Digitalt og autentisk

Planlegging av ny depotløsning for Arkivverkets digitalt skapte arkivmateriale

Del 2:

Vedlegg til prosjektrapport

Riksarkivet 01.03.2010

Innhold

Kravspesifikasjon til Arkivverkets arbeid med digitalt skapt arkivmateriale

Oversikten følger disposisjonen i TRAC – Trustworthy Repositories Audit & Certification: Criteria and Checklist[1]*. Den omfatter: 1) utvalgte krav fra TRAC som vurderes som relevante og gyldige for Arkivverkets depotfunksjoner, og 2) krav knyttet spesifikt til håndteringen av autentisk arkivmateriale som ikke er formulert i TRAC. De sistnevnte bygger på dokumentasjonen fra InterPARES-prosjektet og en vurdering av Arkivverkets nåværende praksis. Det gis spesifikke referanser til TRAC i de tilfeller kravene er hentet fra denne standarden, eventuelt i en tilpasset eller utvidet form.*

Sist i dokumentet følger en terminologioversikt som relaterer anvendte norske betegnelser til OAIS-standarden og TRAC.

A. Organisatorisk infrastruktur

		TRAC-ref:
	Organisasjonsstruktur, bemanning og kompetanse (TRAC A2)	
1	Arkivverket må ha en stab med adekvat kompetanse, arbeidstrening og rolle-fordeling. For depotfunksjonene spesielt bør bemanningen dimensjoneres og struktureres med sikte på å oppnå sertifisering i en TRAC-basert evaluerings-prosess for digital langtidsbevaring. Følgende dokumentasjon må foreligge: a) en vurdering og beregning av bemannings- og kompetansebehovet i relasjon til virksomhetens aktiviteter og forpliktelser, b) en plan for kompetanseutvikling basert på utviklingsmål, spesielt for digital langtidsbevaring.	*A2.1-3*
	Ansvarlighet, dokumenterte prosedyrer og policy-rammeverk (TRAC A3)	
2	Arkivverkets politikk for å bevare digitalt skapt arkivmateriale og prosedyrene for å iverksette den må være allment tilgjengelig, og oppfattes som autoritativ og praktisk anvendelig av de organer og miljøer som den omfatter.	*A3.1*
3	Metodikken og prosedyrene for å bevare digitalt arkivmateriale må være fullstendig dokumentert, og gjenstand for jevnlig evaluering og revisjon for å forholde seg til teknologiutviklingen, endrede omgivelser og interne behov.	*A3.2-4*
4	Det må bevares dokumentasjon om endringer i metodegrunnlag, prosedyrer og infrastruktur med vekt på å beskrive konsekvenser for bevart materiale.	*A3.6*
5	Det må foreligge dokumentasjon av systemopplegg som er etablert for å sikre den bevarte arkivbestandens integritet, herunder loggingssystem o.a. mekanismer for å bekrefte at alt informasjonsinnhold har vært gjenstand for uavbrutt integritetssikring, og fortsatt samsvarer med mottatt innhold.	*A3.8*

[1] Research Libraries Group (RLG) og National Archives and Records Administration (NARA) Digital Repository Certification Task Force, 2007. http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf

6	Arkivverket må være forpliktet til å følge opplegg for en regelmessig egen-vurdering og ekstern evaluering eller sertifisering. En eventuell sertifisering må også medføre en forpliktelse til å varsle vedkommende akkrediteringsinstans om endringer i virksomheten som kan endre status for sertifiseringen.	*A3.9*
	Økonomisk bærekraft og langsiktighet (TRAC A4)	
7	Det må kunne legges fram sykliske virksomhets- og budsjettplaner som viser at arbeidet med å forvalte digitalt arkivmateriale har langsiktig bærekraft.	*A.4.1-3*
8	Arkivverket må holde løpende oversikt over alle forhold som medfører økonomisk risiko, og være forpliktet til å overvåke utviklingen når det gjelder forholdet mellom egne tilgjengelige ressurser og de faktiske kostnadene ved å ivareta det langsiktige forvalteransvaret for den digitale arkivbestanden.	*A.4.4-5*
	Formaliserte avtaler med arkivskapere (TRAC A5)	
9	Kontrakt- og avtalebaserte bestemmelser om råderett og tilgang til bevart materiale må være underlagt et regime for administrasjon og oppfølging. Når materiale bevares med status som deponering, må det finnes avtaler som spesifiserer rettigheter og ansvarsforhold. Disse må også sikre rettigheter til å utføre nødvendige vedlikeholdsoperasjoner på materialet.	*A5.1-5*
10	For materiale som bevares med status som deponering, må tidspunktet for statusskiftet til avlevering fastsettes, og partenes rettigheter og plikter i deponeringsperioden klargjøres. For avlevert materiale må det uttrykkelig fastslås at råderetten til arkivversjonen er overdratt til Riksarkivaren.	-

B. Administrasjon av digitale objekter

	Aksesjon av arkivinnhold (TRAC B1) – I. Tilrettelegging for bevaring	
11	Gjennom regelverk, standarder og konkret rådgivning må Arkivverket bidra til at IT-systemer med arkivinformasjon får implementert funksjonalitet som tilrettelegger denne informasjonen for bevaring og for eksport i form av arkiv-versjoner. Jf. også punkt 17 og 18.	-
12	Bevaringsverdig digitalt arkivmateriale må identifiseres gjennom aktiv kartlegging. For statlig materiale som ikke omfattes av generelle påbud om bevaring og avlevering, må det fattes konkrete bevaringsvedtak. For bevarings-verdig privat materiale må det gjøres avtale om bevaring og avlevering/ deponering med den enkelte arkiveier.	-
13	For digitalt arkivmateriale som er vedtatt eller avtalt bevart, må arkivversjonens innhold og format(er), det konkrete tidspunktet for nærmeste avlevering/deponering og en plan for oppfølgende avleveringer/deponeringer spesifiseres i formaliserte avtaler med den enkelte arkivskaper. Avtalene skal gi Arkivverket en samlet oversikt over hva som skal avleveres/deponeres fra hvilke organer til hvilke tidspunkt.	-
14	Arkivverket må ha et apparat som ajourholder oversikt over avtaler, og følger dem opp ved en aktiv inndriving av berammede avleveringer/ deponeringer.	-

	Aksesjon av arkivinnhold (TRAC B1) – II. Definisjon av arkivversjoner	
15	Arkivverket må kunne identifisere hvilke egenskaper ved digitale objekter som skal bevares, og klargjøre dette gjennom bestemmelser, programformuleringer eller konkrete avtaler.	*B1.1*
16	Generelle avleverings-/deponeringsbestemmelser eller konkrete avtaler må spesifisere hvilken dokumentasjon (metadata) som skal være tilknyttet informasjonsinnholdet når en arkivversjon mottas for bevaring som en avleveringspakke.	*B1.2*
17	Den informasjon i et IT-system som representerer det eller de arkivdokumenter som skal ekstraheres og kopieres til vedkommende arkivversjon, må i hvert tilfelle kunne defineres eksakt av Arkivverket.	-
18	Arkivverket må også kunne definere innholdet i arkivversjonen slik at dette er frikoblet fra produksjonssystemets tekniske struktur, og avgrenset til de komponenter i produksjonssystemet som representerer arkivdokumentene og deres logiske struktur. Arkivversjonen må da være organisert slik at alle komponentene i et arkivobjekt kan sammenstilles til et hele, og slik at arkiv-objektene samlet danner en struktur som viser deres relasjoner og innbyrdes forbindelser, jf. avleveringsformatet i Noark-5.	-
	Aksesjon av arkivinnhold (TRAC B1) – III. Fremstilling av avleveringspakker	
19	Det må finnes mekanismer for å bekrefte at arkivinnholdet i en arkivversjons avleveringspakke har det opphav som forventes, og at materialets proveniens er opprettholdt.	*B1.3*
20	En avleveringspakke må være slik organisert at den sikrer tilgang til det fullstendige digitale innholdet (bit-innholdet) i alle objekter som den omfatter. Bestemmelser og avtaler må fastslå at objekter ikke kan bevares i form av referanser til andre kilder.	*B1.5*
21	Informasjonsinnholdet i avleveringspakken må representere en eksakt, uendret og feilfri reproduksjon av den nærmere definerte og avgrensede informasjon i vedkommende produksjonssystem som skal bevares iht. fastsatte bestemmelser eller inngåtte avtaler. Jf. også punkt 25-27, nedenfor.	-
22	Til arkivversjonen i en avleveringspakke må det være knyttet: a) opplysninger om det samlede informasjonsinnholdets spesifikke opphavs- og brukssammenheng, b) beskrivelser av format(er), struktur- og innhold (tekniske metadata) som er nødvendige for å fremstille materialet i en tilgjengelig form.	-
23	Når en avleveringspakke omfatter flere arkivdokumenter, f.eks. journalposter med tilhørende saksdokumenter, må hvert arkivdokument være tilknyttet originale metadata om sin identitet, opphavs- og brukssammenheng for å opprettholde informasjonens autentisitet og muliggjøre en verifisering av den.	-
24	En avleveringspakke må oppfylle format-, dokumentasjons- og mediekravene som er fastsatt i Riksarkivarens avleveringsbestemmelser, jf. FOR 1999-12-01 nr 1566, kapittel VIII.	-

