



AAU Sikkerhedshåndbogen

Sikkerhedshåndbogen beskriver informationssikkerhed på forskellige områder på AAU. Indholdet er godkendt af Informationssikkerhedsudvalget og er gældende pr. 15. december 2018.

Sidst redigeret: 11.10.2023

1. Informationssikkerhedspolitikker

1.1 Retningslinjer for styring af informationssikkerhed

1.1.1 POLITIKKER FOR INFORMATIONSSIKKERHED

PUBLICERING AF SIKKERHEDSPOLITIK

Politik for informationssikkerhed på AAU skal offentliggøres og kommunikeres til alle relevante interessenter, herunder alle medarbejdere.

1.1.2 GENNEMGANG AF POLITIKKER FOR INFORMATIONSSIKKERHED

REVISION AF SIKKERHEDSPOLITIK

Der skal ske revision af informationssikkerhedspolitikken mindst en gang om året. Informationssikkerhedsudvalget behandler i 2. kvartal dette emne, og sender forslag til ny informationspolitik til rektor for endelig godkendelse.

DEFINITION PÅ INFORMATIONSSIKKERHED

Informationssikkerhed defineres som de samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet af AAU's informationer. Foranstaltninger inkluderer tekniske, proceduremæssige, lov- og regelmæssige kontroller.

GODKENDELSE AF SIKKERHEDSPOLITIK

Informationssikkerhedspolitikken, inkl. eventuelle ændringer, skal hvert år i juni måned godkendes af rektor.



2. Organisering af informationssikkerhed

2.1.1 ROLLER OG ANSVARSOMRÅDER FOR INFORMATIONSSIKKERHED

SIKKERHEDSANSVAR FOR IT-FUNKTIONER

Alle kritiske it-funktioner, der kræver specialviden, færdighed eller erfaring, skal identificeres, og der skal udpeges en driftsansvarlig ejer. Sikkerhedsansvarlige systemejere for virksomhedskritiske systemer skal identificeres og gøres opmærksom på dette ansvar. Disse ejere skal have ansvar og beføjelser til at sikre tilstrækkelig beskyttelse.

EJERSKAB

Alle informationsaktiver skal have udpeget en ejer (dataejer), som er ansvarlig for at klassificere det enkelte aktiv og tilse, at beskyttelse sker i henhold til klassifikationen.

SIKKERHEDSORGANISATION

Direktionen nedsætter et informationssikkerhedsudvalg. (se kommissorium)

KOORDINATION AF INFORMATIONSSIKKERHEDEN

Ansvar for koordination af den overordnede informationssikkerhed påhviler Informationssikkerhedsudvalget (ISU).

LEDELSENS ROLLE

Placering af ansvar er nødvendig, for at sikre AAU's informationsaktiver.

Ledelsen skal støtte virksomhedens informationssikkerhed, ved at udstikke klare retningslinjer, udvise synligt engagement, tildele ressourcer, definere roller samt følge op på arbejdet om informationssikkerhed.

2.1.2 FUNKTIONSADSKILLELSE

SIKRING AF FORRETNINGSKRITISKE SYSTEMER

Funktionsadskillelse skal implementeres, hvis lovgivningen kræver det eller hvis enhedsledelsen vurderer, at det vil være nødvendigt for at nedsætte risikoen for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af AAU's fortrolige og kritiske informationer.

2.1.3 KONTAKT MED MYNDIGHEDER

Ved brud på sikkerheden skal der være etableret en procedure for kommunikation og rapportering til relevante myndigheder, herunder Datatilsynet og Center for Cybersikkerhed.

2.1.4 KONTAKT MED SÆRLIGE INTERESSEGRUPPER

IT-afdelingen (ITS) skal holde sig orienteret om nye trusler mod de benyttede platforme og netværk. Det sker ved at etablere interne og eksterne kontakter til information og videndeling samt opkvalificering.

2.1.5 INFORMATIONSSIKKERHED VED PROJEKTSTYRING

Informationssikkerhed skal være en integreret del af projektledelse, hvor kravspecifikationer omfatter krav til informationssikkerhed - herunder beskyttelse af persondata - og hvor nødvendige sikringstiltag udpeges på basis af risikovurderinger.

2.2.1 POLITIK FOR MOBILT Udstyr

ADGANG TIL MOBILE ENHEDER

Brugere af AAU's mobile enheder er ansvarlige for at beskytte de data, der behandles på disse, samt enhederne selv. Adgang til informationer på mobile enheder skal være beskyttet med adgangskontrol. Mobile enheder må ikke efterlades ulåste eller uden opsyn i ualåste rum.

2.2.2 FJERNARBEJDSPLADSER

ADGANG FRA DISTANCEARBEJDSPLADSER

Medarbejdere ved AAU har mulighed for at arbejde hjemmefra eller på farten. Der skal anvendes krypteret forbindelse, hvor en risikovurdering tilsiger dette. Adgang gives kun til brugere, der er autentificerede med brugernavn og adgangskode samt evt. enten en personlig digital nøgle eller 2-faktorvalidering.

SIKRING AF HJEMMEARBEJDSPLADSER

Hjemmearbejdspladser og deres kommunikationsforbindelser skal beskyttes i forhold til de informationer og forretningssystemer, de benyttes til.

3. Personalesikkerhed

3.1 Før ansættelsen

3.1.1 SCREENING

BAGGRUNDSCHECK AF ANSATTE

HR-afdelingen skal tilse, at der foretages nødvendigt baggrundscheck af medarbejdere med ansvar for kritiske eller følsomme informationer.

VERIFIKATION AF REFERENCER

Ansættelsesmyndigheden er ansvarlig for nødvendig gennemgang og kontrol af oplysninger givet af medarbejdere og ansøgere inden ansættelse.

Baggrundscheck af medarbejdere kan fx omfatte:

- Personlige referencer.
- Ansøgerens CV.
- Uddannelser, certificeringer og professionelle kvalifikationer.
- Identitetskontrol. (skal altid foretages)

BAGGRUNDSCHECK AF KONSULENTER

Enhedslederen skal tilse, at der sker nødvendig baggrundscheck af konsulenter.

3.1.2 ANSÆTTELSESVILKÅR OG -BETINGELSER

Når en person første gang bliver oprettet som bruger af AAU's informationsaktiver, skal der informeres om de regler, der gælder for brugen af AAU's aktiver (se afsnit 4 Styring af aktiver).

Der genereres automatisk en mail til brugeren med et link til www.informationssikkerhed.aau.dk

Ansættelsesaftalen bør indeholde og uddybe:

- Det retlige ansvar og rettigheder for medarbejderen.
- Medarbejderens ansvar i forbindelse med informationsbehandling.
- Oplysninger om AAU's behandling af personoplysninger om den ansatte.
- Ansvarsplacering når der arbejdes uden for AAU's egne områder eller uden for normal arbejdstid, fx i forbindelse med arbejde hjemmefra eller på rejse.
- Beskrivelse af, hvad der skal ske, hvis medarbejdere ignorerer arbejdsgivers krav til sikkerhed.

3.2 Under ansættelsen

3.2.1 LEDELSESANSVAR

Informationssikkerheden på AAU afhænger i høj grad af medarbejderne. Medarbejdere skal derfor uddannes i informationssikkerhed i relation til deres jobfunktion og modtage nødvendige informationer. Det er ledelsens ansvar, at alle medarbejdere:

- er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med sikkerhed, før de tildeles adgang til AAU's systemer og data.
- er gjort bekendt med nødvendige retningslinjer, således at de kan leve op til AAU's informationssikkerhedspolitik.
- opnår et opmærksomhedsniveau i spørgsmål vedrørende informationssikkerhed, der er i overensstemmelse med deres roller og ansvar på AAU.
- holder sig inden for de retningslinjer og bestemmelser, der er for ansættelsen, inkl. AAU's informationssikkerhedspolitik og konkrete arbejdsmetoder.
- får viden om, hvordan informationer klassificeres.

3.2.2 BEVIDSTHED OM, UDDANNELSE OG TRÆNING I INFORMATIONSSIKKERHED

UDDANNELSE I SIKKERHEDSPOLITIKKEN

Alle medarbejdere skal læse AAU's informationssikkerhedspolitik. Alle nye medarbejdere modtager en henvisning til AAU's informationssikkerhedspolitik senest på første arbejdsdag. Alle medarbejdere modtager løbende instruktioner i overholdelse af og uddannelse i AAU's informationssikkerhedspolitik.

Enhedsledelsen har ansvar for, at nye medarbejdere gives en introduktion, hvor der bl.a. opnås kendskab til AAU's it-kodeks.

Inden brugere får adgang til informationsaktiver, skal der gives en fornøden instruktion i log on-/log off-procedurer, anvendelse af applikationer m.m.

SIKKERHEDSUDDANNELSE FOR IT-MEDARBEJDERE

Alle it-medarbejdere skal specifikt uddannes i sikkerhedsaspekter for at minimere risikoen for sikkerhedshændelser.

It-medarbejdere skal i forbindelse med deres ansættelse gøres bekendt med informationsikkerhedsprincipperne med tilhørende bilag og supplerende retningslinjer.

3.2.3 SANKTIONER

Ledelsen skal etablere en formel sanktionsprocedure for medarbejdere, studerende og andre, der anvender AAU's informationer eller informationssystemer, og som bryder AAU's politikker, regler eller retningslinjer for informationssikkerhed.

Det er ledelsens ansvar, at sanktioner for brud på AAU's informationssikkerhedspolitikker, regler eller retningslinjer håndhæves i overensstemmelse med gældende lovgivning.

Overtrædelser af informationssikkerheden sanktioneres på samme måde som andre overtrædelser af AAU's politikker og regler (irrettesættelse, advarsel, afskedigelse, inddragelse af retten til brug af AAU's netværk, bortvisning og i særlige tilfælde politianmeldelse).

3.3 Ansættelsesforholdets ophør eller ændring —

3.3.1 ANSÆTTELSESFORHOLDETS OPHØR ELLER ÆNDRING

Medarbejderen skal aflevere alle de af AAU udleverede informationer og aktiver ved ansættelsens ophør. Medarbejderen skal desuden slette virksomhedens informationer fra privat udstyr ved ansættelsens ophør. HR skal i samarbejde med IT lave og vedligeholde en procedure for inddragelse af privilegier i forbindelse med ændringer i ansættelsesforholdet, fratrædelse eller afskedigelse af personale.

