Sikkerhedshåndbog

Godkendt af Informationssikkerhedsudvalget og gældende pr. 15. september 2018.

Indholdsfortegnelse

5 Informationssikkerhedspolitikker

5.1 Retningslinjer for styring af informationssikkerhed

5.1.1 Politikker for informationssikkerhed

Publicering af sikkerhedspolitik
Politik for Informationssikkerhed på AAU skal offentliggøres og kommunikeres til alle relevante interessenter, herunder alle medarbejdere.

5.1.2 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 informationssikkerhedspolitik 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.

6 Organisering af informationssikkerhed

6.1 Intern organisering

6.1.1 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
Ansvaret 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.

6.1.2 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.

6.1.3 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.

6.1.4 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.

6.1.5 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.

6.2 Mobilt udstyr og fjernarbejdspladser
6.2.1 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 uaflåste rum.

6.2.2 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.

7 Personalesikkerhed
7.1 Før ansættelsen
7.1.1 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.

7.1.2 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 ("Regler for ansvarlig it-brug ved Aalborg Universitet" og "it-kodeks for ansatte og studerende" kan findes på www.informationssikkerhed.aau.dk)

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.

7.2 Under ansættelsen

7.2.1 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.

7.2.2 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 informationssikkerhedshåndbogen med tilhørende bilag og supplerende retningslinjer.

7.2.3 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. (irettesættelse, advarsel, afskedigelse, inddragelse af retten til brug af AAU's netværk, bortvisning og i særlige tilfælde politianmeldelse.)

7.3 Ansættelsesforholdets ophør eller ændring
7.3.1 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.

8 Styring af aktiver
8.1 Ansvar for aktiver
8.1.1 Fortegnelse over aktiver
Der skal forelægge en oversigt over AAU's kritiske og følsomme informationsaktiver, som samtidig iagttager lovkrav vedr. fortegnelser over persondata.

8.1.2 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.

8.1.3 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. (se nærmere på http://informationssikkerhed.aau.dk/)

8.1.4 Tilbagelevering af aktiver

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

8.2 Klassifikation af information

8.2.1 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:

0. Offentlige: Informationer som er til rådighed for offentligheden eller hvor offentliggørelse ikke gør skade på AAU.
1. 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).
2. 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).
3. 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 dataejeren og efter dennes instruks.
- **Bruger**: Person eller organisation som anvender data.

8.2.2 Mærkning af information

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

Ansvar for adgangsrettigheder
Dataejer har ansvaret for at fastlægge og løbende revurdere adgangsrettigheder.

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

8.2.3 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.

8.3 Mediehåndtering

8.3.1 Styring af bærbare medier

Opbevaring og registrering af datamedier
Dataejeren 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..

8.3.2 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.

8.3.3 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.

9 Adgangsstyring

9.1 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 dataejere at indføre en mere striks politik, såfremt en risikovurdering fordrer dette.

9.1.1 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.

9.1.2 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 på http://www.its.aau.dk/vejledninger/wifi/.

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 netværksadgang
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.

9.2 Administration af brugeradgang

9.2.1 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.

9.2.2 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.

9.2.3 Styring af privilegerede adgangsrettigheder

Beskyttelse af adgange
Der skal altid benyttes adgangskode for adgange 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.

9.2.4 Styring af hemmelig autentifikationsinformation om brugere

Lagring af adgangskoder
Adgangskoder må aldrig lagres elektronisk i klartekst.

9.2.5 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.

9.2.6 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. Brugerne tildeles adgang til AAU alene ud fra et arbejds- og/eller studiebetinget 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 studiebetinget 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.

9.3 Brugernes ansvar

9.3.1 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 på http://www.sikkerhed.aau.dk

Krav til skift af adgangskode
Adgangskoder skal ændres ved mistanke om, at andre har fået kendskab til disse og mindst hvert halve år (marts 2015). 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 8 tegn og mindst 3 forskellige tegntyper (eksempelvis store og små bogstaver og tal). Adgangskoder med udvidede rettigheder, fx administratorer, skal indeholde mindst 10 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.

9.4 Styring af system- og applikationsadgang

9.4.1 Begrænset adgang til informationer

9.4.2 Procedurer for sikker log-on

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

9.4.3 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 inden for en fastlagt historik, fx de 20 senest benyttede.

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.

9.4.4 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.

9.4.5 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.

10 Kryptografi

10.1 Kryptografiske kontroller

10.1.1 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.

10.1.2 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.

11 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.

11.1 Sikre områder

11.1.1 Fysisk perimetersikring

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

11.1.2 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
Adgangskontrolkort er personlige. De skal opbevares forsvarligt og må ikke overdrages til tredjepart.