25	Med avleveringspakken skal det følge dokumentasjon som beskriver hvordan arkivversjonen er blitt fremstilt, og hvordan informasjonsinnholdet er blitt integritetssikret i forhold til innholdet i vedkommende produksjonssystem. Det skal i denne sammenheng også dokumenteres hvordan det er kontrollert at antallet poster og evt. antallet dokumenter i arkivversjonen er identisk med det tilsvarende originale antallet i produksjonssystemet.	-
26	Med avleveringspakken skal det følge en egen sjekksum som gjør det mulig for Arkivverket å verifisere at mottatt innhold er identisk med innholdet i versjonen som ble produsert fra vedkommende produksjonssystem. Sjekksummen må overføres atskilt fra informasjonsinnholdet. Det må dokumenteres hvilken algoritme som ble brukt for å generere sjekksummen.	-
27	For å kunne verifisere at informasjonsinnhold og metadata ikke er endret etter at arkivversjonen er blitt fremstilt, *bør* krav 26 være implementert slik at sjekksum genereres under eksporten av informasjon fra produksjonssystemet. Det skal da genereres en egen sjekksum for alle eksporterte metadata. Dersom også elektroniske dokumenter inngår i arkivversjonen, *bør* hvert dokument være tilknyttet en sjekksum som er generert på grunnlag av innholdet. Sjekksummer skal genereres under prosessen med eksport til arkivversjonen. Dersom dokumentene allerede har sjekksummer (evt. i form av digitale signaturer) i produksjonssystemet, skal det vurderes i det enkelte tilfelle om det er behov for å generere nye sjekksummer ved eksport.	-
28	Dersom avleveringspakkens arkivversjon omfatter XML-filer, skal det være dokumentert at disse er blitt validert mot tilhørende XML Schema eller DTD.	-
29	Arkivbeskrivelsen som medfølger i avleveringspakken, jf. punkt 22a, skal være Asta-kompatibel iht. Riksarkivarens spesifikasjoner.	-
30	Det skal være attestert av en ansvarlig representant for avhenderen at avleveringspakkens informasjonsinnhold og medfølgende dokumentasjon er gyldig og korrekt.	-
	Aksesjon av arkivinnhold (TRAC B1) – IV. Kontroll av avleveringspakker	
31	Avleveringspakker skal håndteres i et kontrollert miljø fra de mottas til de blir innlemmet i Arkivverkets digitale depot. Materiale skal integritetssikres umiddelbart ved mottak for å eliminere muligheter for en senere uautorisert endring av informasjonsinnhold, og for aktivt å kunne verifisere at det er bevart uendret fra og med mottak. Integritetssikring skal utføres ved å generere en samlet sjekksum for hver avleveringspakke slik den foreligger ved mottak.	-
32	Et kontrollert miljø gjennom prosessen med overføring og testing må også ivareta kravene til konfidensialitetssikring av avleveringspakkens informasjonsinnhold. Dersom materialets opprettholdte integritet sikres ved bruk av sjekksum, vil kravet til konfidensialitetssikring likevel være usvekket.	-
33	Arkivverket må ha prosedyrer for å verifisere om informasjonsinnholdet i en mottatt avleveringspakke er blitt overført komplett og korrekt. Det må også være etablert faste kriterier og prosedyrer for å håndtere, og eventuelt avvise en avleveringspakke med feil eller med et innhold som avviker fra det fastsatte.	*B1.4*

34	Arkivverket må ha prosedyrer for å verifisere om en avleveringspakkes informasjonsinnhold er korrekt og komplett iht. fastsatte bestemmelser eller inngåtte avtaler, og om innholdet er tilknyttet de tekniske og logiske metadata som kreves for at det kan bevares med opprettholdt autentisitet og lesbarhet.	-
35	Mangler eller inkonsistens i en avleveringspakke som påvises ved Arkivverkets kontroll, må dokumenteres. Det må klargjøres om disse kan tilbakeføres til tilsvarende mangler eller inkonsistens i vedkommende produksjonssystem. Dersom en slik sammenheng ikke kan fastslås, må også dette dokumenteres.	-
36	Når en avleveringspakke inneholder sjekksummer eller andre mekanismer for å verifisere informasjonsinnhold, må Arkivverket ha prosedyrer for å utføre og dokumentere en slik verifisering.	-
37	Arkivskapere som overfører en avleveringspakke, må gis tilbakemelding om tidsrammen for godkjenningsvurderingen og i nødvendig grad orienteres om status underveis i arbeidet. Når en avleveringspakke aksepteres for bevaring etter utført kontroll, skal arkivskaperen motta formelt brev om at Arkivverket påtar seg bevaringsansvaret.	*B1.6-7*
38	Det må bevares dokumentasjon om alle relevante hendelser og prosesser i tilknytning til aksesjoner for å bekrefte at prosessene er forskriftsmessig gjennomført.	*B1.8*
	Organisering av mottatte arkivversjoner som arkivpakker (TRAC B2)	
39	Hver arkivversjon som aksepteres og innlemmes i Arkivverkets depot, skal lagres som en samlet arkivpakke (bevaringspakke). For en arkivpakke må det finnes en definisjon som beskriver hvordan informasjonsinnholdet er tilknyttet de metadata som praktisk og logisk er nødvendige for å kunne identifisere, fremvise og forstå innholdet som autentisk arkivmateriale, jf. krav nr. 45 og 46. Definisjonen skal knytte komponentene sammen til en logisk enhet som alltid må kunne gjenfinnes og håndteres samlet.	*B2.1-2*
40	Definisjonen av arkivpakker som innlemmes i Arkivverkets digitale depot, skal baseres på standardene METS og PREMIS. Kategoriene i Arkivverkets arkivpakker skal kunne relateres til OAIS-standarden.	-
41	Det må finnes dokumentasjon som verifiserer at hver enkelt arkivpakke er fullstendig og korrekt generert (transformert) fra vedkommende mottatte avleveringspakke. Dersom arkivpakken er blitt transformert eller normalisert i forhold til avleveringspakken, må det fremgå hvordan den er konstruert på grunnlag av den. I tilfeller hvor det brukes standardiserte og dokumenterte prosesser for å generere en arkivpakke, er det nok å vise at disse prosessene er blitt gjennomført uten rapporterte feil.	*B2.3 og B2.11*
42	Det må finnes dokumentasjon som identifiserer alle mottatte avleveringspakker, og viser hvordan de er behandlet, og hvilke bevarte arkivpakker de utgjør eller fordeler seg på.	*B2.4*
43	Det må anvendes regler for navngiving som gir synlige, bestandige og unike identifikatorer for alle arkivpakker i digitalt depot.	*B2.5*