4. Styring af aktiver

4.1 Ansvar for aktiver —

4.1.1 FORTEGNELSE OVER AKTIVER

Der skal forelægges en oversigt over AAU's kritiske og følsomme informationsaktiver, som samtidig iagttager lovkrav vedr. fortegnelser over persondata.

4.1.2 EJERSKAB AF AKTIVER

SIKKERHEDSANSVAR FOR INFORMATIONSAKTIVER

Der skal udpeges en ansvarlig dataejer, som er ansvarlig for at klassificere det enkelte aktiv og tilse, at beskyttelse sker i henhold til klassifikationen.

Det er enhedslederens ansvar, at der udarbejdes og vedligeholdes en liste over informationsaktiver. Listen skal angive data- og systemejer for hvert enkelt aktiv.

UDARBEJDELSE AF EN OVERORDNET RISIKOVURDERING

Ud fra listen over informationsaktiver foretages regelmæssige risikovurderinger til fastlæggelse

af nødvendige informationssikkerhedsforanstaltninger.

Det er enhedsledelsens ansvar, at der udarbejdes risikovurderinger for enhedens kritiske og følsomme informationsaktiver. Vurderingen skal belyse hvilke trusler, der findes, sandsynligheden for at de indtræffer samt de mulige konsekvenser. Risikovurderingen kan udføres i samarbejde med informationssikkerhedschefen og skal dokumenteres i centralt værktøj.

Risikovurderingerne skal ajourføres mindst hvert år og desuden ved større forandringer i organisationen og/eller i informationsaktiverne, som kan have indflydelse på det samlede risikobillede.

Det samlede materiale udgør AAU's overordnede risikovurdering.

4.1.3 ACCEPTERET BRUG AF AKTIVER

ACCEPTERET BRUG AF INFORMATIONSAKTIVER

Der er udarbejdet et "it-kodeks for ansatte og studerende". Dette kodeks beskriver nærmere regler og generelle retningslinjer for brugeradfærd.

4.1.4 TILBAGELEVERING AF AKTIVER

Alle brugere skal aflevere AAU's aktiver, der er i deres besiddelse, når deres aftale med AAU ophører.

4.2 Klassifikation af information

4.2.1 KLASSIFIKATION AF INFORMATION

Alle ansatte bør have kendskab til, hvorledes informationer klassificeres. For at sikre informationers fortrolighed er der udarbejdet en klassifikationsmodel efter 4 niveauer:

- Offentlige: Informationer som er til rådighed for offentligheden eller hvor offentliggørelse ikke gør skade på AAU.
- Interne: Informationer, som kun brugere, med et rent arbejdsbetinget behov, må og kan få adgang til, men hvor et brud på fortroligheden vil have en lav skadevirkning for AAU, privatpersoner eller samarbejdspartner(e).
- Fortrolige: Informationer, som kun brugere, med et rent arbejdsbetinget behov, må og kan få adgang til, og hvor et brud på fortroligheden vil have en middel skadevirkning for AAU, privatpersoner eller samarbejdspartner(e).
- Følsomme: Informationer, som kun brugere, med et rent arbejdsbetinget behov, må og kan få adgang til, og hvor et brud på fortroligheden vil have en høj skadevirkning for AAU, privatpersoner eller samarbejdspartner(e).

Uanset klassifikationsniveau kan der være implementeret adgangskontrol til informationer på flere niveauer.

DEFINITIONER AF ROLLER I FORBINDELSE MED KLASSIFICERING, BEHANDLING OG BRUG AF DATA:

- Dataejer: Den, der er ansvarlig for klassifikation af data samt at tilse, at beskyttelse sker i henhold til klassifikationen.

- Administrator: Person eller organisation, der på baggrund af dataejerens klassificering og instruks administrerer adgang til data.
- Databehandler: Person eller organisation, der behandler data på vegne af dataejerens og efter dennes instruks.
- Bruger: Person eller organisation som anvender data.

4.2.2 MÆRKNING AF INFORMATION

De enkelte dataejere har ansvaret for, at informationer er behørigt klassificeret.

ANSVAR FOR ADGANGSRETTIGHEDER

Dataejere har ansvaret for at fastlægge og løbende revurdere adgangsrettigheder.

KLASSIFIKATIONSMÆRKNING

AAU's informationer skal identificeres og klassificeres i overensstemmelse med reglerne for klassifikation.

4.2.3 HÅNDTERING AF AKTIVER

KONTROL MED KLASSIFICEREDE INFORMATIONER

Informationssikkerhedsudvalget er ansvarlig for at definere et fast sæt af egnede og relevante sikkerhedsforanstaltninger til beskyttelse af de enkelte informationer.

4.3 Mediehåndtering

4.3.1 STYRING AF BÆRBARE MEDIER

OPBEVARING OG REGISTRERING AF DATAMEDIER

Dataejerens skal sikre, at medier eller informationerne på mediet klassificeres, og at brugere er instrueret i at opbevare mediet i henhold til regler for klassifikationen.

BRUG AF DATAMEDIER

Det valgte datamedie skal kunne beskytte informationerne i forhold til deres klassifikation.

BRUG AF BÆRBARE MEDIER TIL FORTROLIGE DATA

Datamedier skal beskyttes mod tab og misbrug jf. reglerne for mobile enheder. Fortrolige og følsomme data, herunder persondata skal krypteres, hvis de opbevares eller transporteres på bærbare medier, fx USB-hukommelse, tablets, telefoner, dvd'er, disketter m.m..

4.3.2 BORTSKAFFELSE AF MEDIER

BORTSKAFFELSE OG GENBRUG AF MEDIER

Alle datamedier, fx harddiske, disketter, cd'er, dvd'er, bånd og hukommelsesenheder skal sikkerhedsslettes eller destrueres inden bortskaffelse, såfremt de indeholde data, der ikke er klassificeret "Offentlig". Der henvises til "Skrotnings-/genanvendelsesprocedure for IT udstyr på AAU", som varetages af ITS Support.

4.3.3 FYSISKE MEDIER UNDER TRANSPORT

Alle datamedier, fx harddiske, disketter, cd'er, dvd'er, bånd og hukommelsesenheder, der

indeholder fortrolige eller følsomme data skal krypteres. Det gældende krypteringskrav er mindst 256 bits AES kryptering.

5. Adgangsstyring

5.1 Forretningsmæssige krav til adgangsstyring

Kravene til adgangsstyring er bestemt af værdien af de data og systemer, der gives adgang til. Der skal tilstræbes en lagdelt sikkerhed, således at jo tættere man kommer på de mest kritiske og følsomme informationer, des større krav stilles til adgangskontrollen. Gives der eksempelvis blot adgang til Internettet, dvs. til offentlige data og systemer, er det ikke nødvendigt at stille samme krav til adgangskoder, som der skal stilles, hvor der gives adgang til fortrolige og følsomme oplysninger internt på AAU. Nærværende regler skal betragtes som minimumkrav, og det er derfor tilladt for den enkelte system- og dataejer at indføre en mere striks politik, såfremt en risikovurdering fordrer dette.

5.1.1 POLITIK FOR ADGANGSSTYRING

BEGRÆNSET ADGANG TIL INFORMATIONER

Adgang for brugere og personale til brugersystemers funktioner og informationer skal begrænses i overensstemmelse med de fastlagte arbejds- og forretningsbetingede krav samt informationernes klassifikation.

INDDRAGELSE AF PRIVILEGIER VED FRATRÆDELSE

Der skal forefindes en opdateret procedure for inddragelse af privilegier i forbindelse med fratrædelse, organisatorisk omplacering, ændring i stilling eller afskedigelse af personale. Det er enhedsledelsens ansvar at orientere IT- og HR-afdelingen ved ændring af medarbejderes arbejdsopgaver, herunder organisatorisk omplacering samt fratrædelse, så tildelte privilegier kan tilrettes eller fjernes.

5.1.2 ADGANG TIL NETVÆRK OG NETVÆRKSTJENESTER

OVERVÅGNING AF NETVÆRK

ITS Infrastruktur er ansvarlig for kontinuerligt at overvåge brugen og sikkerheden af AAU's netværksinfrastruktur. Det anbefales at anvende automatiske overvågningssystemer.

RETNINGSLINJER FOR BRUG AF NETVÆRKSTJENESTER

Brugere må alene have adgang til de tjenester, de er autoriseret til at benytte.

ADGANG TIL TRÅDLØSE NETVÆRK

Studerende, ansatte og gæster, har mulighed for at benytte trådløse netværk på Aalborg Universitet. [Læs mere her.](#)

OPDELING AF NETVÆRK

For at forbedre driftssikkerheden for kritiske servere skal der etableres separate servernetværk med skærpet filtreringspolitik. Det skal etableres separate netværk til udstyr i forskellige "risikogrupper", fx private computere, universitetets computere og printere.

STYRING AF NETVÆRSADGANG

Kun autoriserede brugere og udstyr må have adgang til netværk på AAU.

AUTENTIFICERING VED ADGANG TIL NETVÆRKET

Adgangen til det interne netværk fra andre lokationer end AAU's, skal være beskyttet i henhold til gældende risikovurdering.

5.2 Administration af brugeradgang

5.2.1 BRUGERREGISTRERING OG -AFMELDING

IDENTIFIKATION OG AUTENTIFIKATION AF BRUGERE

Alle brugere skal have en unik identitet til personligt brug. Der skal benyttes en passende autentifikationsteknik til verifikation af brugernes identitet. Brugeridentiteten skal kunne spores til den person, som er ansvarlig for en given aktivitet. Fælles brugeridentiteter skal undgås.

5.2.2 TILDELING AF BRUGERADGANG

TILDELING AF BRUGERRETTIGHEDER

Dataejer har ansvaret for at sikre, at den enkelte bruger tildeles netop de brugerprivilegier, som brugerens arbejdsopgaver berettiger til.

RETNINGSLINJER FOR ADGANGSSTYRING

Administrator forestår den løbende registrering, styring og overvågning af tildelingen og anvendelsen af privilegier i henhold til dataejerens klassificering af informationer.

ADGANGSBEGRÆNSNING TIL INFORMATIONER

Applikationer skal sikre, at adgang til informationer sker efter en veldefineret adgangspolitik.

5.2.3 STYRING AF PRIVILEGEREDE ADGANGSRETTIGHEDER

BESKYTTELSE AF ADGANGE

Der skal altid benyttes adgangskode for adgang med systemadministratorprivilegier.

