmelser i SIP. I tillegg skal det være klart hvem som er operativt ansvarlig for hvert system/enhet.

Klassene av datanett og systemene som kan plasseres i dem er:

4.1 Klientnett

4.1.1 Lukket nett

- Klient.uib.no – trådfast
    - Stasjonære og bærbare datamaskiner som er eid av UiB og klientdriftet. Disse plasseres i nettverk med tilfeldige offisielle IP-adresser i DHCP-admin.
- Standard nett med offisiell IP-adresse.
    - Systemer som er driftet av IT-avdelingen eller lokalt med godkjenning av IT-avdelingen og driftsavtale. Plasseres i nettverk med fast offisiell IP-adresse. (F.eks. IT-avdelingens 9- og 10-nett.)

4.1.2 Pseudoåpne nett

Alt øvrig utstyr i klassene PC, nettbrett, smarttelefon o.l., som enten er driftet lokalt og ikke har en godkjent driftsavtale eller som er privat. Dette skal ikke registreres i DHCP-admin, og hører hjemme i en av underklassene her:

- Eduroam – wifi
    - Brukere med klientdriftet, egen driftet eller privat utstyr og som er ansatt eller student ved UiB eller tilknyttet en utdanningsinstitusjon som er tilbyder av Eduroam kan bruke dette nettet. Løsningen gir tilgang til internett og åpne interne nettverk.
    - Eduroam skal skille på interne og eksterne brukere, og tildele nettverk ihht. dette.
- Gjestenettet – wifi og trådfast
    - Løsningen er tilgjengelig for alle gjester på universitetsområdet som har mobiltelefon. Brukere får pålogging via telefonnummer og passord på SMS. Nettverket er tilgjengelig både trådfast og trådløst.
- Eksamensnettverket
    - Ved bruk av digital eksamen tilbys det et trådløst nettverk med en forhåndsdelt nøkkel (WPA2-PSK) som gir tilgang til internett. Denne nøkkelen endres regelmessig.

4.2 SAFE - sikker adgang til forskningsdata og e-infrastruktur

- Eget nettverk for behandling av personopplysninger (særlige kategorier) i forskning. UiB stiller krav til at all behandling av personopplysninger (særlige kategorier) i forskning skal foregå i SAFE eller i en tilsvarende sikker løsning.

4.3 Lab-IT

- Nettverk for teknisk utstyr og tilknyttede datamaskiner som brukes i laboratorier og som skal ha nettverkstilgang. Maskinene kommer ofte med ferdiginstallerte operativsystemer og vedlikeholdes gjerne av produsent/leverandør. Disse maskinene skal plasseres på nettverk slik at de står i egen sone for hvert miljø eller hver lab, slik at de bare har kontakt med lagring og er beskyttet fra UiB sitt øvrige nettverk, og heller ikke utgjør en risiko for andre soner eller nettverk.

4.4 AV-nettverk

- Styringspanel for undervisningsrom, castingenheter, prosjektører, skjermer o.l. som brukes til audiovisuelle oppgaver i undervisningsrom, på museer, i TV-produksjon og liknende, legges på egne nett siden de har behov for egne protokoller og er følsomme for annen trafikk.

4.5 Printernettverk

- Skrivere og multifunksjonsmaskiner settes på et eget nettverk med adresser som ikke er tilgjengelig for annet enn tjenere med skriverkøer og annet multifunksjonsoppsett, herunder «scan to mail» og liknende.

4.6 Telefoninettverk

- IP-telefoner som benyttes ved UiB plasseres på egne nettverk med åpning kun for de protokollene som trengs for at de skal fungere.

4.7 Tekniske nettverk med ulike systemklasser som f.eks.:

- Bygg-styringssystemer (SD-anlegg) og liknende automasjonsløsninger
- Kamera og overvåkingsutstyr
- Tilgangskontroll
- Bookingsskjermer, infoskjermer/visningsflater
- Biblioteksystemer for alarm, returmaskiner o.l.

Felles for disse systemene er at de plasseres på nettverk som ikke er direkte tilgjengelige fra internett og er avgrenset fra andre interne nettverk. Det gjøres en kritisk vurdering i hvert enkelt tilfelle, basert på hva systemet skal kommunisere med og hvilke driftsrutiner systemet har.

4.8 IOT-nettverk

- Sensorer eller andre enkle enheter som trenger nett og som ikke passer inn i de øvrige klassene kan plasseres her. Her vil en normalt få tilgang til internett fra enheten og kunne kommunisere med nødvendige enheter i nettverket.

4.9 Datasenter / Servernettverk

- Åpne tjenernettverk med egne filtre for å plassere tjenere driftet av IT-avdelingen.
- Disse er inndelt i flere logiske nettverk etter karakteristikk på tjenestene som tilbys.

4.10 NREC

- NREC er Infrastructure-as-a-Service (IaaS). IaaS tjenesten er en selvbetjent infrastruktur hvor en bruker setter selv opp en standardisert server og lagring etter behov, utfra et gitt ressursbehov. Tjenesten brukes til blant annet for å sette opp web-tjenester, lagring av data og utføre beregninger.

5 Systemer som ikke inngår i IT-avdelingens driftsoppsett

5.1 Egendriftet utstyr

I utgangspunktet skal alt utstyr som ikke driftes av IT-avdelingen eller har driftsavtale med IT-avdelingen, stå på nettverk som er tilpasset utstyrets art, som beskrevet i punkt 4. Hovedregelen er blant annet begrensninger i form av privatnettadresser (IP-adresser som ikke eksponeres utenfor lokalt nett; RFC 1918) og liknende.

Egendriftet utstyr som tilbyr tjenester på nettverk plasseres i egne nettverk. IT-avdelingen vil kunne foreta revisjon av systemene og teste sikkerheten. IT-avdelingen skal ha tilgang til

logger og mulighet for tilgang på systemet ved revisjon eller uønskede hendelser. Logging skal minimum følge UiBs rutiner for logging.

Egendriftet utstyr som må på UiB sitt nettverk og som trenger en offentlig IP-adresse (se pkt. 4.1.1 over), skal godkjennes av IT-direktør i henhold til UiBs føre-var-prinsipp for IT-sikkerhet (SIP Del I).

5.2 Tilleggskrav for utstyr driftet av ekstern leverandør

Dersom det er godkjent at ekstern leverandør kan drifte et system i UiBs nett, er det et krav at disse er på sikrede nettverk eller nettverk med begrenset tilgang. Leverandør får tilgang via jumphost, VPN-løsning eller annen løsning godkjent av IT-avdelingen. UiB loggfører aktivitet for disse nettene.

UiB skal ha tilgang til systemet og logger ved uønskede hendelser og ved revisjon. Det skal gjøres en risikovurdering før systemet settes i drift for å avklare krav til driftsrutiner og sikring. Det skal også avklares hvilke logger som skal oppbevares og oppbevaring og tilgjengeligheten for disse.

Rutiner for drift, vedlikehold og sikring av systemet skal dokumenteres og oversendes IT-avdelingen.

6 Andre juridiske enheter som er på UiB sitt nettverk

Organisasjoner som er tilknyttet UiB og som har systemer på UiB sitt nett, er underlagt samme rammeverk som for øvrige maskiner og tjenester.

Dette skal reguleres av egne avtaler med organisasjonene det gjelder.