44	Arkivverket må ha tilgang til verktøy og hjelpetjenester for å bestemme de bevarte digitale objektenes semantiske eller tekniske kontekst (f.eks. tilgang til internasjonale tjenester for formatinformasjon og tekniske metadata som UK National Archives PRONOM og DCC Representation Information Registry).	*B2.7*
45	Tilknyttede tekniske metadata må bevares med permanent tilknytning til informasjonsinnhold. I de tilfeller slike metadata ikke følger fastsatte standarder, må det innhentes og bevares spesifikk dokumentasjon som gjør det mulig å lese og anvende innhold i form av bits som et informasjonsobjekt.	*B2.8*
46	Bevaringsmetadata må være permanent tilknyttet informasjonsinnholdet for å sikre at det er lagret med integritetssikrende opplysninger, proveniens-opplysninger som viser dets opphav, og kontekstopplysninger som gjør det forståelig ut fra sammenhengen hvor det er skapt og brukt.	*B2.9*
47	Det må finnes en dokumentert prosess for å kontrollere at bevart informasjons-innhold lar seg fremstille med tilknyttede bevaringsmetadata og tekniske metadata, slik at informasjonsinnholdet er anvendelig og tilfredsstiller definerte krav til forståelighet.	*B2.10*
48	Det må være etablert praktiske muligheter for å foreta en uavhengig evaluering av den bevarte arkivbestandens samlede integritet. I denne sammenheng må det eksistere registre med oversikt over: - alle aksesjoner og hvilke arkivpakker som har innhold fra dem, - alle arkivpakker supplert med opplysninger om hvordan hver enkelt er relatert til innførslene i aksesjonsregisteret.	*B2.12*
49	Det må finnes samtidig skapt dokumentasjon om utførte operasjoner og administrative prosesser knyttet til genereringen av arkivpakker.	*B2.13*
	Planlegging av langtidsbevaring (TRAC B3)	
50	Det må være utformet bevaringsstrategier for å håndtere media og formater som blir forgjengelige, og for å hindre korrumpering av data.	*B3.1*
51	Det må finnes mekanismer for monitorering som varsler om fare når formater og tekniske metadata er i ferd med å bli teknologisk forgjengelige, og være planlagt tiltak som reaksjon på slike faresituasjoner.	*B3.2-3*
	Vedlikehold av arkivpakker ved langtidsbevaring (TRAC B4)	
52	Arkivpakker må på en pålitelig måte avspeile det som var gjenstand for datafangst (”capture”) fra den enkelte aksesjon (avleveringspakke), jf. krav 41. Dersom innholdet i arkivpakken senere transformeres, eventuelt som resultatet av migrering, må prosessene være dokumenterte og ettersporbare. TRAC krever at dersom en arkivpakke endres, så må dette skje ved at det lagres en ny versjon i tillegg til den opprinnelige. Det må finnes lenker til den opp-rinnelige pakken fra alle senere transformerte arkivpakker. Samtlige versjoner må dermed beholdes, og være organisert som en kjede av arkivpakker. Dette kravet i TRAC skal ikke oppfylles fullt ut. Ved gjentatte formatkonver-teringer skal det kunne fravikes ved at bare de to nyeste versjonene beholdes i tillegg til den opprinnelige versjonen av arkivpakken. Dette gjelder under	*B4.2-3*

	forutsetning av at det brukes standardiserte og dokumenterte prosesser for konvertering, at prosessene gjennomføres kontrollert og uten rapporterte feil, og at de blir dokumentert som utførte operasjoner. TRAC-kravet skal ikke anvendes for migrering når dette begrenser seg til en ren overkopiering av objekter mellom lagringsenheter. Forutsetningen er at prosessen ved migrering verifiseres og dokumenteres.	
53	De bevarte arkivversjonenes opprettholdte integritet må være gjenstand for aktiv monitorering. Arkivpakker må derfor være tilknyttet integritetsbevarende informasjon i form av sjekksummer. Sjekksummene må være lagret atskilt fra arkivpakkene på en beskyttet måte. Det må eksistere en logg for kontrollen av sjekksummer. Integritetskontrollen må dessuten overvåke den samlede arkivbestanden, og bekrefte at den faktisk omfatter de arkivpakker som skal finnes der – og bare disse.	*B4.4*
54	Det må finnes samtidig skapt dokumentasjon om utførte operasjoner og administrative prosesser knyttet til arkivpakker.	*B4.5*
	Gjenfinning og bruk – "Information management" (TRAC B5)	
55	Det må finnes et minimum av beskrivende metadata for arkivbestandens arkivpakker som gjør det mulig å identifisere og eventuelt gjenfinne arkivinnhold.	*B5.1*
56	Referanseintegritet (bestandige identifikatorer) mellom arkiverte objekter og tilknyttede beskrivende metadata må være etablert. Slik integritet må også være opprettholdt etter utførelsen av operasjoner som innvirker på arkivpakkene og deres identifikatorer.	*B5.3-4*
	Tilgangsstyring og brukertjenester – "Access management" (TRAC B6)	
57	Arkivverkets politikk for å innvilge tilgang til bevart digital arkivinformasjon må være dokumentert og bekjentgjort for brukerne.	*B6.1*
58	Alle hendelser knyttet til tilgang – herunder anmodninger om tilgang – må være systematisk registrert. Brukertilgang til nettbaserte arkivtjenester skal imidlertid ikke være gjenstand for registrering.	*B6.2*
59	Det må praktiseres en politikk for tilgang som er i samsvar med fastsatte regler og inngåtte avtaler for de enkelte arkivpakker, og brukere med innvilget tilgang må få sin identitet validert.	*B6.3*
60	Det må finnes mekanismer for å validere og logge faktisk tilgang. Det må også eksistere mekanismer for å sikre at informasjon ikke endres eller ødelegges ved intern eller ekstern tilgang.	*B6.4*
61	Versjoner som genereres for å tilgjengeliggjøres som brukspakker, må omfatte den informasjonen som brukerne har bedt om, eller er blitt innvilget tilgang til.	*B6.7-8*
62	Brukere må kunne ha tillit til at de har en autentisk kopi av det originale objektet, eller at det lar seg spore tilbake til det originale objektet. I tilfeller hvor brukere uttaler behov for det, bør det være mulig å demonstrere hvordan brukspakken er konstruert på grunnlag av den eller de aktuelle arkivpakkene.	*B6.10*

C. Teknologier, teknisk infrastruktur og sikkerhet

	Infrastruktur på systemnivå (TRAC C1)	
63	Lagringssystemene for den bevarte digitale arkivbestanden må være velegnet for formålet, og godt supportert. Prosessene, maskinvaren og programvaren for sikkerhetskopiering må håndtere den samlede arkivbestanden på en tilfredsstillende måte.	*C1.1-2*
64	Alle (identiske) kopier av lagringssystemets bevarte objekter må kunne lokaliseres. Det må finnes mekanismer som sikrer synkronisert lagring av objekter og kopier.	*C1.3-4*
65	Alle former for korrumpering eller tap av data må detekteres umiddelbart, også feil ved migrering eller synkronisering av kopier. Alle former for korrumpering eller tap av data må loggføres og rapporteres. Også alle tiltak for å restituere eller erstatte data i slike feilsituasjoner må loggføres. Prosedyrene for å gjenopprette data og standardene for å måle effekten av disse prosedyrenes bør være dokumenterte.	*C1.5-6*
66	Det bør finnes en plan for utskifting av utstyrskomponenter basert på en vurdering av deres levetid, og foreligge opplegg for å iverksette mediemigrering. Det bør også være foretatt beregninger av hvor lang tid migreringen vil ta.	*C1.7*
67	En prosess for å identifisere og håndtere kritiske forandringer i systemopplegg og prosedyrer som kan svekke Arkivverkets evne til å ivareta sine bevaringsoppgaver, må være definert og dokumentert.	*C1.8*
68	En prosess for forhåndstesting av kritiske endringer som skal gjøres i lagringssystemet, bør være definert og dokumentert. Det må være definert en egen prosess for å vurdere og respondere på tilgjengelige oppdateringer av sikkerhetsprogramvare. Hver implementert oppdatering må være dokumentert, og det må finnes opplysninger om prosessens resultat.	*C1.9-10*
	Hensiktsmessige teknologier (TRAC C2)	
69	Arkivverket må ha en maskin- og programvareutrustning som er velegnet og tilpasset for oppgavene med å forvalte den digitale arkivbestanden. Virksomheten må ha etablerte prosedyrer for drift og monitorering, og kunne vurdere når det er behov for teknologiske endringer.	*C2.1-2*
	Sikkerhet (TRAC C3)	
70	Det må være foretatt en systematisk analyse av risiko- og sikkerhetsaspekter knyttet til lagrede data, systemer, personell og fysiske forhold, og denne analysen må holdes kontinuerlig a jour.	*C3.1*
71	Det må være iverksatt tiltak for å håndtere alle definerte sikkerhetsbehov på en adekvat måte, jf. ISO 17799.	*C3.2*
72	Staben av medarbeiderne må være autorisert for definerte roller og ansvarsområder. Implementering av systemendringer må kreve spesiell autorisasjon.	*C3.3*

73	Arkivverket må ha en dokumentert katastrofeberedskaps- og gjenopprettings-plan. Den må omfatte minst én off-site backup av all bevart informasjon og en off-site kopi av gjenopprettingsplanen.	*C3.4*

Terminologi

Anvendte betegnelser relatert til terminologien i OAIS-standarden og TRAC:

Norsk betegnelse	***Forklaring***	***Betegnelse i OAIS og TRAC***
Arkivdokument	Informasjonsinnhold (dokument) med tilknyttede logiske metadata om opphav og kontekst	Record (Archival Record)
Arkivversjon	Arkivdokumentene som inngår i et datauttrekk for avlevering med alle tilhørende tekniske metadata og bevaringsmetadata	Ikke egen betegnelse. Her brukes de spesifiserte betegnelsene SIP, AIP og DIP, jf. nedenfor
Informasjonsinnhold	Informasjonsobjektet uten tilknyttede bevaringsmetadata	Content Information
Tekniske metadata	Beskrivelse av teknisk struktur og format	Representation Information
Bevaringsmetadata (herunder:)	Beskrivelse av materialets identitet, opp-havs/brukssammenheng og håndtering	Preservation Description Information
- kontekstopplysninger		- Context Information
- proveniensopplysninger		- Provenance Information
- integritetssikrende opplysninger		- Fixity Information
Avleveringspakke	Arkivversjon med tilhørende dokumentasjon slik den overføres fra arkivskaper og mottas av depot	SIP – Submission Information Package
Arkivpakke	Arkivversjon slik den blir bevart av depot	AIP – Archival Information Package
Brukspakke	Arkivversjon slik den gjøres tilgjengelig for bruk av depot	DIP – Dissemination Information Package

Spesifikke krav til Arkivverkets forvaltning av digitalt skapt arkivmateriale i tilknytning til digitalt depot

Nedenfor foretas en videre spesifisering av utvalgte momenter i vedlegg 1: Kravspesifikasjon til Arkivverkets arbeid med digitalt skapt arkivmateriale. Utvalget er begrenset til temaer med direkte relevans for oppgavene i tilknytning til Arkivverkets digitale depot. Oversikten konsentrerer seg om momenter som forutsettes å utgjøre sentrallinjen i et rutineopplegg med hovedfokus på integritetssikring. Oversikten følger ikke opp temaer i vedlegg 1 som gjelder tilrettelegging for bevaring, krav til arkivskapere, rutiner for journalføring og Asta-registrering av aksesjoner. Bruksversjoner av materiale i digitalt depots ytre sone behandles heller ikke.

Høyre kolonne (K-ref.) gir referanser til kravspesifikasjonen i vedlegg 1.

		K-ref:
	Overordnede krav til integritets- og konfidensialitetssikring	
1	Deponert og avlevert digitalt arkivmateriale må håndteres innenfor strengt kontrollerte omgivelser. Arkivverkets kontrollregime må omfatte forvaltningen av arkivversjoner fra og med mottak, og gjøre det mulig å verifisere: c) at bevart informasjonsinnhold fortsatt samsvarer med mottatt innhold, d) at bare autoriserte personer har hatt tilgang til materiale, e) at kopiering av materiale utelukkende er foretatt for autoriserte formål.	*31-32*
	Aksesjon av arkivversjoner – Håndtering ved mottak	
2	Umiddelbart etter mottak av en avleveringspakke må to prosedyrer utføres kombinert for å muliggjøre en verifisering av at integritets- og konfidensialitetskravene under punkt 1 er oppfylt: a) For avleveringspakken genereres en samlet sjekksum[2]. b) Avleveringspakken kopieres til eget område for initiell kontroll (mottakskontroll), herunder virus-sjekk. Lagringen må verifiseres. Begge operasjonene skal være attestert av to personer. Området for mottakskontroll skal være fysisk frittstående i forhold til lagringssystemene i digitalt depot, men tilgang til og kopiering av materiale som ligger på dette området, må være underlagt de samme styrings- og loggingsfunksjoner som materiale i DSM, jf. punkt 13. Påfølgende testing av materialet skal skje på eget kontrollområde innenfor digitalt depot.	*41*

[2] Dette skal også gjøres når sjekksummer medfølger fra arkivskaperen (jf. punkt 3 b) – og dessuten lar seg verifisere. I noen tilfeller kan det være naturlig å generere separate sjekksummer for informasjonsinnhold og medfølgende metadata i stedet for en samlet sjekksum, eventuelt i tillegg til den.

3	Arkivverket skal dokumentere hvordan arkivskaperen har integritetssikret avleveringspakken, eventuelt om det medfølger dokumentasjon om utført verifisering eller mekanismer for en fortsatt verifisering, f.eks.: a) opplysninger om antallet poster og eventuelt antallet dokumenter i vedkommende produksjonssystem (eller den aktuelle delen av det) for å muliggjøre kontroll av at informasjonsinnholdet er overført komplett, b) sjekksum(mer) generert ved den automatiserte produksjonen av avleveringspakkens datauttrekk for å muliggjøre kontroll av at informasjonsinnholdet ikke er endret etter fremstillingen, c) dokumentasjon som bekrefter at informasjonsinnhold er blitt kontrollert mot innholdet i vedkommende produksjonssystem, og representerer en eksakt, uendret og feilfri reproduksjon av dette. Kombinasjonen av punkt b og c gjør at informasjonsinnholdet kan bevares med status som autentisk i seg selv. Operasjonene ved mottak under foregående punkt 2 gir bare mulighet for å verifisere det basale: at informasjonsinnholdet bevares identisk med det som ble mottatt av Arkivverket.	*25-27*
4	Ved mottak av en avleveringspakke skal følgende kontrolleres: a) at arkivversjonen er tilfredsstillende autorisert av avgiveren, b) at informasjonsinnholdet er korrekt og komplett iht. fastsatte bestemmelser eller inngåtte avtaler, c) at antall poster og eventuelle dokumenter i arkivversjonen er identisk med det tilsvarende antallet i produksjonssystemet, jf. punkt 3a, d) at eventuell(e) medfølgende sjekksum(mer) verifiserer at informasjons-innholdet er uendret etter fremstillingen av arkivversjonen, jf. punkt 3b, e) at innholdet er tilknyttet de tekniske og logiske metadata som kreves for at det kan bevares med opprettholdt lesbarhet og autentisitet, f) at avleveringsbestemmelsenes format-, dokumentasjons- og mediekrav er oppfylt, g) at arkivskaperen har kontrollert medfølgende XML-filer mot tilhørende XML Schema eller DTD, h) at de tekniske referansene (identifikatorene) mellom de interne elementene i datauttrekket er konsistente og bestandige, jf. punkt 5.	*19-30 og 34*
5	Uoverensstemmelser eller mangler under punkt 4b-4f gir grunnlag for å nekte godkjenning av en avleveringspakke. Mangler under punkt 4a og 4g krever tilleggsdokumentasjon fra arkivskaperen. Om punkt 4h: Manglende referanseintegritet mellom koblede tabeller gir ikke grunnlag for godkjenningsnekt dersom medfølgende dokumentasjon (jf. punkt 3c) eller arkivskaperens oppfølgende kontroll i vedkommende produksjons-system viser at dette avspeiler en tilsvarende inkonsistens i produksjonssystem-et. Jf. i denne sammenheng også punkt 7, nedenfor. Manglende referanse-integritet mellom tabeller (metadata) og tilknyttede elektroniske dokumenter gir derimot grunnlag for å nekte godkjenning når dette forekommer gjennom-gående. Det gjelder selv om uoverensstemmelsene er originale, og kan tilbake-føres til produksjonssystemet. I slike tilfeller er primærkravet at arkivskaperen må rette referansene i produksjonssystemet, og deretter fremstille en ny	*33-38*

	avleveringspakke.	
6	Dersom Arkivverket selv foretar teknisk retting i en avleveringspakke, må dette dokumenteres. I alle slike tilfeller – også når rettingene er utført etter avtale med arkivskaperen – må den mottatte avleveringspakken bevares i DSM i tillegg til den korrigerte versjonen, jf. også punkt 12, nedenfor. Dette gjelder så sant det ikke på annen måte lar seg sikkert verifisere at rettingene faktisk er avgrenset til de dokumenterte. Rettede versjoner må integritetssikres med sjekksum på samme måte som avleveringspakker ved mottak.	*41*
7	Det må bevares dokumentasjon om alle relevante hendelser og prosesser i tilknytning til den enkelte aksesjon for å bekrefte at prosessene er forskrifts-messig gjennomført. Dersom en avleveringspakke med et teknisk inkonsistent datauttrekk likevel blir akseptert for bevaring, må dette dokumenteres særskilt, og det må klar-gjøres om manglende konsistens kan tilbakeføres til produksjonssystemet. Resultatet av Arkivverkets testing skal dokumenteres slik at det også kan tjene som informasjonsgrunnlag ved fremstillingen av bruksversjoner og ved faktisk bruk av materialet. Et godt dokumentert testresultat er spesielt viktig når manglende referanseintegritet eller annen teknisk inkonsistens vil gjøre det umulig å fremstille en ordinær bruksversjon av et datauttrekk. I slike tilfeller kan dokumentasjonen gi opplegg for alternative måter å utnytte materialet på.	*38*
	Organisering av bevarte arkivpakker i digitalt depot	
8	Når en avleveringspakke er formelt godkjent etter testing, skal den overføres fra kontrollområdet, og lagres i DSM som en original arkivpakke. Testdokumen-tasjonen skal da vedlegges arkivpakken sammen med opplysninger om aksesjonen og supplerende arkivbeskrivende informasjon (”Asta-informasjon”), jf. punkt 7. For tilleggsinformasjonen skal det produseres en egen sjekksum. Dette gjøres for å unngå en endring av avleveringspakkens tidligere integritetssikrede innhold.	*39-49*
9	En original arkivversjon (avleveringspakke) som innlemmes i DSM, skal organiseres som en samlet arkivpakke med følgende komponenter: I. En overordnet definisjon som identifiserer pakken, gir en fortegnelse over innholdet og beskriver hvordan komponentene er sammenkoblet II. Arkivdokumentet, dvs. pakkens ”record” eller ”records” a) Bevaringsmetadata - Arkivbeskrivelse, proveniens- og kontekstinformasjon - Dokumentasjon om opprinnelig systems prosesser og bruk - Logiske (autentiserende) metadata - Aksesjon, bevaringsstatus (deponert/avlevert), klausuler mm. - Testdokumentasjon - Utførte operasjoner i depot (justeringer/tillegg i tekniske metadata eller transformering ved konvertering) b) Informasjonsobjektet – original representasjon - Informasjonsinnhold (datauttrekket) - Tekniske metadata	*39-40*