UDVIDEDE ADGANGSRETTIGHEDER

De udvidede adgangsrettigheder, fx administratorrettigheder, må kun tildeles i begrænset omfang og alene ud fra et arbejdsbetinget behov. De udvidede adgangsrettigheder skal registreres. De udvidede adgangsrettigheder må ikke sættes i kraft, før den fornødne autorisation er indhentet. Automatiserede systemtekniske processer skal anvendes i videst muligt omfang for at begrænse behovet for tildeling af udvidede rettigheder.

De enkelte brugerprogrammer skal, så vidt muligt, tilrettelægges, så de begrænser behovet for indgreb med udvidede rettigheder. Der skal benyttes særlige brugeridentiteter til de udvidede rettigheder af hensyn til overvågning og opfølgning.

ÆNDRING AF KODER MED UDVIDEDE ADGANGSRETTIGHEDER

Adgangskoder med udvidede rettigheder skal ændres eller tilbagekaldes ved mistanke om, at udenforstående har fået kendskab til disse, eller hvor en autoriseret bruger ændrer jobfunktion, som ikke længere berettiger de udvidede rettigheder.

SKIFT AF ADGANGSKODE TIL UDVIDEDE RETTIGHEDER VED FRATRÆDELSE

Hvis en person med kendskab til udvidede adgangsrettigheder fratræder, skal disse adgangskoder ændres med det samme.

5.2.4 STYRING AF HEMMELIG AUTENTIFIKATIONSINFORMATION OM BRUGERE

LAGRING AF ADGANGSKODER

Adgangskoder må aldrig lagres elektronisk i klartekst.

5.2.5 GENNEMGANG AF BRUGERADGANGSRETTIGHEDER

GENNEMGANG AF BRUGERPROFILER

Alle brugerprofiler skal gennemgås mindst en gang årligt for at identificere inaktive profiler eller tilsvarende, der skal fjernes eller ændres.

5.2.6 INDDRAGELSE ELLER JUSTERING AF ADGANGSRETTIGHEDER

BRUGERPROFILER

Gæster og eksterne konsulenter må alene oprettes som brugere med tidsbegrænset adgang. Normalt må tidsbegrænsningen ikke overstige 12 måneder inden fornyet godkendelse. Brugere tildeles adgang til AAU alene ud fra et arbejds- og/eller studiebetings behov.

FRATRÆDELSE

Når ansættelse eller midlertidige kontrakter ophæves, skal tilknyttede rettigheder vurderes og om nødvendigt ændres eller fjernes. ID-kort og lignende skal afleveres og it-udstyr skal inddrages.

MEDARBEJDERES OMPLACERING

Tildelte adgangsrettigheder og privilegier skal revurderes i forbindelse med afgang eller omplacering. Det er enhedsledelsens ansvar, at der etableres lokale procedurer for dette.

REGISTRERING AF BRUGERE

Brugere skal have unikt brugernavn og bruger-ID. Adgangsrettigheder skal afstemmes med de forretningsmæssige behov. Der skal ske en verifikation af, at rettighedsniveauet er i overensstemmelse AAU's generelle sikkerhedsretningslinjer. Serviceleverandører skal anvende tilsvarende eller samme autorisationsprocedure som AAU.

Systemejer skal autorisere brugeradgang og vedligeholde brugerfortegnelser for systemet. AAU skal vedligeholde vejledninger for, hvordan brugere eller brugeres rettigheder fjernes eller ændres ved ophør eller ændring af brugeres jobfunktion. Adgangsrettigheder må ikke krænke eventuelle krav om funktionsadskillelse. Procedurerne skal omfatte hele den periode, hvori adgangsrettighederne er gældende, dvs. fra registrering af en bruger til formel afmelding af en bruger, der ikke længere har et arbejds- eller studiebetings behov for adgang.

Det skal tilstræbes, at brugeren har den samme identifikation på samtlige af de it-systemer, som brugeren har adgang til. Fælles-id for en gruppe medarbejdere skal i videst muligt omfang undgås.

5.3 Brugernes ansvar

—

5.3.1 BRUG AF HEMMELIG AUTENTIFIKATIONSINFORMATION

VALG AF SIKRE ADGANGSKODER

Brugerne skal følge god sikkerhedspraksis ved udvælgelsen og brug af adgangskode. Der bør vælges en adgangskode, der er nem at huske men svær at gætte. [Se gældende vejledning og hjælp her.](#)

KRAV TIL SKIFT AF ADGANGSKODE

Adgangskoder skal ændres ved mistanke om, at andre har fået kendskab til disse og mindst en gang om året. For informationer der er beskyttet via en mere kvalificeret adgangskontrol (hvor adgangskontrollen består af mere og andet end blot brugernavn/adgangskode), kan hyppigheden af skift af adgangskode ændres efter nærmere aftale med Informationssikkerhedsudvalget og Informationssikkerhedschefen.

KRAV TIL LÆNGDE AF ADGANGSKODE

Adgangskoder for brugere skal indeholde mindst 14 tegn og mindst 3 ud af 4 forskellige tegntyper (store og små bogstaver, tal eller specialtegn). Adgangskoder med udvidede rettigheder, fx administratorer, skal indeholde mindst 14 tegn og mindst 4 forskellige tegntyper (store bogstaver, små bogstaver, tal eller specialtegn).

GENBRUG AF ADGANGSKODE

Det er ikke tilladt at bruge den samme adgangskode på AAU's systemer, som benyttes på eksterne systemer.

ADGANGSKODER ER STRENGT PERSONLIGE

Adgangskoder er strengt personlige og må ikke deles med andre.

RETNINGSLINJER FOR ADGANGSKODER

Ved brugeroprettelse eller nulstilling af adgangskode skal brugere tildeles en sikker, midlertidig adgangskode, som skal ændres umiddelbart efter første anvendelse. Der skal etableres og vedligeholdes en procedure for, hvordan en brugers identitet fastslås, før en ny midlertidig adgangskode må udleveres. Midlertidige adgangskoder skal være unikke, må ikke genbruges og skal opfylde de almindelige krav til adgangskoder.

SIKRING AF KRITISKE INFORMATIONER

Efter installation af et nyt system, skal standardadgangskoderne ændres øjeblikkeligt i dette.

5.4 Styring af system- og applikationsadgang

–

5.4.1 PROCEDURER FOR SIKKER LOG-ON

SIKKER LOG-ON

Systemadgang skal beskyttes af en sikker log-on-procedure.

5.4.2 SYSTEM FOR ADMINISTRATION AF ADGANGSKODER

SYSTEMER TIL STYRING AF ADGANGSKODER

It-systemerne skal, så vidt dette er muligt, sikre, at kravene til adgangskoder overholdes, og at de ikke genbruges.

IMPLEMENTERING AF ET SYSTEM TIL HÅNDTERING AF ADGANGSKODER

Der skal implementeres et adgangskodehåndteringssystem (password management system) for kritiske systemer, der ikke integrerer med AD, og som håndhæver AAU's adgangskoderegler.

5.4.3 BRUG AF PRIVILEGEREDE SYSTEMPROGRAMMER

BRUG AF SYSTEMVÆRKTØJER

Al brug af systemværktøjer skal logges. It-afdelingen skal sikre, at brugen af systemværktøjer (fx utilities, der kan påvirke eller omgå systemers eller enheders sikkerhed) begrænses til et minimum af betroede og autoriserede brugere.

5.4.4 STYRING AF ADGANG TIL KILDEKODER TIL PROGRAMMER

ADGANGSKONTROL FOR KILDETEKST

Kildetekst til applikationer under udvikling skal beskyttes med adgangskontrolsystemer for at sikre integriteten.

KONTROLLERET ADGANG TIL KILDEKODE

Kildekoden til udviklingsprojekter skal sikres mod uautoriseret adgang. Ændringer skal kontrolleres for at sikre integritet, og der skal være etableret versionsstyringsprocesser. Eventuelle udskrifter af kildekode skal opbevares sikkert.

6. Kryptografi

6.1 Kryptografiske kontroller

6.1.1 POLITIK FOR ANVENDELSE AF KRYPTOGRAFI

KRYPTERING AF FILER

Filer med information klassificeret som fortroligt eller følsomt beskyttes i henhold til AAU's dataklassifikationsmodel ved i visse sammenhænge at benytte kryptografi.

GODKENDELSE AF KRYPTERINGSPRODUKTER

Der må alene anvendes kryptografi, der anvender anerkendte krypteringsmetoder.

BRUG AF KRYPTERING I FORBINDELSE MED OPBEVARING AF INFORMATIONER

Fortrolige og følsomme informationer skal altid sendes krypteret, når de behandles elektronisk udenfor AAU's netværk.

6.1.2 ADMINISTRATION AF ELEKTRONISKE NØGLER

NØGLEHÅNDTERING

Der skal etableres og vedligeholdes en procedure for nøglehåndtering skal beskrive hvordan generering, distribution, opbevaring og destruktion af nøgler håndteres.

7. Fysisk sikring og miljøsikring

7.1 Fysisk sikring og miljøsikring

Fysisk sikkerhed omfatter blandt andet døre, vinduer, alarmer, videoovervågning - samt tyverisikring af Universitetets fysiske aktiver, eksempelvis it-udstyr. Dertil kommer adgangskontrolsystemer, som ligeledes er et element af den fysiske sikkerhed og som til en vis grad sikrer, at kun personer med legalt ærinde får adgang til Universitetets område i de tidspunkter hvor systemet er slået til.

7.2 Sikre områder

7.2.1 FYSISK PERIMETERSIKRING

INDBRUDSALARMER

De fleste AAU-områder har etableret skalsikring, og der foreligger aftaler med et vagtselskab om overvågning, tilkald og udrykning ved alarm.

7.2.2 FYSISK ADGANGSKONTROL

Fysisk sikkerhed og adgangsregler er en del af AAU's sikkerhedspolitik. Systemer til adgangskontrol er et element af fysisk sikkerhed, der sikrer, at kun personer med legalt ærinde får adgang til AAU's område.

ADGANGSKORT

Adgangskort er personlige. De skal opbevares forsvarligt og må ikke overdrages til tredjepart.

7.2.3 SIKRING AF KONTORER, LOKALER OG FACILITETER

SIKRING AF KONTORER, LOKALER OG Udstyr

Kontorer og andre lokaler, hvor der opbevares fortrolige og følsomme informationer, skal kunne låses.

OPLYSNINGER OM SIKRE OMRÅDER

Oplysninger om sikre områder og deres funktion skal alene gives ud fra et arbejdsbetinget behov.

