Godkjent av: IT-direktør Tore Burheim **Godkjent dato:** 24.09.2020
Versjon: 2.0 **Arkivsak nr:** 20yy/xxxx

Styringssystem for informasjonssikkerhet og personvern
Del II – Vedlegg 1A -
Instruks for drift av IT-utstyr og systemer

Innhold:

Versjonshistorikk

Dato	Versjon	Endring	Utført av
dd.05.2020	2.0	Inngår som vedlegg i SIP Del II	Sidsel Storebø
24.9.2020	2.0	Godkjent	Tore Burheim

1 Innledning

Instruks for drift av IT-utstyr og systemer (heretter benevnt Driftsinstruksen) gjelder som en overordnet driftsinstruks for all drift av IKT-tjenester ved UiB, uavhengig av hvem som drifter og forvalter disse. Instruksen godkjennes av IT-direktøren, og skal revideres årlig.

2 Systemeier og systemansvarlig

Alle IT-systemer og alt IT-utstyr har en definert systemeier basert på bestemmelsene i Styringssystem for informasjonssikkerhet og personvern Del I og Del II. Som del av sitt ansvar for å sørge for sikker drift og forvaltning skal systemeier utpeke noen med det daglige operative ansvaret for systemet/utstyret. Den operative evnen skal ut fra en risikovurdering, sikkerhetsvurdering og krav til tilgjengelighet for brukere være tilstrekkelig dekket.

3 Anskaffelse av maskin- og programvare

Alle innkjøp skal foretas i henhold til regler for offentlige anskaffelser. De fleste innkjøp vil være dekket gjennom rammeavtaler, og der UiB har rammeavtaler skal disse benyttes. Der det ikke foreligger rammeavtaler skal anskaffelser gjennomføres som egne anbud eller konkurranser etter reglene for offentlige anskaffelser.

Det skal så langt det er mulig benyttes standard maskinvare og programvare. Det er et mål å kjøpe løsninger med lang levetid og forutsigbart kostnadsbilde i levetiden. Nye systemer må passe inn i eksisterende infrastruktur.

Større anskaffelser skal gjennom et testløp før de går i produksjon. Maskiner og programvare skal være innenfor støtte (support og serviceavtale eller garanti) fra leverandør i forventet levetid.

4 Merking av maskinvare

Alle investeringer (innkjøp i artsklasse 4***) blir registrert i UiBs anleggsregister. I tillegg til dette skal alle nøkkelkomponenter være merket med maskinnavn og være beskrevet i UiBs konfigurasjonsdatabase (CMDB). Mindre komponenter og personlige datamaskiner registreres i relevante driftssystemer (AD, Foreman, Nav, mm).

Alle kabler mellom maskinvare i maskinhaller og datarom skal være merket i begge ender.

5 Medieregister og merking av lagringsmedier

Alle driftsgrupper skal vedlikeholde et medieregister som inneholder installasjonsmedium til all programvare som er i bruk. Taper som er i bruk i backupsystemet merkes og dokumenteres i backupsystemet. Disse er til enhver tid i backup-roboter, og fjernes ikke fra disse før de går ut av produksjon.

6 Konfigurasjonskontroll

Alle viktige komponenter skal være registrert i UiBs konfigurasjonsdatabase CMDB[1], eller i andre systemer som holder på konfigurasjon (NAV, AD, Puppet, GiT, SCCM, DHCPAdmin, mm). Konfigurasjonskontroll utføres i henhold til prosessbeskrivelse for endringsprosessen.

7 Systeminstallasjon og oppsett

Følgende krav gjelder til installasjon og systemoppsett av systemer og oppsett på UiB