	- Sjekksum(mer), separate kategorier for algoritme og hashverdi c) Evt.: Informasjonsobjektet – konvertert/justert representasjon - underkategorier som II b III. Integritetssikring og tilgangsstyring - integritetssikring (med separate kategorier for sjekksummens algoritme og hashverdi) gjelder her pakken som helhet, og skal være fysisk plassert utenfor pakken.	
10	Det må anvendes regler for navngiving som gir synlige, bestandige og unike identifikatorer for alle objektene i en arkivpakke. Navngivingen skal være basert på URN.	*43*
11	Sjekksummer må være lagret på en beskyttet måte. Sjekksummer for å ivareta integritetssikring (bit-integritet) i depot skal både være knyttet til informasjonsinnholdet (som i OAIS-standarden) og til arkiv-pakken som helhet, jf. punkt 9. På objektnivå skal egne sjekksummer være tilknyttet henholdsvis informasjonsinnhold og metadata. Integriteten vil dermed ikke brytes dersom det foretas endringer eller tilføyelser i bevaringsmetadata (punkt 9, II a). Endringer i bevaringsmetadata gjør det imidlertid nødvendig å resignere arkivpakken som helhet. Genereringen av ny pakkesjekksum skal da registreres blant ”Utførte operasjoner i depot” (punkt 9, II a).	*41*
12	Dersom det gjøres endringer i en arkivpakkes informasjonsinnhold eller metadata, skal det genereres et nytt rettet og signert informasjonsobjekt som bevares i tillegg til det opprinnelige og med lenke til dette (jf. punkt 9, II c). Alternativt skal en ny arkivpakke genereres og lenkes til den opprinnelige. Denne prosedyren skal alltid brukes når Arkivverket foretar ordinære rettinger – ved mottak eller senere. Prosedyren ovenfor skal også brukes dersom det foretas en normalisering av datauttrekk, f.eks. fra eldre databasestruktur til relasjonell form, og dersom det foretas en gjennomgående formatkonvertering av lagrede dokumenter i DSM. Ved gjentatt formatkonvertering skal likevel bare de to nyeste versjonene beholdes i tillegg til det opprinnelige objektet som inneholder avleverings-pakken (SIP-delen). Dette gjelder under forutsetning av at det brukes standardiserte og dokumenterte prosesser for slik konvertering, at prosessene blir gjennomført kontrollert og uten rapporterte feil, og at de blir registrert som ”Utførte operasjoner”, jf. punkt 9, II a. Migreringer som består i en flytting av objekter mellom lagringsenheter, medfører ingen endring av informasjon. Men gjennomførte migreringer skal verifiseres og dessuten dokumenteres som ”Utførte operasjoner”. Annet ledd ovenfor lemper på TRAC-kravet om at samtlige versjoner av objekter eller arkivpakker må beholdes etter gjentatte konverteringer for å gjøre prosessene fullstendig ettersporbare (TRAC B4.2-3). Men det støtter seg samtidig på sentrale forutsetninger i TRAC B2.3 og B2.11.	*41, 52*
13	Mekanismer for validering og logging av tilgang må finnes på objektnivå, og være knyttet til den enkelte arkivpakke, jf, punkt 9, III. Kopiering av informasjonsinnhold må logges særskilt.	*60*

14	Det må finnes mekanismer som sikrer at informasjon bare kan endres eller slettes ved spesielle prosedyrer og med spesiell autorisasjon.	*60*
	Sentrale styrings- og monitoreringsfunksjoner	
15	Det må finnes systemer for å identifisere alle lagrede arkivpakker i digitalt depot og informasjonsobjektene i dem. Systemet for å administrere lagrings-systemet må kunne aksessere informasjonsobjektene for å utføre monitorerings-funksjonene under punkt 16-19.	*63, 64*
16	Det må finnes funksjoner for å overvåke den samlede arkivbestanden, og bekrefte at den faktisk omfatter de arkivpakker som skal finnes der – og bare disse.	*53*
17	Arkivpakkenes opprettholdte integritet må være gjenstand for en aktiv monitorering. Det må eksistere en logg for kontrollen av sjekksummer.	*53*
18	Det må finnes mekanismer for monitorering som varsler om fare når formater og tekniske metadata er i ferd med å bli teknologisk forgjengelige.	*51*
19	Administrasjonssystemet må umiddelbart detektere korrumpering eller tap av data, også feil ved migrering eller synkronisering av kopier på tape-roboter. Alle former for korrumpering eller tap av data må loggføres og rapporteres. Også alle tiltak for å restituere eller erstatte data i slike feilsituasjoner må loggføres. Det må finnes etablerte prosedyrer for å gjenopprette data. Standardene for å måle effekten av disse prosedyrene bør være dokumenterte.	*65*
	Driftsopplegg og driftssikkerhet	
20	IT-avdelingen må ha minimum 3 medarbeidere med kompetanse og særskilt autorisasjon for drift av SAN-systemet. En av disse skal være utpekt som systemansvarlig. Det må være definert roller som: - ansvarlig for tilsyn av sikkerhetskopieringen (tape-roboter), - oppfølgingsansvarlig for monitorerings- og loggingsfunksjoner, - ansvarlig for migrering til nye disker iht. fastsatt utskiftingsplan.	*1*
21	Bare medarbeidere med egen autorisasjon og adgangskort skal ha fysisk tilgang til DSMs datarom. Medarbeidere skal aldri ha tilgang til fysisk magasin alene. Den fysiske adgangskontrollen må være arrangert slik at det alltid kreves to personer for å få tilgang. En av disse må være autorisert for drift. Fysisk tilgang til digitalt magasin skal også logges.	*71, 72*
22	Informasjonen i DSM skal bare være tilgjengelig i et eget, lukket nett. Medarbeidere med kontorarbeidsplasser som er tilknyttet dette nettet, skal ikke ha mulighet for å kommunisere med utstyr i Arkivverkets åpne nett.	*70-72*
23	Medarbeidere med nettaksess til DSM må være autorisert for definerte roller og arkivfaglige ansvarsområder. Det må bl.a. være definert roller som: - ansvarlig for (arkivfaglig) vedlikehold av selve arkivbestanden - ansvarlig for (Elark-seksjonens) innledende kontroll ved mottak, - ansvarlig for å gjennomføre program for å innlemme/konvertere nåværende	*70-72*

	arkivbestand på CD-er til DSM.	
24	Det må finnes en dokumentert katastrofeberedskaps- og gjenopprettingsplan. Den må omfatte en off-site kopi av all bevart informasjon og en off-site kopi av gjenopprettingsplanen. Inntil avtaler om dette foreligger, skal kopiene lagres i magasin 2E.	*73*

Sikkerhetstiltak basert på en risiko- og sårbarhetsanalyse av system-, drifts- og rutine-opplegg i tilknytning til Arkivverkets lagringssystem for digitalt skapt arkivmateriale[3]

Sannsynlighet: *Svært stor* = (kan inntreffe) flere ganger pr. år, *Stor* = årlig, *Sannsynlig* = år om annet (på lang sikt), *Liten* = en gang pr. 50-100 år
Konsekvens: *Katastrofal, Kritisk, Alvorlig, Lite farlig*