7.2.4 BESKYTTELSE MOD EKSTERNE OG MILJØMÆSSIGE TRUSLER

BRANDSIKRING

Serverrum må ikke benyttes som lager for brændbare materialer. Farlige eller brandfarlige materialer skal lagres i behørig afstand fra de sikre områder. Der skal altid etableres automatiske sluknings- og brandalarmsanlæg i rum, hvor den samlede værdi af it- og andre informationsaktiver overstiger 700.000 kr. i år 2018 prisniveau.

MILJØMÆSSIG SIKRING AF SERVERRUM

Serverrum, krydsfelter og tilsvarende områder skal sikres passende mod miljømæssige hændelser som brand, vandindtrængen, eksplosion og tilsvarende påvirkninger.

7.2.5 ARBEJDE I SIKRE OMRÅDER

AFLÅSNING AF LOKALER OG BYGNINGER

Alle døre og vinduer med adgang til/fra bygningerne skal lukkes og låses ved arbejdstids ophør.

Døre til sikrede lokationer i bygningerne skal ligeledes aflåses.

7.2.6 OMRÅDER TIL AF- OG PÅLÆSNING

AF- OG PÅLÆSNINGSOMRÅDER

Leverancer skal registreres i henhold til gældende varemodtagelsesprocedure.

7.3 Udstyr

7.3.1 PLACERING OG BESKYTTELSE AF UDSTYR

AFLÅSNING AF HOVEDKRYDSFELTER OG LIGNENDE TEKNIKRUM

Alle krydsfelter og teknikrum skal være sikrede og aflåste.

ADGANG TIL SERVERRUM OG HOVEDKRYDSFELTER

Adgang til serverrum og hovedkrydsfelter er beskrevet i vejledning vedr. "Adgang til maskinstuer".

UDLÅN AF ADGANGSKORT OG/ELLER NØGLER

Adgang til sikrede områder kan midlertidigt tildeles håndværkere, teknikere og andre, såfremt alle regler for adgange overholdes.

ADGANG FOR SERVICELEVERANDØRER

Serviceleverandører må kun få adgang til sikre områder, når dette er påkrævet og adgangen overvåges.

7.3.2 UNDERSTØTTENDE FORSYNINGER (FORSYNINGSSIKKERHED)

NØDSTRØMSANLÆG

Den risikovurdering, som foreligger for kritiske aktiver, skal inkludere en vurdering om anvendelse af nødstrømsanlæg (UPS).

FORSYNINGSSIKKERHED

Datakommunikation sikres gennem etablering af redundans og strategisk placering af udstyr og linjer, for at undgå "single point of failure".

7.3.3 SIKRING AF KABLER

Kabler til datakommunikation skal beskyttes mod uautoriserede indgreb og skader. Det skal sikres, at kabler i terræn registreres hos relevante interessenter. Faste kabler og udstyr skal altid mærkes klart og entydigt. Dokumentation skal opdateres, når den faste kabelføring ændres.

7.3.4 VEDLIGEHOVELSE AF UDSTYR

VEDLIGEHOVELSE AF UDSTYR OG ANLÆG

Systemejere bør vedligeholde udstyr efter leverandørens anvisninger. Kun kvalificerede leverandører må udføre reparationer og vedligeholdelse. Reparationsvirksomheden skal overholde de gældende sikkerhedskrav, hvis udstyr repareres eller vedligeholdes uden for AAU.

Kritiske og følsomme informationer skal slettes fra udstyr, der repareres eller vedligeholdes uden for AAU. Systemforvaltere er ansvarlige for, at der føres log over alle fejl og mangler samt reparationer og forbyggende vedligeholdelse.

7.3.5 FJERNELSE AF AKTIVER

Enhedsledelsen fastsætter regler for autoriseret bortskaffelse af AAU's aktiver.

7.3.6 SIKRING AF Udstyr OG AKTIVER UDEN FOR ORGANISATIONEN

OPSYN MED MOBILE ENHEDER

Mobile enheder må ikke efterlades uden opsyn i uaflåste rum. Bærbart udstyr skal konfigureres i henhold til de gældende AAU's regler for mobile enheder.

7.3.7 SIKKER BORTSKAFFELSE ELLER GENBRUG AF Udstyr

BORTSKAFFELSE ELLER GENBRUG AF Udstyr

It-udstyr, der indeholder lagermedier - fx fastmonterede harddiske i arbejdsstationer, servere og kopimaskiner - skal kontrolleres før fjernelse for at sikre, at alle informationer tillige med licenserede og egne brugerprogrammer er slettet.

7.3.8 BRUGERUDSTYR UDEN OPSYN

PLACERING AF Udstyr

Bærbare computere og lignende udstyr bør, hvis det efterlades på et kontor uden opsyn (fx efter arbejdstid), låses inde, således det ikke er umiddelbart synligt udefra. Udstyr skal placeres eller beskyttes, så risikoen for skader og uautoriseret adgang minimeres. Udstyr, der benyttes til at behandle kritiske eller følsomme informationer, skal placeres, så informationerne ikke kan aflures af uvedkommende.

7.3.9 POLITIK FOR RYDDELIGT SKRIVEBORD OG BLANK SKÆRM

OPBEVARING AF FYSISKE DOKUMENTER

Fortrolige og følsomme informationer skal opbevares i aflåst skab eller skuffe efter arbejdstid, jf. dataklassifikationsmodellen.

BRUG AF ADGANGSKODEBESKYTTET PAUSESKÆRM

Brugere skal aktivere adgangskodebeskyttet skærmlås, når arbejdsstationen forlades. Systemet skal som hovedregel aktivere adgangskodebeskyttet skærmlås på computere efter max. 15 minutters inaktivitet.

UDSKRIVNING

Printkøer og lignende med følsomt eller kritisk indhold skal sikres mod uautoriseret adgang. Brugere skal sikre, at fortrolige og følsomme udskrifter afhentes straks. Hvor muligt benyttes Follow-You-printsystemet til udskrifter.

8. Driftssikkerhed

8.1 Driftsprocedurer og ansvarsområder

—

8.1.1 DOKUMENTEREDE DRIFTSPROCEDURER

SIKRING AF SERVERSYSTEMER

Alle servere skal sikres og godkendes inden overgang til produktion.

DOKUMENTATION

Enhedsledelsen skal sikre, at der foreligger velbeskrevne driftsprocedurer for alle kritiske it-systemer i produktion.

DRIFTSANSVAR

It-afdelingen er ansvarlig for drift og administration af it-systemer samt disses sikkerhed. Dette inkluderer efterlevelse af sikkerhedspolitikker, regler og procedurer.

DRIFTSAFVIKLINGSPROCEDURER

Driftsafviklingsprocedurer skal være dokumenterede, ajourførte og tilgængelige for driftsafviklingspersonalet og andre med et arbejdsbetinget behov.

REGISTRERING AF DRIFTSSTATUS

Væsentlige forstyrrelser og uregelmæssigheder i driften af systemerne samt årsager hertil, skal registreres.

BESKYTTELSE AF DIAGNOSE- OG KONFIGURATIONSPORTE

Fysisk og logisk adgang til diagnose- og konfigurationsporte skal kontrolleres. Indgange til fjerndiagnose og -vedligehold - herunder specielle diagnoseporte, konsolswitche, out-of-band management mv. - skal sikres mod uautoriseret anvendelse.

Procedurer for eksterne leverandørers adgang til fjerndiagnose skal udarbejdes af systemejer. Enhver anvendelse af diagnoseporte bør logges.

8.1.2 ÆNDRINGSSTYRING

ÆNDRINGSSTYRING

It-afdelingen følger principperne for ændringsstyring i ITIL, hvilket nedenstående regler er eksempler på. Ved ændringer skal der foregå en gennemgang af sikringsforanstaltninger og integritetskontroller for at sikre, at disse ikke forringes ved implementeringen.

Der skal indhentes godkendelse fra systemejer, før ændringen gennemføres. Systemdokumentation skal opdateres ved hver ændring. Forældet systemdokumentation skal arkiveres eller destrueres.

Der skal vedligeholdes en versionsstyring for alle systemændringer, samt en log over alle ændringer. Hvor det er muligt, skal der foretages test af driftsfunktionaliteten før ændringer gennemføres.

PLANLÆGNING, TEST OG GODKENDELSE AF ÆNDRINGER

Ændringer skal følge en formaliseret procedure inden iværksættelse, som indebærer planlægning og hvor muligt afprøvning inden idriftsætningen. Desuden skal ændringernes konsekvenser vurderes, inden de iværksættes.

RETNINGSLINJER FOR ÆNDRINGER

Ændringer skal kun gennemføres, når der er begrundet behov.

It-afdelingen har ansvaret for, at der foregår en entydig identifikation og registrering af væsentlige ændringer. Information vedrørende udførte ændringer skal formidles til relevante interessenter. It-afdelingen har ansvaret for, at der findes en nødprocedure pr. System/service til at mindske effekten af fejlslagne ændringer.

8.1.3 KAPACITETSSTYRING

KAPACITETSPLANLÆGNING

It-systemernes dimensionering skal afpasses efter kapacitetskrav. Belastning skal overvåges, således at opgradering og tilpasning kan finde sted løbende. Der skal til enhver tid være høj fokus på alle forretningskritiske systemer.

KAPACITETSOVERVÅGNING

Alle serversystemer skal overvåges for at sikre tilstrækkelig kapacitet, pålidelig drift og tilgængelighed. Større afvigelser fra normal-kapacitet skal registreres og håndteres som en hændelse.

8.1.4 ADSKILLELSE AF UDVIKLINGS TEST- OG DRIFTSMILJØER

SIKRING AF APPLIKATIONSUDVIKLINGSMILJØERNE

Udviklingsmiljøer skal sikres mod trusler som uautoriseret adgang, ændringer og tab. Informationer skal sikres i forhold til deres klassifikation.

ADGANG TIL PRODUKTIONSDATA

Systemadministratorers adgang til fortrolige oplysninger skal begrænses.

ADSKILLELSE AF UDVIKLING, TEST OG DRIFT

Udviklings- og testmiljøer skal være systemteknisk eller fysisk adskilt fra driftsmiljøet.

8.2 Beskyttelse mod malware

8.2.1 KONTROLLER MOD MALWARE

KRAV OM ANTIVIRUS PÅ COMPUTERE

Alle computere skal anvende et opdateret antivirusprogram, eller være tilsvarende beskyttet med andre metoder. Dette gælder også private computere, som kobles på AAU's netværk. Der skal benyttes beskyttelsesforanstaltninger imod spyware og andet malware, hvor dette skønnes nødvendigt.