a) Alle fysiske servere som leverer tjenester til UiB skal plasseres i avlåste rom, med begrenset tilgang og adekvat kjøling. Servere skal i utgangspunktet ha avbruddsfri strømforsyning, men der avvik fra dette skal vurderes eksplisitt i ROS-analysen.
b) Alle systemer skal herdes for å kunne stå eksponert for internett, da de fleste av UiBs systemer plasseres direkte på internett, uten annen brannmur enn aksesslister i grenserutere. Tjenester, porter og programvare som ikke benyttes skal stenges ned. Det skal være etablert lokal brannmur, med kun de nødvendige åpninger for at systemet skal kunne fungere. Avvist trafikk skal logges.
c) Alle systemer skal oppdateres fortløpende med sikkerhetsoppdateringer og det skal etableres rutiner for å ivareta dette i helger, helgedager og i ferier.
d) Alle relevante sikkerhetsfunksjoner i komponenter skal benyttes. Der systemet ikke kan sikres direkte må utstyret penetrasjonstestes fra innenfor og utenfor UiB og adekvate filtre på brannmur og andre sikkerhetstiltak implementeres.
e) For de systemer hvor datavirus kan være en risiko, skal det kjøres antivirusprogramvare. Epost skal inspiseres for å hindre annen skadevare. Kodebeskyttelse for å stoppe ukjente sårbarheter i å bli utnyttet skal implementeres der det er mulig[2].
f) Driften skal så langt det lar seg gjøre utføres med automatisering, dette for å gjøre driften mest mulig effektiv og standardisert, og for å gjøre det enkelt å gjenskape systemer.
g) Konfigurasjoner skal beskyttes mot uautorisert endring, og sikkerhetskopieres. Så langt det er mulig bør endringer i konfigurasjon loggføres og overvåkes.
h) Systemer skal plasseres i sikkerhetssoner i henhold til funksjon, tilgangsbehov og klassifisering av data. Trafikk mellom sonene skal gå gjennom en stateful brannmur. Trafikk mot internett skal filtreres av aksesslister etter behov.
i) Trådløst nett, bortsett fra UiBs gjestenett, skal ha autentisering mot brukerkonto og tilstrekkelig kryptering.
j) Alle nettverksporter som blir eksponert for brukere skal ha 802.1x autentisering.
k) Passord og krypteringsnøkler må oppbevares slik at uvedkommende ikke får tilgang til dem, med godt nok sikkerhetsnivå. Disse må lagres slik at flere personer enn en har tilgang til dem. Eksempler på dette kan være PGP-krypterte filer eller lignende.

8 Test og idriftsetting

Det skal benyttes separate miljøer for utvikling, test og produksjon slik at operative virksomhetsprosesser og produksjonsdata ikke blir påvirket ved feil i utvikling- og testløp.

Testmiljø må så langt det er mulig settes opp med genererte testdata. Testdata skal beskyttes tilsvarende produksjonsmiljø slik at sikkerhetstester blir gjennomført så reelt som mulig og sensitiv informasjon ikke kommer på avveie.

[1] CMDB = Configuration management database

[2] Ref punkt 2.3.10 i NSM grunnprinsipper for sikker drift

Det skal gjennomføres tilstrekkelig testing gjennom hele anskaffelses- og utviklingsløpet slik at feil og mangler rettes opp så tidlig som mulig og før idriftsetting. Dette kan inkludere enhetstesting, integrasjonstesting, systemtest, akseptansetest, pilottest, penetrasjonstest og stresstest.

9 Endringskontroll

Det skal gjennomføres dokumentert endringskontroll av alle endringer og oppgraderinger. Alle endringer skal:

a) Vurderes med hensyn på kritikalitet.
b) Vurderes i forhold til påvirkning på, eller avhengighet av andre systemer og andre systemers avhengighet tilbake (kompatibilitet).
c) Testes på forhånd så langt det er mulig og formålstjenlig sett i lys av risiko.
d) Varsles i god tid til brukere og andre som kan påvirkes.
e) Varsles til de som har ansvar for brukerstøtte på systemet.
f) Vurderes i forhold til og planlegges for eventuell rulling tilbake (reversere endringen) dersom det oppstår feil under eller umiddelbart etter endringen.
g) Gjennomføres innenfor forhåndsannonserte og planlagte vedlikeholdsvindu, fortrinnsvis utenom ordinær arbeidstid eller på andre tidspunkt som i minst mulig grad påvirker brukere negativt. For systemer med få brukere kan endringer gjennomføres i arbeidstid dersom dette ikke påvirker brukere negativt eller er avtalt.
h) Ved endringer i systemer som behandler sensitive data skal det vurderes særskilt om kravene om konfidensialitet og øvrige sikkerhets- og personvernkrav ivaretas både under og etter endringen er gjennomført.

Alle endringer skal godkjennes av bemyndiget person eller fora (endringsmøte) basert på vurderingene. Rekkefølge på gjennomføring av endringer skal vurderes og planlegges sammen med dette.