A. Informasjonssikkerhet i digitalt sikringsmagasin (DSM)

	Hendelse	*Sannsynlighet*	*Konsekvens*	*Tiltak*
1	Installasjoner og lagret informasjon i DSM ødelegges som følge av: - brann - sabotasje eller terroranslag, - elektromagnetisk puls - tilsiktede handlinger av egne ansatte med administrasjons- eller tilgangsrettigheter.	Liten	Katastrofal	I tillegg til den fysiske sikringen av datarom i fjellmagasin skal følgende tiltak være iverksatt for å muliggjøre restituering av informasjon: - Informasjonsobjektene lagres i 3 identiske eksemplarer på 2 ulike teknologier (disk og tape) i separate magasinrom. - En ekstra tape-kopi lagres off-site.
2	Feil ved strømforsyning eller kjølingssystem resulterer i skade på anlegg og tap eller korrumpering av lagret informasjon.	Sannsynlig	Kritisk	Strømforsyningen skal være redundant, og kjølingssystemet skal være monitorert. Jf. ellers punkt 1: restituering av informasjon.
3	Lagrede informasjonsobjekter går tapt eller blir korrumpert uten at dette kan tilbakeføres til dramatiske hendelser som under punkt 1 og 2.	Sannsynlig	Kritisk	Det skal finnes mekanismer for monitorering som viser om objektene er bevart uendret og komplett, jf. punkt 7. Tapte og korrumperte objekter skal kunne restitueres, jf. punkt 1.
4	Uautoriserte personer trenger seg fysisk inn i DSMs datarom i fjellmagasin.	Liten	Kritisk	Datarom skal ha adgangskontroll basert på nøkkelkort. Tilgang til datarom krever 2 personer. Tilgang skal valideres og logges.

[3] Tiltakene (høyre kolonne) er av forebyggende karakter. Det er behov for å supplere oversikten med referanser til oppfølgingstiltak dersom uønskede hendelser inntreffer. Slike oppfølgingstiltak forutsettes å være beskrevet i en beredskaps- og katastrofeplan.

	Hendelse	*Sannsynlighet*	*Konsekvens*	*Tiltak*
5	Uautoriserte personer skaffer seg tilgang til DSM-installasjoner via kommunikasjonslinjer.	Sannsynlig	Alvorlig	Informasjonsobjekter i DSM skal bare være tilgjengelige for autoriserte personer i lukket og sikret nett. Kontorarbeidsplasser tilknyttet dette nettet skal ikke kunne kommunisere med annet utstyr. All tilgang til informasjon skal logges.
6	Gradert informasjon i DSM blir tilgjengelig for andre enn de personer som er særskilt autorisert for tilgang.	Liten	Alvorlig	Gradert informasjon skal lagres på frittstående, dedikert utstyr i eget, sikret datarom, og bare være tilgjengelig her – for særskilt autoriserte.
7	Lagrede informasjonsobjekter i DSM blir endret på uautorisert måte.	Sannsynlig	Alvorlig	Sjekksummer skal ivareta integritetssikring. Objekter skal bare kunne endres (og slettes) ved spesiell autorisasjon. Endringer skal logges og monitoreres. Objekter i original mottatt versjon skal ikke kunne endres. Alternative, endrede versjoner skal da lagres som tillegg.
8	Nye informasjonsobjekter blir på uautorisert måte innlemmet og lagret i DSM.	Sannsynlig	Alvorlig	Nye arkivversjoner (arkivpakker) som lagres i DSM, skal ha sjekksum(mer) og være attestert av 2 autoriserte personer.
9	Informasjonsobjekter i DSM blir kopiert på uautorisert måte.	Sannsynlig	Alvorlig	Kopiering av objekter skal logges.
10	Informasjonsobjektene som er lagret i DSM, lar seg ikke fremsøke samlet eller enkeltvis.	Liten	Alvorlig	Administrasjonssystemet skal både kunne lokalisere samlede arkivpakker og objekter i hver dem – ut fra relevante kriterier.
11	Sjekksummer blir ikke lagret på en beskyttet måte.	Sannsynlig	Alvorlig	Sjekksummer skal være sikkert lagret – atskilt fra de tilknyttede informasjonsobjektene.
12	Tilgangslogg eller logg for kontroll av sjekksummer blir manipulert og endret.	Liten	Kritisk	Logger skal være integritetssikret slik at ingen har autorisasjon for å endre dem.

	Hendelse	*Sannsynlighet*	*Konsekvens*	*Tiltak*
13	Informasjonsobjektenes opprettholdte integritet lar seg ikke monitorere.	Liten	Kritisk	Objekter skal ikke kunne innlemmes, endres eller migreres uten å være tilknyttet informasjon for monitorering.
14	Verifisering etter migrering av informasjonsobjekter til nytt lagringsmedium blir ikke utført.	Sannsynlig	Alvorlig	Migrering skal logges, og kunne verifiseres og dokumenteres automatisert av systemet.
15	Migreringer, konverteringer og andre utførte vedlikeholdsoperasjoner på lagrede informasjonsobjekter lar seg ikke detektere.	Sannsynlig	Alvorlig	Forutsetningen er at slike operasjoner blir dokumentert på foreskrevet måte. Operasjonene skal logges, og det skal være definert en egen tilsynsrolle for denne typen operasjoner.
16	En samlet migrering av arkivbestanden til nye lagringsmedier (disker) lar seg ikke gjennomføre i løpet av medienes levetid (garantitid) på 3-5 år.	Liten	Kritisk	Før oppstart av DSM må det være utarbeidet en prognose som klargjør at migreringsbehovet ikke overskrider systemets migreringskapasitet.
17	Lagringssystemets informasjon om de bevarte objektene er teknologibundet på en slik måte at den ikke lar seg migrere til et annet lagringssystem.	Liten	Katastrofal	Informasjonsobjektene skal være slik organisert og formatert at de uten videre kan overføres til et annet lagringssystem. Systemets styringsinformasjon og sentrale oversikt over lagrede objekter skal kunne konverteres og migreres.
18	Feil ved lagring, verifisering, migrering eller synkronisering av kopier på tape-roboter blir ikke systematisk loggført og rapportert	Sannsynlig	Kritisk	Det skal defineres en rolle med tilsyns- og oppfølgingsansvar for lagring, migrering og tape-kopiering i DSM.
19	HW- eller SW-feil i DSM blir ikke systematisk loggført og rapportert.	Sannsynlig	Alvorlig	Jf. punkt 18.
20	Kopiering til tape (tape-roboter og off-site lagring) blir ikke utført. Evt.: kopier lar seg ikke verifisere.	Sannsynlig	Kritisk	Jf. punkt 18.

	Hendelse	*Sannsynlighet*	*Konsekvens*	*Tiltak*
21	Administrasjonsavdelingen makter bare periodevis å følge opp oppgavene i forbindelse med bruker-autorisasjon og adgangskontroll (inkl. logging eller varsling av hendelser knyttet til tilgang).	Stor	Kritisk	En bemanningsplan skal finnes til enhver tid, og sikre at funksjonene er kontinuerlig bemannet.
22	IT-avdelingen har ikke driftspersonell med nødvendig kompetanse for å operere DSM.	Stor	Kritisk	Opplæring – før lagringssystemet tas i bruk.
23	IT-avdelingen har ikke tilstrekkelig bemanning for å ivareta de roller og funksjoner som kreves for å forvalte DSM.	Svært stor	Kritisk	En bemanningsplan skal finnes til enhver tid. Roller for følgende spesifikke ansvarsområder skal være fylt (eventuelt i kombinasjon): - SAN-adminstrasjon og systemdrift - Hardware-vedlikehold og -utskiftning iht. utviklingsprogram - Monitorering/overvåking av funksjoner - Operasjons- og hendelseslogger til bruk for oppfølgingen av adgangskontroll (jf. punkt 21) og kvalitetssikring (jf. punkt 59) - Tilsyn/betjening av tape-roboter, herunder synkronisering av kopiversjoner - Off site sikkerhetskopi (egen og NBs) - Migrering og migreringsprogram - Ansvar for dokumentasjon av driftsrutiner og dokumentasjon av driftshendelser - Ansvar for planlegging og prognoser