8.3 Backup

8.3.1 BACKUP AF INFORMATION

SIKKERHEDSKOPIERING AF INFORMATIONER PÅ SERVERSYSTEMER

It-afdelingen er ansvarlig for sikker lagring og backup af informationer på serverudstyr, samt for opbevaring og sikkerhedskopiering af alle forretningskritiske informationer på serversystemer. Der skal forefindes en procedure eller vejledning for sikkerhedskopiering af alle essentielle/forretningskritiske data, programmer og parameteropsætninger

Backup skal være nøjagtig, fuldstændig og omfatte dokumenterede restore-procedurer. Omfanget og hyppigheden af backup skal afspejle de nuværende forretnings-, it- og lovkrav. Backup-data skal beskyttes med passende logisk og fysisk adgangskontrol. Sikkerhedskopierede informationer skal testes regelmæssigt for at sikre, at informationerne

gendannes korrekt. Backup-data skal opbevares off-site, for at sikre redundans i tilfælde af katastrofer.

OVERVÅGNING AF PROCEDURER FOR SIKKERHEDSKOPIERING

Muligheden for at retablere informationer fra backup-systemer skal regelmæssigt testes af. Endvidere skal retablering testes efter system- eller procesændringer, der kan påvirke backup-rutiner.

NØDPLANER FOR SIKKERHEDSKOPIERING

Alle kritiske systemer skal have en nødplan for sikkerhedskopiering, således at risikoen for tab af informationer minimeres.

OPBEVARING AF SIKKERHEDSKOPIER PÅ EKSTERN LOKATION

Datamedier til retablering af kritiske systemer skal opbevares på et sikkert opbevaringssted i passende afstand fra produktionsdata.

8.4 Logning og overvågning

8.4.1 HÆNDELSESLOGNING

HÆNDELSESLOGNING

Alle produktionssystemer skal logge information om adgang og forsøg på adgang for at kunne spore uautoriseret aktivitet. Logfiler skal gennemgås regelmæssigt og med fordel ved hjælp af automatiserede værktøjer.

Alle informationssikkerhedshændelser skal logges og opbevares i en fastlagt periode af hensyn til opfølgning på adgangskontroller og eventuel efterforskning af fejl og misbrug. IT-afdelingen er ansvarlig for at konfigurere systemerne på en måde, så relevante oplysninger logges og gemmes til evt. senere brug.

OPBEVARING AF OPFØLGINGSLOG

AAU's regler for logning skal opfylde gældende dansk lovgivning.

OVERVÅGNING AF INTERNET-BRUG

AAU forbeholder sig ret til at filtrere, logge og begrænse brugen af netværk herunder internet, i det omfang hensynet til driften kræver det.

8.4.2 BESKYTTELSE AF LOGOPLYSNINGER

Logfiler kan indeholde oplysninger, som ikke må være offentlig tilgængelige. Log-faciliteter og log-oplysninger skal beskyttes mod manipulation og tekniske fejl.

Alle logregistreringer skal beskyttes mod uautoriseret adgang gennem anvendelse af adgangskontrolsystemer, fysisk adskillelse eller netværkssegmentering. Logregistreringer skal umiddelbart overføres til en central logserver eller til et sikkert medie, som kun vanskeligt kan modificeres. Kun personer, hvis arbejde kræver dette, tildeles adgang til logs.

8.4.3 ADMINISTRATOR- OG OPERATØRLOG

OVERVÅGNING AF SERVICELEVERANDØREN

It-afdelingen skal regelmæssigt overvåge serviceleverandørerne, gennemgå de aftalte rapporter

og logninger samt udføre egentlige revisioner for at sikre, at aftalen overholdes, og at sikkerhedshændelser og -problemer håndteres på betryggende vis.

ADMINISTRATORLOG

Der skal foretages logning af alle handlinger udført af personer med administratorrettigheder i forbindelse med kritiske systemkomponenter, der er i drift, inkl. netværksudstyr.

8.4.4 TIDSSYNKRONISERING

Det kræves, at alt udstyr (servere, PC'er, netudstyr), der leverer log i henhold til reglerne om logning, synkroniserer deres ure vha. NTP.

8.5 Styring af driftssoftware

8.5.1 SOFTWAREINSTALLATION PÅ DRIFTSSYSTEMER

Vedligeholdelse og opdatering af it-systemer er nødvendigt for at opretholde et passende sikkerhedsniveau for AAU. Drift af it-systemer inkluderer elementer af overvågning af systemernes helbredstilstand, opdatering og sikkerhedskopiering af data. De fleste it-systemer i dag er afhængige af netværk og derfor er administration, opbygning, sikring og vedligeholdelse af netværk vitalt for AAU. Den trussel, som uautoriseret adgang indebærer, gør det nødvendigt med klare regler for brugen af AAU's netværk samt overvågning af infrastrukturen.

8.6 Sårbarhedsstyring

8.6.1 STYRING AF TEKNISKE SÅRBARHEDER

RETTELSE TIL OPERATIVSYSTEMER OG APPLIKATIONS-PROGRAMPAKKER

It-afdelingen skal løbende vurdere tilgængelige sikkerhedsrettelser, fx patches eller hot-fixes, til anvendte operativsystemer og applikationer. Udrulning og installation af kritiske sikkerhedsrettelser på relevante systemer skal foretages hurtigst muligt og normalt senest en uge efter vurdering og positiv funktions- og kompatibilitetstest.

STØRRE OPERATIVSYSTEMOPDATERINGER, FX "SERVICE PACKS"

Når større opdateringer, fx "service packs", er gjort tilgængelige fra leverandører, skal it-afdelingen vurdere, om disse skal installeres. Opdateringer i kritiske systemer skal testes grundigt for kompatibilitet med anvendte applikationer, inden opdateringerne installeres i produktionsmiljøet.

SOFTWAREOPDATERINGER GENERELT

It-afdelingen skal holde sig informeret om programrettelser til programmer, der anvendes på AAU og snarest installere disse på alle computere, fx servere og arbejdsstationer, når det vurderes, at rettelserne har positiv indflydelse på den samlede sikkerhed. Systemejere er ansvarlige for, at der løbende sker regelmæssig opdatering af anvendt software.

ÆNDRINGER I KRITISKE SYSTEMER

Alle ændringer i kritiske systemer skal udføres efter godkendt procedure i.h.t. ITIL standarden. Alle procedurer skal indeholde en alternativ plan til retablering af det kritiske system. Vilklårene for aktivering af den alternative plan skal ligeledes fremgå af proceduren.

8.7.1 KONTROLLER I FORBINDELSE MED AUDIT AF INFORMATIONSSYSTEMER

SIKKERHED I FORBINDELSE MED REVISION

Revisionskrav og revisionshandlinger i forbindelse med systemer i drift skal planlægges omhyggeligt og aftales med de involverede for at minimere risikoen for forstyrrelser af AAU's forretningsaktiviteter.

De planlagte revisionshandlinger må kun omfatte læseadgang til systemer og data. Hvis revisionen nødvendiggør mere end læseadgang, må dette kun tillades på kopier af de berørte filer, der skal slettes efter brug. Al adgang i forbindelse med revision skal logges. De personer, der udfører revisionen, skal være uafhængige af det reviderede område.

BESKYTTELSE AF REVISIONSVÆRKTØJER

Adgangen til revisionsværktøjer skal begrænses for at forhindre misbrug.

9. Kommunikationssikkerhed

9.1 Styring af netværkssikkerhed

9.1.1 NETVÆRKSSTYRING

INSTALLATION AF NETVÆRKSUDSTYR

Installation af netværksudstyr skal koordineres gennem netværksgruppen.

OPSÆTNING AF TRÅDLØSE ADGANGSPUNKTER (ACCESS POINTS)

Trådløse netværk må alene opsættes efter aftale med den centrale netværksgruppe.

TILSLUTNING AF Udstyr til netværk

It-afdelingen skal udarbejde og publicere regler for tilslutning af udstyr til lokalnetværket.

INDKOMMENDE NETVÆRKSFORBINDELSER

Lokalnetværk tilstræbes opdelt i zoner med en veldefineret filterpolitik mellem zonerne. Filterpolitikken skal sikre, at der kun bliver åbnet adgang til nødvendige tjenester og ressourcer (servere, pc'er m.m.). Filtreringen kan foretages centralt eller lokalt.

SIKRING AF NETVÆRK

Netværksgruppen har det overordnede ansvar for at beskytte AAU's netværk.

BRUG AF TRÅDLØSE LOKALNETVÆRK

Studerende og ansatte på AAU anbefales at benytte det trådløse netværk AAU-1x. [Læs nærmere om trådløse netværk her.](#)

INSTALLATION AF TRÅDLØST Udstyr

Trådløst netværk (access points) må ikke opsættes på campus uden forudgående aftale med it-afdelingens netværksgruppe.

ADGANG TIL NETVÆRKET

Adgangen til AAU's netværk må kun ske gennem sikkerhedsgodkendte løsninger.

ADGANG TIL INFORMATIONER PÅ AAU'S NETVÆRK

Adgang til informationer på AAU's netværk skal foregå gennem sikkerhedsgodkendte løsninger og i henhold til informationernes klassifikation.

OPBEVARING AF FORTROLIGE ELLER FØLSOMME INFORMATIONER PÅ PRIVAT UDSTYR

Behandling eller opbevaring af følsomme eller fortrolige informationer på udstyr, der ikke tilhører AAU, skal overholde reglerne beskrevet for dataklassifikation.

9.1.2 SIKRING AF NETVÆRKSTJENESTER

BRUG AF KRYPTERING I FORBINDELSE MED INFORMATIONSDVEKSLING

Det kræves, at filer, der indeholder fortrolige eller følsomme informationer, altid er krypteret under transmission til modtagere udenfor AAU, jf. 10.1.1.

INTERNETBASEREDE TJENESTER

Det er tilladt at bruge internettjenester, der ikke indebærer forøgede sikkerhedsrisici.

FJERNSTYRING OG ADMINISTRATION

Forbindelser til fjernadministration til brug for vedligeholdelses- og supportopgaver må kun aktiveres, når de er nødvendige og efter anmodning til systemejereren.

9.2 Informationsoverførsel

—

9.2.1 POLITIKKER OG PROCEDURER FOR INFORMATIONSOVERFØRSEL

UDLEVERING AF FORTROLIGE INFORMATIONER OG OPLYSNINGER

Information der ikke er klassificeret "Offentlig", må ikke videregives til tredjepart i nogen form, uden godkendelse af dataejereren. Ønsker om agtindsigt bør henvises til ledelsessekretariatet (ved rektor/direktøren).