Ved kritiske feilsituasjoner som for eksempel kritiske sikkerhetshull kan det gjennomføres nødendring med kort frist etter godkjenning av systemeier eller dens stedfortreder eller annen bemyndiget person. Endringskontroll ved nødendring kan gjennomføres muntlig og dokumenteres i ettertid.

10 Kommunikasjon

All kommunikasjon og administrasjon skal gå over krypterte protokoller, med det som til enhver tid anses som godt nok nivå på kryptering. Det kan gjøres unntak for denne regelen for trafikk som går på linjer der UiB har full kontroll på linjene ende til ende, uten risiko for lekkasje av informasjon.

11 Systemovervåking

Alle viktige tjenester skal overvåkes med overvåkningsverktøy, og det skal gå varsel til driftspersonell og/eller vakthavende ved feilsituasjoner.

Alle logger skal sendes til sentralt loggemottak og behandles der for å avdekke uønsket aktivitet. Nettverk skal overvåkes, og aksesslister i grenseruter justeres for å stenge ute uønsket trafikk

12 Brukeradministrasjon/tilgangskontroll

Brukerkonti skal styres gjennom UiBs system for brukeradministrasjon og tilgangsstyring.

Rettigheter til brukere styres av godkjennere gjennom UiBs system for brukeradministrasjon og tilgangsstyring, og ved at det meldes inn behov gjennom relevant saksbehandlingsverktøy og definerte prosesser.

I tillegg til konti for brukere opprettes det systembrukere for forskjellige applikasjoner. Disse skal ha et sterkt unikt passord.

Systemadministratorer skal ha egne separate, dedikerte og navngitte konti med utvidete rettigheter. Disse skal kun benyttes til driftsoppgaver, og ha tofaktor autentisering. Disse skal opprettes i sentrale katalogtjenester. Der det er mulig skal man først logge inn med en upriviligert bruker, for deretter å bytte til konto med systemadministrasjonsrettigheter. Dette skal logges. Systemadministrative konti skal ikke ha rettigheter i hele eller større deler av IKT strukturen eller en systemportefølje. Administrative konti skal stenges så snart tjenstlig behov opphører.

Brukere skal ikke ha mer rettigheter enn det som er nødvendig for å få utført sine oppgaver. Rettigheter skal stenges så snart tjenstlig behov opphører.

Administratorer skal benytte dedikerte maskiner for alle systemadministrative oppgaver, eller oppgaver som krever forhøyede tilganger. Maskinene bør isoleres fysisk fra virksomhetens primære nettverk. Maskinene bør ikke benyttes til å lese privat e-post, utarbeide dokumenter eller ha mulighet til å surfe på internett. Det anbefales bruk av jumpstation eller egne administrasjonsmaskiner.

13 Beredskapstiltak

De lokale beredskapsplanene som gjelder for UiBs ulike organisasjonsenheter skal også dekke beredskapssituasjoner knyttet til informasjonsverdier og data, samt IT-utstyr og IT-systemer der dette er relevant.

Alle produksjonssystemer skal tas backup av. Det skal foreligge planer for hvordan systemer skal gjenskapes etter kritiske feil (kontinuitet).

Systemer skal settes opp med redundans på tvers av flere fysiske lokasjoner. Det skal øves jevnlig på å slå over driften mellom disse lokasjonene. Avvik skal vurderes og dokumenteres i forhold til risiko og kritikalitet.

Alle kritiske fagområder skal dekkes med minst 2 personer med kompetanse til å foreta drift på systemene. Hvis ikke dette er tilfelle, må det tas egne forholdsregler for å dekke opp ved fravær.

14 Vedlikehold og reparasjon

Alt utstyr som er i produksjon, skal ha tilgang på reservedeler. Responstid skal være i forhold til kritikalitet på tjenesten som leveres. Tilgang på deler kan gjøres gjennom serviceavtaler og/eller gjennom å ha reservedeler lokalt.

15 Avhending og tilintetgjøring

Utstyr som går ut av produksjon skal leveres til resirkulasjon. Utstyr som ikke inneholder data resirkuleres gjennom UiBs generelle ordning for dette. Utstyr (disker, taper, mm) som kan inneholde data resirkuleres gjennom en sikret løsning med sertifikater for at data blir håndtert forsvarlig og slettet. Disker som kan inneholde sensitive data beholdes ved feilsituasjoner, og resirkuleres sikkert. Utstyr som kasseres skal føres ut av CMDB, og fjernes fra anleggsregisteret ved UiB.