B. Aksesjon av arkivversjoner (avleveringspakker) – Håndtering ved mottak

	Hendelse	*Sannsynlighet*	*Konsekvens*	*Tiltak*
24	Avleveringspakker blir kompromittert eller kommer på avveier ved sending/overføring.	Sannsynlig	Alvorlig	Kryptert lagring ved overføring(?)
25	Avleveringspakker kommer til ikke-autoriserte personer eller på avveier i forbindelse med mottak.	Sannsynlig	Kritisk	Definerte mottaksrutiner skal sikre at bare autoriserte personer håndterer materialet. Det skal finnes en rolle som ansvarlig for mottak og fordeling til behandlingsansvarlige.
26	Avleveringspakker inneholder ondsinnet programvare	Sannsynlig	Alvorlig	Virus-kontroll skal alltid utføres ved mottak.
27	Avleveringspakker blir ikke integritetssikret på autorisert måte og beskyttet ved mottak slik at det senere lar seg verifisere at bevart informasjonsinnhold samsvarer med mottatt innhold.	Stor	Kritisk	Avleveringspakker skal umiddelbart ved mottak lagres integritetssikret med sjekksum på eget kontrollområde. Verifisering mot den mottatte versjonen skal utføres. Operasjonene skal attesteres av 2 autoriserte personer.
28	Avleveringen/deponeringen blir ikke journalført i ePhorte og registrert som tilvekst i Asta.	Sannsynlig	Lite farlig	Ansvarlig for mottak og koordinator for testing skal kontrollere utført registrering.
29	Det blir ikke utført tilfredsstillende kontroll av at avleveringspakken er overført iht. bestemmelser og avtaler, at innholdet er i samsvar med generelle eller spesifikke BK-bestemmelser og at nødvendige administrative og tekniske metadata følger vedlagt.	Sannsynlig	Alvorlig	Det skal være definert en rolle som (tilsyns)-ansvarlig for å utføre slik innledende kontroll av innholdselementer mot inngåtte avtaler og fastsatte bestemmelser. Denne rollen skal også være tillagt oppfølgingsansvaret for tilgangs-føringen, jf. punkt 28.
30	Det blir ikke utført tilfredsstillende identitets- og integritetskontroll av det mottatte materialet med utgangspunkt i arkivskapers/avgivers dokumentasjon og (evt.) medfølgende verifiseringsmekanismer.	Sannsynlig	Alvorlig	Identitets- og integritetskontroll skal utføres og dokumenteres av den ansvarlige for innledende mottakskontroll. Dersom avleveringspakken ikke er fullgodt attestert av arkivskaper, skal dette avkreves.

	Hendelse	*Sannsynlighet*	*Konsekvens*	*Tiltak*
31	Avleveringspakker mottas i et omfang og med en frekvens som overskrider Arkivverkets kapasitet for mottakshåndtering og godkjenningskontroll.	Sannsynlig	Kritisk	Omfanget av avleveringene skal reguleres i samsvar med Arkivverkets mottakskapasitet gjennom de avleveringsavtaler som inngås.
32	Arkivskaper eller annen avgiver responderer ikke på forespørsler eller krav som fremmes som ledd i Arkivverkets godkjenningsvurdering.	Sannsynlig	Lite farlig	Det skal fastsettes frister for arkivskapers tilbakemelding.
33	Teknisk godkjenningskontroll av materialet iht. avleveringsbestemmelsene §§ 8-10 til 8-28 og 8-31 til 8-34 blir ikke utført, eller kontrollen stilles i bero uten å være ferdigstilt, og uten at Arkivverket formelt frasier seg ansvaret for materialet.	Stor	Alvorlig	Det skal være etablert oppfølgingsrutiner for å sjekke behandlingsstatus for alt materiale i mottaksfasen. Med mindre kontrollen stilles i bero etter avtale med arkivskaper eller pga. gjennomføringsproblemer (jf. punkt 34), skal den som hovedregel avsluttes uten godkjenning hvis den ikke kan ferdigstilles på vanlig måte.
34	Arkivverket mangler egnet verktøy for å utføre en tilfredsstillende teknisk godkjenningskontroll	Stor	Alvorlig	Tiltakene under punkt 29-30 skal gjennomføres. Det skal foretas teknisk kontroll så langt tilgjengelig verktøy tillater. Resterende kontroll stilles i bero inntil verktøy foreligger.
35	Arkivverket må akseptere å bevare mottatt materiale som ikke er kvalifisert for godkjenning, evt. materiale som ikke har vært gjenstand for kontroll, fordi det har gått uakseptabel lang tid siden overføringen, og fordi saken heller ikke er spilt tilbake til arkivskaper i form av forespørsel, krav eller andre forbehold.	Stor	Alvorlig	Jf. punkt 33 og 41.
36	Den tekniske godkjenningsvurderingen blir basert på krav som er for strenge og detaljerte i forhold til avleveringsbestemmelsenes krav – med det resultat at arkivversjoner som burde vært godkjent, blir avvist.	Stor	Alvorlig	Beslutninger etter utført kontroll skal autoriseres ved intern instansbehandling. Beslutninger kan likevel delegeres til kontrollansvarlige forutsatt at kontrollen gjennomføres etter et autorisert oppsett for vedkommende oppgave.

	Hendelse	*Sannsynlighet*	*Konsekvens*	*Tiltak*
37	Den tekniske godkjenningsvurderingen blir basert på krav som ikke er strenge og detaljerte nok i forhold til avleveringsbestemmelsenes krav – med det resultat at arkivversjoner med feil eller mangler blir godkjent.	Stor	Alvorlig	Tiltak som punkt 36.
38	Sjekksum som medfølger fra arkivskaperen (jf. punkt 30) og/eller sjekksum som er generert ved mottak (jf. punkt 27) lar seg ikke verifisere etter operasjoner som er foretatt i forbindelse med godkjenningskontrollen.	Sannsynlig	Kritisk	Systemtekniske låser skal prinsipielt forhindre en slik korrumpering av data, men en oppfølgende verifisering skal likevel foretas. Ved samsvarsfeil må den mottatte avleveringspakken kopieres til DSMs kontrollområde på ny, og integritetssikres iht. punkt 27.
39	Det lar seg ikke verifisere at retting i avleveringspakker som medarbeidere i Arkivverket selv måtte ha foretatt ved en godkjenningskontroll – evt. etter avtale med arkivskaper – faktisk er avgrenset til de endringer som er angitt og dokumentert.	Sannsynlig	Kritisk	Den mottatte avleveringspakken skal alltid bevares i original, uendret versjon, jf. punkt 7 og 27. Dersom det foretas rettinger, skal disse lagres som egne metadata- eller innholdsobjekter i tillegg til de originale. Utførte endringer skal dokumenteres
40	Resultatet av den tekniske godkjenningsvurderingen er ikke fullgodt dokumentert.	Sannsynlig	Alvorlig	Testrapport skal medfølge som bevaringsmetadata
41	Avleveringspakker som blir akseptert for bevaring tross påviste feil eller mangler ved godkjenningskontrollen, blir lagret uten vedlagt dokumentasjon som identifiserer og forklarer feilene.	Sannsynlig	Lite farlig	Feil eller mangler skal dokumenteres i bevaringsmetadata
42	Det lar seg ikke verifisere at mottatt avleveringspakke som er kopiert til DSMs kontrollsone, er lagret uendret, og at den senere ikke uautorisert er erstattet med en annen versjon eller slettet. jf. punkt 27.	Sannsynlig	Kritisk	Lagringssystemet skal ha funksjoner for monitoring og verifisering på objektnivå. Avleveringspakker i original mottatt versjon skal ikke kunne endres etter mottak, jf. punkt 7.

	Hendelse	*Sannsynlighet*	*Konsekvens*	*Tiltak*
43	Det lar seg ikke verifisere at utelukkende autoriserte personer har hatt tilgang til et spesifikt informasjons-objekt i DSMs kontrollsone.	Sannsynlig	Alvorlig	Lagringssystemet skal ha funksjoner for styring og logging av tilgang på objektnivå, jf. punkt 5.
44	Det lar seg ikke detektere om et spesifikt informa-sjonsobjekt i DSMs kontrollsone har vært gjenstand for kopiering (av autorisert person).	Sannsynlig	Alvorlig	Lagringssystemet skal ha funksjoner for å styre og logge kopiering på objektnivå, jf. punkt 9.
45	Arkivskaper blir ikke tilsendt kvittering for mottatt avleveringspakke.	Sannsynlig	Lite farlig	Kontroll skal utføres av ansvarlig for mottak og oppgavefordeling.
46	Arkivskaper blir ikke tilsendt formell melding om utfallet av godkjenningsvurderingen.	Sannsynlig	Alvorlig	Kontroll skal utføres av ansvarlig for mottak og oppgavefordeling.
47	Arkivverket kan ikke lokalisere mottatt avleverings-pakke eller fremskaffe oversikt over behandlings-status for mottatte avleveringspakker som ikke er godkjent etter testing (testrestanser).	Sannsynlig	Kritisk	Arkivverket skal ha systemer for dette formålet, og det skal være etablert roller og rutiner for å holde systemene a jour til enhver tid.
48	Arkivverket kan ikke produsere en samlet oversikt over alt digitalt arkivmateriale som det må innestå for å ha mottatt, og ikke fremskaffe oversikt over de respektive ansvarlige for pågående og utført mottaks-kontroll.	Sannsynlig	Kritisk	Jf. tiltak 47.