KRYPTERING AF ADMINISTRATIVE NETVÆRKSFORBINDELSER

Netværksforbindelser, der benyttes til administration af it-udstyr, skal krypteres, hvis det er muligt.

PROCEDURER FOR INFORMATIONSDVEKSLING

Den enkelte enhedsleder har ansvaret for, at der foreligger lokale retningslinjer og procedurer for enhver kritisk eller følsom form for informationsudveksling, både fysisk og elektronisk.

UDSKRIFTER

Brugerne skal afhente udskrifter med fortrolige og følsomme informationer straks. Hvor muligt benyttes Follow-You-printsystemet til udskrifter.

9.2.2 AFTALER OM INFORMATIONSOVERFØRSEL

AFTALER OM INFORMATIONSDVEKSLING

Ved udveksling af information og software imellem AAU og tredjepart, skal AAU's regler i forbindelse med klassifikation af informationer overholdes.

9.2.3 ELEKTRONISKE MEDDELELSER

ELEKTRONISK UDVEKSLING AF POST OG DOKUMENTER

Fortrolige og følsomme informationer skal altid sendes krypteret, når de behandles elektronisk udenfor AAU's netværk.

AUTENTIFICERING

Brugere skal være opmærksomme på, at kommunikation via sociale tjenester på internettet kan være usikkert og derfor ikke giver vished for, hvem du kommunikerer med.

VEDHÆFTEDE FILER

It-afdelingen kan vælge at blokere for filtyper, som vurderes farlige eller u hensigtsmæssige.

PHISHING OG BEDRAGERI

Som en del af den løbende awareness-træning gøres brugere opmærksomme på "phishing" og "social engineering", der fx kan betyde, at de modtager tilsyneladende oprigtige e-mails, der forsøger at franarre værdifulde oplysninger eller forsøger at få brugeren til at foretage uønskede handlinger.

FORTROLIG MAIL

E-mail med fortroligt eller følsomt indhold, der sendes til eksterne modtagere, skal krypteres med en anerkendt metode, jf. 10.1.1.

MEDARBEJDERES PRIVATE BRUG AF E-MAIL

Medarbejderne må anvende mailsystemerne til personligt brug i begrænset omfang, hvis dette ikke har indflydelse på AAU's drift og sikkerhed i øvrigt. Private e-mails skal gemmes i en folder med navnet: "PRIVAT".

AAU'S INFORMATIONER PÅ SOCIALE NETVÆRK

Kun offentlige informationer må deles på et eksternt socialt netværk.

PRIVAT BRUG AF INTERNETADGANG

AAU's internetadgang må anvendes til private formål, såfremt sikkerhedspolitikken i øvrigt overholdes, og såfremt arbejdsrelateret brug ikke generes på nogen måde.

BEHANDLING AF PERSONDATA

Behandling af persondata og procedure ved utilsigtet offentliggørelse af information på internettet er beskrevet i AAU's privatlivspolitik.

OPBEVARING OG SLETNING AF E-MAIL

E-mail, der indeholder persondata, skal behandles i overensstemmelse med den gældende persondatalov.

INTEGRITET AF MEDDELELSER

Hvis der er behov for verifikation af en meddelelses integritet, kan der stilles krav om brug af medarbejdercertifikat eller lignende løsning til signering af sådanne meddelelser.

SPAM-MAIL BESKYTTELSE

AAU bortfiltrerer e-mails, der opfylder AAU's kriterier for spam-mails.

9.2.4 FORTROLIGHEDS- OG HEMMELIGHOLDELSAFTALER

INDHOLD AF TAVSHEDSERKLÆRINGERNE

Skabelon for en tavshedserklæring definerer kravene til indholdet i erklæringerne.

TAVSHEDSERKLÆRING FOR TREDJEPART

Enhedslederen skal sikre, at tredjepart med adgang til systemer og informationer er omfattet af krav til fortrolighed.

10. Anskaffelse, udvikling og vedligeholdelse af systemer

10.1 Sikkerhedskrav til informationssystemer

10.1.1 ANALYSE OG SPECIFIKATION AF INFORMATIONSSIKKERHEDSKRAV

SIKKERHED I APPLIKATIONSUDVIKLING

Informationssikkerhed og herunder persondataskyttelse skal inkluderes som en integreret del af alle udviklingsprojekter.

ANSKAFFELSESPROCEDURER

Enhedslederen skal sikre, at nyanskaffelser ikke giver anledning til konflikt med eksisterende krav i vedtagne politikker. Dette dokumenteres i en risikovurdering.

Hvor anskaffelser giver anledning til forøget risiko for sikkerhedshændelser, skal ledelsen acceptere dette.

10.1.2 SIKRING AF APPLIKATIONSTJENESTER PÅ OFFENTLIGE NETVÆRK

SIKRING AF APPLIKATIONER PÅ OFFENTLIGE NETVÆRK

Der skal benyttes sikre autentifikations- og autorisationsprocesser for at sikre servicetransaktioner over offentlige netværk. Informationers integritet og fortrolighed skal sikres, når der benyttes applikationsservices over offentlige netværk ved hjælp af fx:

- Kryptografiske løsninger (såsom SSL, SFTP, HTTPS, sikre API'er eller webservices)
- Integritetssikring (fx hashing)

10.1.3 BESKYTTELSE AF HANDELSAPPLIKATIONER OG -TJENESTER

ONLINE TRANSAKTIONER

Systemer, hvor eksterne brugere tilbydes mulighed for direkte opdatering i AAU's databaser, skal have særlige sikringsforanstaltninger for at forhindre transmissionsfejl, fejladressering, manipulation samt uautoriseret adgang og gentagelse af allerede gennemførte transaktioner.

ELEKTRONISK HANDEL

Informationer vedrørende elektronisk handel over offentlige net skal beskyttes mod svindel, kontraktlige uoverensstemmelser, uautoriseret adgang og ændringer. AAU skal for at sikre sin elektroniske handel iværksætte en række forskellige foranstaltninger. Det omfatter et sæt handelsbetingelser, som er tilgængelige, forstået og accepteret af kunden, og hvoraf det fremgår, hvordan autenticitet fastslås, hvem der fastsætter priserne og hvad kravene til

fortrolighed, integritet og tilgængelighed er. Beskyttelsen skal gælde såvel informationsudvekslingen som de systemer, der anvendes til at lagre eller behandle data.

10.2 Sikkerhed i udviklings- og hjælpeprocesser

10.2.1 SIKKER UDVIKLINGSPOLITIK

VALIDERING AF INDDATA

Data der sendes ind i systemerne, skal valideres for korrekthed. Periodisk gennemgang af nøgledata skal bekræfte deres validitet og integritet. Der testes om data virker plausible, før de sendes ind i systemerne. Der skal genereres log over de aktiviteter, der sender data ind i systemet.

Datavalidering skal beskytte aktiver mod inddatafejl. Inddata skal valideres for at sikre, at de overholder formelle formatkrav, fx kontrol af datoformat og cpr-numre.

DATABASEINTEGRITET

Det skal vurderes, om de anvendte dataopdateringsprocedurer sikrer dataintegritet.

10.2.2 PROCEDURER FOR STYRING AF SYSTEMÆNDRINGER

10.2.3 TEKNISK GENNEMGANG AF APPLIKATIONER EFTER ÆNDRING AF DRIFTSPLATFORME

GENNEMGANG AF SYSTEMER EFTER ÆNDRINGER

Før driftsmiljøerne ændres, skal kritiske forretningssystemer gennemgås og testes for at sikre, at det ikke har utilsigtede afledte virkninger på AAU's daglige drift. Ved eksternt tilgængelige systemer og særligt kritiske systemer skal det altid ud fra en risikomæssig vurdering overvejes, om der skal foretages en egentlig penetrationstest via eksternt uafhængig tredjepart.

10.2.4 BEGRÆNSNING AF ÆNDRINGER AF SOFTWAREPAKKER

ÆNDRINGER I STANDARDSYSTEMER

Ændringer i eksternt leverede standardsystemer skal begrænses til nødvendige ændringer og sådanne ændringer skal styres omhyggeligt, og vurderes i forhold til eventuelle kompatibilitetsproblemer med anden software, der anvendes i AAU. Indbyggede sikringstiltag, fx logning samt adgangs- og integritetskontrol, bør gennemgås for at sikre, at de ikke er kompromitterede.

Det skal vurderes i hvor høj grad AAU vil blive ansvarlig for den fremtidige vedligeholdelse af softwaren.

10.2.5 PRINCIPPER FOR UDVIKLING AF SIKRE SYSTEMER

SIKKERHEDSKRAV TIL INFORMATIONSBEHANDLINGSSYSTEMER

AAU's kravspecifikationer til såvel nye som bestående systemer skal omfatte informationssikkerhed og herunder persondataskyttelse, som afpasses i henhold til konkrete risikovurderinger for løsningen.

SIKKERHED I SYSTEMPLANLÆGNING

Ved planlægning af systemer skal informationssikkerhedsbetragtninger altid medtages i overvejelserne.

Informationssikkerhedskrav skal tages i betragtning ved både design, test, implementering og opgradering af it-systemer samt ved systemændringer.

SPECIFIKATION AF SIKKERHEDSKRAV

Alle nye informationsaktiver og tilhørende systemer skal klassificeres og risikovurderes. Tilsvarende gælder ved enhver større ændring til eksisterende systemer.

KONTROL AF INTERN DATABEHANDLING

Validerings- og afstemningskontroller skal indbygges i systemerne for at afsløre inkonsistens og sikre dataintegritet. Kontrolniveauet afhænger af informationernes klassificering og skal beskrives i kravspecifikationen.

10.2.6 SIKKERT UDVIKLINGSMILJØ

SIKRING AF UDVIKLINGSMILJØER

Ved risikovurdering af systemudvikling bør følgende overvejes:

- Omfanget af fortrolige og følsomme informationer
- Lovkrav
- Adskillelse af udviklings-, test og produktionsmiljøer
- Politikker for adgangskontrol og revisionsspor
- Sikker udveksling af informationer mellem systemer og mellem udvikling, test og produktion og eventuelle eksterne parter
- Sikker lagring af backup
- Revisionsspor af ændringer i miljøer

Sikkerhedskravene bør identificere alle relevante sikkerhedsaspekter ved behandling af informationer. Analysen af sikkerhedskrav skal desuden tage hensyn til følgende:

- Krav til adgangstildeling og godkendelsesprocesser
- Understøttelse af rollebaseret adgang
- Krav fra andre systemgrænseflader
- Krav til logning
- Kompatibilitet med andre systemer og sikkerhedsløsninger

10.2.7 OUTSOURCET UDVIKLING

SYSTEMUDVIKLING UDFØRT AF EKSTERN LEVERANDØR

AAU kræver adgang til at overvåge udviklingsprocessen, gennemførelse af afleveringstest samt dokumenteret løbende kvalitetssikring.

Udvælgelse af leverandør skal overvejes grundigt for at sikre stabil udvikling og vedligeholdelse. Der skal udformes funktionskrav til systemer, herunder specifikation af inddata- og driftsvalidering og netværkstyring. Forholdene omkring ejerskab af eller brugsrettigheder til systemet og informationer skal fremgå i den aftale, der laves med leverandøren. Det skal overvejes, om det vil være hensigtsmæssigt, at der indgås en vedligeholdelsesaftale med leverandøren.

EKSTERN REVISION AF OUTSOURCING-PARTNERE

Outsourcing-partnere skal sørge for ekstern revision mindst en gang om året og skal på anfordring kunne fremvise revisionserklæringen.

10.2.8 SYSTEMSIKKERHEDSTEST

10.2.9 SYSTEMGODKENDELSESTEST

GODKENDELSE AF NYE ELLER ÆNDRERE SYSTEMER

It-afdelingen skal etablere en godkendelsesprocedure for nye systemer, nye versioner og for opdateringer af eksisterende systemer samt de afprøvninger, der skal foretages, inden de kan godkendes og sættes i drift.

10.3 Testdata

10.3.1 SIKRING AF TESTDATA

SIKRING AF TESTDATA

Data til test skal udvælges, kontrolleres og beskyttes omhyggeligt og i henhold til deres klassifikation. Kopiering af data fra et driftsmiljø til et testmiljø, skal godkendes af dataejer, og persondata skal som udgangspunkt altid anonymiseres. Kopiering og brug af data fra driftsmiljøet til test skal logges for at sikre kontrolsporet.

Beslutninger omkring brug af helt eller delvist komplette data fra et driftsmiljø skal altid dokumenteres.

11. Leverandørforhold

11.1 Informationssikkerhed i leverandørforhold

11.1.1 INFORMATIONSSIKKERHEDSPOLITIK FOR LEVERANDØRFORHOLD

INFORMATION TIL EKSTERNE PARTNERE

Tredjepart skal gøres opmærksom på det ønskede sikkerhedsniveau, eventuelt i form af adgang til gældende politikker.

VURDERING OG GODKENDELSE AF OUTSOURCING-LEVERANDØR

Leverandøren skal kunne dokumentere et tilfredsstillende sikkerhedsniveau.

11.1.2 HÅNDTERING AF SIKKERHED I LEVERANDØRAFTALER

OUTSOURCING-PARTNERE

Inden indgåelse af aftaler skal sikkerhedsniveauet ved partneren afklares og godkendes af system- og dataejerne. Der skal foreligge en ISO/IEC 27001-certificering, en ISAE 3402/3401-revisionserklæring fra outsourcing partnere eller tilsvarende relevant dokumentation for efterlevelse af et passende sikkerhedsniveau.

SIKKERHED VED SAMARBEJDE MED PARTNERE

Risici ved brug af eksterne serviceleverandører skal vurderes og dokumenteres før etablering af et samarbejde og sikkerhedsforanstaltninger skal aftales og fremgå af kontrakten. Ved integration af AAU's systemer og processer med tredjepart er kravene til sikkerhedsforanstaltninger højere.

SIKKERHEDSVURDERING AF TREDJEPART

Der skal altid udføres en sikkerhedsvurdering af relevante tredjeparter før etablering af et samarbejde med en leverandør.

HÅNDBLIVNING AF SIKKERHED I PROCEDURER FOR LEVERANDØRAFTALER

Relevante sikkerhedskrav skal identificeres og aftales med leverandører, der har adgang til, behandler, opbevarer eller leverer it-infrastruktur til organisationens informationsaktiver. Kravene indeholder (men er ikke begrænset til):

- Beskrivelse af de relevante informationsaktiver
- Tilpasning af organisationens og leverandørers klassifikationssystemer
- Identifikation af lovkrav, såsom regler for databeskyttelse, ophavsret, intellektuel ejendomsret og overholdelse af industrikrav (PCI DSS, ISO/IEC 27001)
- Politikker for acceptabel brug
- Hændelsesstyring og BCM-krav
- Sikkerhedskrav for logisk og fysisk adgang
- Sikkerhedskrav for udveksling af data og informationer
- Retten til at udføre revision
- Leverandørens forpligtelse til at være i overensstemmelse med organisatoriske sikkerhedspolitikker
- Awareness- og uddannelsesprogrammer.

11.1.3 FORSYNINGSKÆDE FOR INFORMATIONS- OG KOMMUNIKATIONSTEKNOLOGI

NETVÆRKSSIKKERHED - OUTSOURCING-LEVERANDØR

Leverandøren skal sikre en hensigtsmæssig opbygning af netværk, firewall, segmentering og kryptering.

11.2 Styring af leverandørydelser

—

11.2.1 OVERVÅGNING OG GENNEMGANG AF LEVERANDØRYDELSER

OVERVÅGNING OG AUDIT - CLOUDLØSNING

Udbyderen skal kunne dokumentere et passende sikkerhedsniveau, eksempelvis en revisionserklæring, et intern audit, ISO/IEC 27001-certificering, outsourcing-revisionserklæring eller tilsvarende. Udbyderen skal kunne levere rapportering for, i hvilken grad aftalte servicemål er opfyldt. AAU skal vurdere, i hvilket omfang egen auditering af leverandøren er nødvendig.

11.2.2 STYRING AF ÆNDRINGER AF LEVERANDØRYDELSER

STYRING AF ÆNDRINGER HOS SERVICELEVERANDØREN

Det skal sikres, at ændringsstyring af serviceleverandørens ydelser følger samme retningslinjer som AAU's egne.

12. Styring af informationssikkerhedsbrud

12.1 Styring af informationssikkerhedsbrud og forbedringer

12.1.1 ANSVAR OG PROCEDURER

INFORMATION OM SIKKERHEDSHÆNDELSER

AAU skal informere berørte parter om eventuelle informationssikkerhedshændelser under iagttagelse af gældende lovkrav. Enhedslederen for det pågældende hovedområde eller informationssikkerhedschefen bør godkende sådanne informationer, inden de udsendes eksternt.

ANSVAR OG FORRETNINGSGANGE FOR SIKKERHEDSHÆNDELSER

CISO er sammen med ITS ansvarlig for at fastlægge forretningsgange, der sikrer en hurtig, effektiv og metodisk håndtering af informationssikkerhedsbrud.

TILGÆNGELIGHEDSHÆNDELSER

Hændelser, der har indflydelse på tilgængelighed, skal afklares i henhold til gældende driftsaftaler (SLA). Driftshændelser, der ikke kan afklares inden for aftalt tid, skal udløse procedurer for hændeshåndtering og evt. beredskabsplaner. De ramte brugere, system og dataejere skal informeres.

12.1.2 RAPPORTERING AF INFORMATIONSSIKKERHEDSHÆNDELSER

RAPPORTERING AF FORMODEDE SIKKERHEDSHÆNDELSER

Ved konstatering af, eller mistanke om, brud på informationssikkerhedsforanstaltninger, skal dette straks rapporteres til den nærmeste leder og til ITS via formularen for sikkerhedshændelser. Undtagelsesvis direkte til ITS support (support@its.aau.dk eller tlf.: 9940 2020). Såvel AAU som eksterne tjenesteudbydere er forpligtede til at indberette enhver observeret sikkerhedshændelse eller mistanke herom. Der bør være let adgang til rapportering af disse hændelser. Alle sikkerhedshændelser skal dokumenteres i gældende supportværktøj og arkiveres jf. gældende lovgivning, pt. i 5 år.

12.1.3 RAPPORTERING AF INFORMATIONSSIKKERHEDSSVAGHEDER

RAPPORTERING AF PROGRAMFEJL

Brugere, der observerer programfejl, som de ikke har oplevet før, skal rapportere dette til support@its.aau.dk tlf.: 9940 2020.

12.1.4 VURDERING AF OG BESLUTNING OM INFORMATIONSSIKKERHEDSHÆNDELSER

VURDERING AF TIDLIGERE HÆNDELSER

Informationssikkerhedsudvalget skal regelmæssigt gennemgå den forgangne periodes hændelser og på denne baggrund anbefale, hvorvidt informationssikkerheden kan forbedres.

Dette kan udmunde i en opdateret risikovurdering, samt forslag til nye eller ændrede tekniske, fysiske eller adfærdsmæssige foranstaltninger.

OPFØLGNING PÅ RAPPORTEREDE SIKKERHEDSHÆNDELSER

ITS Support er ansvarlig for at indsamle data til statistik for rapporterede informationssikkerhedshændelser.

12.1.5 HÅNDBLING AF INFORMATIONSSIKKERHEDSBRUD

ITS skal i samarbejde med CISO sørge for at udarbejde procedurer for håndtering af informationssikkerhedsbrud, herunder fejlafhjælpning, kontrolleret reetablering efter et brud og kommunikation til interne og eksterne personer, organisationer eller myndigheder.

12.1.6 ERFARING FRA INFORMATIONSSIKKERHEDSBRUD

KONTROL OG OPFØLGNING PÅ SIKKERHEDSBRUD

Brud på informationssikkerheden og uautoriseret adgang til systemer og informationer skal registreres.

12.1.7 INDSAMLING AF BEVISER

INDSAMLING AF BEVISER

Hvis et sikkerhedsbrud afstedkommer et retsligt efterspil - uanset om sikkerhedsbruddet er foretaget af en person eller en virksomhed - skal der indsamles, opbevares og præsenteres et fyldestgørende bevismateriale. Sikring af beviser er vanskeligt, og der bør i hvert enkelt tilfælde koordineres med eksperter på området. En forkert fremgangsmåde kan resultere i, at beviser bliver forkastet i retten.

KONTAKT MED RELEVANTE MYNDIGHEDER

Enhedslederen har ansvaret for kontakt med eksterne parter i informationssikkerhedssager.

13. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

13.1 Informationssikkerhedskontinuitet

–

13.1.1 PLANLÆGNING AF INFORMATIONSSIKKERHEDSKONTINUITET

NØDPROCEDURER FOR KRITISKE PROCESSER OG SYSTEMER

Der skal, for alle forretningskritiske processer og systemer, eksistere en opdateret nødprocedure (beredskabsplan), der kan sættes i drift og som løbende bliver testet. Det skal være klart defineret, hvem der har ansvaret for at aktivere nødplaner.