	Hendelse	*Sannsynlighet*	*Konsekvens*	*Tiltak*
49	Nødvendige roller knyttet til aksesjon og mottaks-kontroll er ikke etablert og fylt.	Stor	Kritisk	Roller for følgende funksjonsområder skal være ivaretatt (eventuelt i kombinasjon): - ansvar for mottak og oppgavefordeling - ansvar for innledende kontroll av avleveringspakker - ansvar for teknisk kontroll - ansvar for autorisasjon av beslutninger om godkjenning - ansvar i forhold til SAH, SAK og SAKO - behandlingsansvar – innledende kontroll - behandlingsansvar – teknisk kontroll

C. Forvaltning av arkivpakker i digitalt sikringsmagasin (DSM)

	Hendelse	*Sannsynlighet*	*Konsekvens*	*Tiltak*
50	Avleveringspakke er ikke blitt overført fra kontroll-området etter mottakskontroll og innlemmet i DSM som en arkivpakke.	Sannsynlig	Lite farlig	Innlemmelsen i DSM skal utføres eller auto-riseres av ansvarlig koordinator for teknisk kontroll. Operasjonen skal attesteres av den ansvarlige for vedlikehold eller annen autorisert person, og logges.
51	Arkivpakke er blitt innlemmet i DSM uten å være fullgodt dokumentert og /eller riktig organisert.	Sannsynlig	Alvorlig	En arkivpakke skal omfatte selve informa-sjonsobjektet med tekniske og logiske meta-data, bevaringsmetadata med bl.a. arkiv-beskrivelse og testdokumentasjon, integritets-sikrende informasjon og pakkens overordnede definisjon. Organiseringen skal gjøre det mulig for administrasjonssystemet å aksessere og monitorere nøkkelopplysninger. Det skal være definert en rolle som ansvarlig

	Hendelse	*Sannsynlighet*	*Konsekvens*	*Tiltak*
				for kvalitetssikring av dokumentasjon.
52	(Fil)referansene til objektene i en arkivpakke fungerer ikke.	Sannsynlig	Alvorlig	Navngivingen skal være basert på URN for å gi unike, synlige og bestandige identifikatorer.
53	Opplysninger om innlemmet arkivpakke i DSM er ikke lagt inn i SAN-administrasjonssystemet, og pakken kan derfor ikke identifiseres og monitoreres.	Sannsynlig	Alvorlig	Den ansvarlige for kvalitetssikring av dokumentasjon skal utføre etterkontroll av SAN-opplysningene. SAN-administrasjonssystemet skal kunne detektere uidentifiserte objekter i DSM.
54	Fra SAN-administrasjonssystemet lar det seg ikke påvise om en arkivpakke er blitt supplert med informasjon, eller om innhold har vært gjenstand for migrering, endring eller konvertering.	Sannsynlig	Alvorlig	En arkivpakke skal inneholde opplysninger om utførte operasjoner, og disse skal kunne monitoreres fra SAN-systemet. SAN-systemet har loggingsfunksjoner mm. som også gjør det mulig å detektere migreringer eller endringer i tilfeller hvor dette ikke er blitt dokumentert. Rutinemessig kontroll skal utføres av ansvarlig for kvalitetssikring av dokumentasjon
55	Verifisering av arkivpakkers opprettholdte integritet etter migreringer og vedlikeholdsoperasjoner blir ikke utført.	Sannsynlig	Kritisk	Kontroll skal utføres av ansvarlig for kvalitets-sikring av dokumentasjon
56	Det lar seg ikke verifisere at en arkivpakkes informasjonsinnhold er bevart uendret gjennom migreringer og andre vedlikeholdsoperasjoner i DSM, og fortsatt samsvarer med innholdet som ble mottatt fra vedkommende arkivskaper.	Sannsynlig	Kritisk	I arkivpakker skal opprinnelig mottatt informasjonsinnhold og medfølgende metadata utgjøre egne objekter med tilknyttede sjekk-summer. Ved en slik organisering vil disse objektene være bevart uendret og i en fortsatt verifiserbar form selv om andre objekter i arkivpakken eller arkivsamlepakken oppdateres eller suppleres.

	Hendelse	*Sannsynlighet*	*Konsekvens*	*Tiltak*
57	Informasjonsobjekter i DSM er ikke lenger tilfredsstillende lesbare fordi lagringsformatet (dokumentformatet) er foreldet, og ikke støttes av oppdatert fremstillingsverktøy.	Sannsynlig	Alvorlig	SAN-systemet skal ha monitoreringsfunksjoner for å skaffe oversikt over forekomsten av formater som trues av forgjengelighet. Det skal finnes en instans for å vedta nødvendige gjennomgående formatkonvertinger.
58	Det skapes tvil om dokumenters og info-objekters opprettholdte integritet og pålitelighet etter at det er blitt foretatt en gjennomgående konvertering av et eldre dokumentformat (evt. tekstfilformat) til et nytt i DSM.	Sannsynlig	Kritisk	Sjekksum kan ikke bekrefte opprettholdt innholdsintegritet etter en formatkonvertering. Opprinnelig mottatt informasjonsinnhold skal derfor alltid beholdes (i originalformat) etter en konvertering. Ved en påfølgende ny konvertering skal imidlertid bare de to versjonene beholdes i tillegg til den opprinnelige . Dette gjelder under forutsetning av at det brukes standardiserte og dokumenterte prosesser, at prosessene gjennomføres kontrollert og uten rapporterte feil, og at de dokumenteres som utførte operasjoner.
59	Nødvendige roller for kvalitetssikring og vedlikehold av opplysninger i DSM er ikke etablert og fylt.	Stor	Kritisk	Roller for følgende funksjonsområder skal være fylt (eventuelt i kombinasjon): - ansvar for teknisk kontroll og verifisering - ansvar for kopiering til og fra DSM - ansvar for vedlikehold av arkivpakker - ansvar for kvalitetssikring av dokumentasjon (herunder Asta-oppdatering) - ansvar for planlegging og prognoser - behandlingsansvar (med generelle tilgangs- og registreringsrettigheter)

SAN-administrasjonssystemet - informasjonselementer og egenskaper

Prosjektet legger til grunn at systemet for SAN-administrasjon skal være et standard-produkt. Oversikten nedenfor omfatter primært informasjon som administrasjonssystemet forutsettes å ha tilgang til. Når denne informasjonen ikke genereres av SAN-systemet, må den gjøres tilgjengelig for SAN-systemet av forvaltningssystemet for digitalt depot.

1. Identifikasjon av arkivpakke i SAN
   - Pakke-ID (URN)
   - Tabell som kobler ID med fysisk plassering (oppdateres fra forvaltningssystemet)
   - Type (mottatt SIP, AIP, DIP, AIC)

2. Opplysninger om aksesjon
   - Arkivpakke (AIP, AIC) generert og lagret dato
   - Tape-versjoner generert og lagret dato
   - Verifisering av versjoner ved lagring/kopiering

3. Referanser
   - Referanser mellom digitale objekter på disk og tape-kopier
   - Ingen opplysninger om forbindelser mellom arkivobjekter (AIC-er og DIP-er), men de enkelte arkivobjekter forutsettes å kunne identifiseres ut fra Pakke-ID
   - Ingen andre referanser til Asta enn ID (URN)

4. Tilgang
   - Bestemmelser må være knyttet til de enkelte arkivobjekter

5. Integritetssikring
   - Administrasjon/lagring av sjekksum for samlede pakker (+ algoritme)
   - Logg for generering av samlet sjekksum for pakker (evt. bare i forvaltningssystemet)
   - Logg for verifisering av samlet sjekksum for pakker
     - Utført av/dato
     - Verifisering etter migrering

6. Utførte depotoperasjoner
   - Migrering (i betydningen overkopiering)
     - Utført av/dato
     - Verifisering etter migrering
   - Transformering av arkivobjekters representasjon (evt. bare i forvaltningssystemet)
     - Type operasjon
     - Utført av/dato
     - Logg for generering og verifisering av sjekksum, jf. pkt. 5

7. Overvåking
   - Oversikt over formater som forekommer i arkivpakker (med referanser). Oversikten må også kunne aksesseres av forvaltningssystemet.
   - Logg for tilgang til og kopiering av informasjonsinnhold (samlet for alle pakker)
   - Logg for lagring av arkivpakker og endring av innhold i arkivpakker
   - Logg for overkopiering og verifisering
   - Aktiv detektering av endret innhold i arkivpakker
   - Kontroll av at verifisering er utført etter lagring av arkivpakker