RAMME FOR BEREDSKABSPLANER

Med afsæt i forretningskonsekvensanalyser udarbejdes en beredskabsplan for de mest forretningskritiske systemer for at minimere konsekvenserne for informationssikkerheden af ulykker og fejl i AAU. Beredskabsplanen skal indeholde og adressere alle forretningskritiske systemer.

Ledelsen skal fastlægge en ensartet ramme for AAU's beredskabsplan for at sikre, at den er sammenhængende og tilgodeser alle sikkerhedskrav, samt at den fastlægger prioriteringen af afprøvning og vedligeholdelse. Beredskabsplanen skal afspejle muligheden for, at de fysiske lokationer kan være utilgængelige eller ødelagt.

13.1.2 IMPLEMENTERING AF INFORMATIONSSIKKERHEDSKONTINUITET

AKTIVERING AF BEREDSKABSPLANEN

Det skal være klart defineret, hvem der har ansvaret for aktivering af beredskabsplanen. Medarbejdere, der udgør en del af beredskabsplanen, skal være informeret om dette ansvar. Alle medarbejdere skal være informeret om beredskabsplanens eksistens.

13.1.3 VERIFICER, GENNEMGÅ OG EVALUER INFORMATIONSSIKKERHEDSKONTINUITETEN

UDDANNELSE I BEREDSKABSPLANER

ITS har ansvaret for, at der foregår en tilstrækkelig uddannelse af medarbejdere i de aftalte beredskabsprocedurer, inklusive krisehåndtering.

AFPRØVNING OG VEDLIGEHOLDELSE AF BEREDSKABSPLANER

Beredskabsplaner skal løbende afprøves og opdateres for at sikre, at de er tidssvarende og effektive. Afprøvning af beredskabsplaner skal omfatte mindst én af følgende:

- En skrivebordstest af de forskellige scenarier.
- Simuleringer (med henblik på at træne deltagerne i håndtering af deres roller efter episoden).
- Teknisk retablering (sikring af at tekniske systemer kan retableres effektivt).
- Retablering i andre lokaler end de oprindelige (gennemførelse af parallel drift i andre lokaler).

OPDATERING AF KATASTROFEPLANER

Mindst 1 gang om året skal beredskabsplaner gennemgås med henblik på opdatering.

13.2 Redundans

—

13.2.1 TILGÆNGELIGHED AF INFORMATIONSBEHANDLINGSFACILITETER

AAU tager løbende stilling til forretningskravene til tilgængeligheden af informationssystemer med henblik på at kunne indarbejde tilstrækkelig redundans i informationssystemerne.

14. Overensstemmelse

14.1 Overensstemmelse med lov- og kontraktkrav

—

14.1.1 IDENTIFIKATION AF GÆLDENDE LOVGIVNING OG KONTRAKTKRAV

OPBEVARING OG BEHANDLING AF PERSONOPLYSNINGER

AAU har udarbejdet en særskilt politik for behandling af personoplysninger: AAU's privatlivspolitik.

KONTROL AF OVERHOLDELSE AF PERSONDATALOVGIVNING

Enhedslederen har ansvaret for, at gældende persondatalovgivning overholdes lokalt i enheden.

SPORBARHED

Behandling af personrelaterede informationer skal så vidt muligt logges automatisk således, at det er muligt for en revisor/auditor at kontrollere hvem, der har arbejdet med hvilke informationer på hvilke tidspunkter.

14.1.2 IMMATERIELLE RETTIGHEDER

RETNINGSLINJER FOR OPHAVSRETTIGHEDER

Ledelsen har det overordnede ansvar for, at AAU fastholder en passende opmærksomhed på at beskytte tredjeparts ophavsrettigheder. Den enkelte bruger er ansvarlig for til enhver tid at overholde gældende lovgivning for ophavsrettigheder. Der skal vedligeholdes dokumentation for ejendomsretten af licenser, originalmateriale og manualer.

Der skal løbende kontrolleres, at software-licensaftaler overholdes, fx at eventuelle begrænsninger i antal brugere, servere eller kopier overholdes. Der skal løbende kontrolleres, at der kun er installeret autoriserede systemer med autoriserede licenser på AAU's udstyr.

ADMINISTRATION AF SOFTWARELICENSER

Registrering af softwarelicenser sker gennem it-afdelingen. Det er det enkelte hovedområdes enhedsleders overordnede ansvar at sikre et tilstrækkeligt antal licenser inden for dennes hovedområde. Brug af software-licenser skal koordineres med it-afdelingen eller den ansvarlige for styring af licenser i enheden.

Medarbejdere må ikke forpligte AAU ved at acceptere licensvilkår i software, som ikke er accepteret af den enkelte enhed. De enkelte enheder skal lokalt registrere, hvilke licenserede programmer, der findes på enhedens it-systemer. Licensregistre skal løbende ajourføres og med fordel i en specialiseret softwareløsning hertil.

14.1.3 BESKYTTELSE AF REGISTRERINGER

LAGRING AF SYSTEMDOKUMENTATION

Systemdokumentation skal opbevares, så længe systemet benyttes til udvikling, test eller drift.

BESKYTTELSE AF SYSTEMDOKUMENTATION

Systemejere skal beskytte systemdokumentation, hvilket bl.a. indebærer at antallet af adgangsrettigheder til systemdokumentation holdes på et minimum og godkendes af systemejeren.

LOVREGULEREREDE DATA

AAU skal beskytte lovregulerede informationer mod ændring, sletning, samt uautoriseret adgang.

OPBEVARING OG BEHANDLING AF DATA

Forretningskritiske informationer skal altid opbevares og behandles således, at integriteten ikke kan drages i tvivl.

14.1.4 PRIVATLIVETS FRED OG BESKYTTELSE AF PERSONOPLYSNINGER

Privatlivets fred og personoplysninger skal beskyttes i overensstemmelse med gældende lovgivning. Der skal implementeres regler for opbevaring, forsendelse, overførsel, videregivelse

og sletning af personoplysninger, som kommunikerer ud til alle ansatte, tilknyttede parter og studerende på AAU, der er involveret i behandlingen af personoplysninger.

14.1.5 REGULERING AF KRYPTOGRAFI

REGULERING PÅ KRYPTOGRAFIOMRÅDET

AAU skal efterleve nationale regler for kryptering. Dette gælder også for medarbejdere, der besøger andre lande, medbringende bærbart og mobilt udstyr.

OVERHOLDELSE AF LOVGIVNINGEN

Alle systemer skal overholde relevante lovmæssige krav.

14.2 Gennemgang af informationssikkerhed

14.1.1 IDENTIFIKATION AF GÆLDENDE LOVGIVNING OG KONTRAKTKRAV

OPBEVARING OG BEHANDLING AF PERSONOPLYSNINGER

AAU har udarbejdet en særskilt politik for behandling af personoplysninger: AAU's privatlivspolitik.

KONTROL AF OVERHOLDELSE AF PERSONDATALOVGIVNING

Enhedslederen har ansvaret for, at gældende persondatalovgivning overholdes lokalt i enheden.

SPORBARHED

Behandling af personrelaterede informationer skal så vidt muligt logges automatisk således, at det er muligt for en revisor/auditor at kontrollere hvem, der har arbejdet med hvilke informationer på hvilke tidspunkter.

14.1.2 IMMATERIELLE RETTIGHEDER

RETNINGSLINJER FOR OPHAVSRETTIGHEDER

Ledelsen har det overordnede ansvar for, at AAU fastholder en passende opmærksomhed på at beskytte tredjeparts ophavsrettigheder. Den enkelte bruger er ansvarlig for til enhver tid at overholde gældende lovgivning for ophavsrettigheder. Der skal vedligeholdes dokumentation for ejendomsretten af licenser, originalmateriale og manualer.

Der skal løbende kontrolleres, at software-licensaftaler overholdes, fx at eventuelle begrænsninger i antal brugere, servere eller kopier overholdes. Der skal løbende kontrolleres, at der kun er installeret autoriserede systemer med autoriserede licenser på AAU's udstyr.

ADMINISTRATION AF SOFTWARELICENSER

Registrering af softwarelicenser sker gennem it-afdelingen. Det er det enkelte hovedområdes enhedsleders overordnede ansvar at sikre et tilstrækkeligt antal licenser inden for dennes hovedområde. Brug af software-licenser skal koordineres med it-afdelingen eller den ansvarlige for styring af licenser i enheden.

Medarbejdere må ikke forpligte AAU ved at acceptere licensvilkår i software, som ikke er accepteret af den enkelte enhed. De enkelte enheder skal lokalt registrere, hvilke licenserede programmer, der findes på enhedens it-systemer. Licensregistre skal løbende ajourføres og med fordel i en specialiseret softwareløsning hertil.

14.1.3 BESKYTTELSE AF REGISTRERINGER

LAGRING AF SYSTEMDOKUMENTATION

Systemdokumentation skal opbevares, så længe systemet benyttes til udvikling, test eller drift.

BESKYTTELSE AF SYSTEMDOKUMENTATION

Systemejere skal beskytte systemdokumentation, hvilket bl.a. indebærer at antallet af adgangsrettigheder til systemdokumentation holdes på et minimum og godkendes af systemejeren.

LOVREGULEREDE DATA

AAU skal beskytte lovregulerede informationer mod ændring, sletning, samt uautoriseret adgang.

OPBEVARING OG BEHANDLING AF DATA

Forretningskritiske informationer skal altid opbevares og behandles således, at integriteten ikke kan drages i tvivl.

14.1.4 PRIVATLIVETS FRED OG BESKYTTELSE AF PERSONOPLYSNINGER

Privatlivets fred og personoplysninger skal beskyttes i overensstemmelse med gældende lovgivning. Der skal implementeres regler for opbevaring, forsendelse, overførsel, videregivelse og sletning af personoplysninger, som kommunikeres ud til alle ansatte, tilknyttede parter og studerende på AAU, der er involveret i behandlingen af personoplysninger.

14.1.5 REGULERING AF KRYPTOGRAFI

REGULERING PÅ KRYPTOGRAFIOMRÅDET

AAU skal efterleve nationale regler for kryptering. Dette gælder også for medarbejdere, der besøger andre lande, medbringende bærbart og mobilt udstyr.

OVERHOLDELSE AF LOVGIVNINGEN

Alle systemer skal overholde relevante lovmæssige krav.