11.1.3 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.

11.1.4 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.

11.1.5 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.

11.1.6 Områder til af- og pålæsning

Af- og pålæsningsområder
Leverancer skal registreres i henhold til gældende varemodtagelsesprocedure.

11.2 Udstyr

11.2.1 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.

11.2.2 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".

11.2.3 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.

11.2.4 Vedligeholdelse af udstyr

Vedligeholdelse 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.

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

11.2.6 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.

11.2.7 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.

11.2.8 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.

11.2.9 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. Brugerne skal sikre, at fortrolige og følsomme udskrifter afhentes straks. Hvor muligt benyttes Follow-You printsystemet til udskrifter.

12 Driftssikkerhed

12.1 Driftsprocedurer og ansvarsområder

12.1.1 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.

12.1.2 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 systemejeren, 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.

12.1.3 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.

12.1.4 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.

12.2 Beskyttelse mod malware

12.2.1 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.

12.3 Backup

12.3.1 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 aftestes. 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.

12.4 Logning og overvågning
12.4.1 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 opfølgningslog
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.

12.4.2 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.

12.4.3 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.

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

12.5 Styring af driftssoftware
12.5.1 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.

12.6 Sårbarhedsstyring
12.6.1 Styring af tekniske sårbarheder

Rettelser 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 operativsystemopdatinger, 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. Vilkårene for aktivering af den alternative plan skal ligeledes fremgå af proceduren.

12.7 Overvejelser i forbindelse med audit af informationssystemer
12.7.1 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.

13 Kommunikationssikkerhed

13.1 Styring af netværkssikkerhed

13.1.1 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 på http://www.its.aau.dk/vejledninger/wifi/.

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.

13.1.2 Sikring af netværkstjenester

Brug af kryptering i forbindelse med informationsudveksling
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 systemejeren.

13.2 Informationsoverførsel

13.2.1 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 dataejeren. 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 informationsudveksling
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.

13.2.2 Aftaler om informationsoverførsel

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

13.2.3 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 uhensigtsmæssige.

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.

13.2.4 fortroligheds- og hemmeligholdelsesaftaler

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.

14 Anskaffelse, udvikling og vedligeholdelse af systemer

14.1 Sikkerhedskrav til informationssystemer

14.1.1 Analyse og specifikation af informationssikkerhedskrav

Sikkerhed i applikationsudvikling
Informationssikkerhed og herunder persondatabeskyttelse 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.

14.1.2 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)

14.1.3 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.

14.2 Sikkerhed i udviklings- og hjælpeprocesser

14.2.1 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.

14.2.2 Procedurer for styring af systemændringer

14.2.3 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 ekstern uafhængig tredjepart.

14.2.4 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.

14.2.5 Principper for udvikling af sikre systemer

Sikkerhedskrav til informationsbehandlingssystemer
AAU's kravspecifikationer til såvel nye som bestående systemer skal omfatte informationssikkerhed og herunder persondatabeskyttelse, 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.

14.2.6 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

14.2.7 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 netværksstyring. 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.

14.2.8 Systemsikkerhedstest
14.2.9 Systemgodkendelsestest

Godkendelse af nye eller ændrede 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.

14.3 Testdata
14.3.1 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 dataejeren, 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.

15 Leverandørforhold
15.1 Informationssikkerhed i leverandørforhold
15.1.1 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.

15.1.2 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.

Håndtering 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.

15.1.3 Forsyningskæde for informations- og kommunikationsteknologi

Netværkssikkerhed - outsourcing-leverandør
Leverandøren skal sikre en hensigtsmæssig opbygning af netværk, firewall, segmentering og kryptering

15.2 Styring af leverandørydelser
15.2.1 Overvågning og gennemgang af leverandørydelser

Overvågning og audit - cloudløsning
Udbyderen skal kunne dokumentere et passende sikkerhedsniveau, eksempelvis en revisionserklæring, et intern audit, ISOIEC 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.

15.2.2 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.

16 Styring af informationssikkerhedsbrud
16.1 Styring af informationssikkerhedsbrud og forbedringer
16.1.1 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 hændelseshåndtering og evt. beredskabsplaner. De ramte brugere, system og dataejere skal informeres.

16.1.2 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.

16.1.3 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.

16.1.4 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.

16.1.5 Håndtering af informationssikkerhedsbrud

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

16.1.6 Erfaring fra informationssikkerhedsbrud

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

16.1.7 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.

17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

17.1 Informationssikkerhedskontinuitet

17.1.1 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.

17.1.2 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.

17.1.3 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.

17.2 Redundans

17.2.1 Tilgængelighed af informationsbehandlingsfaciliteter

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

18 Overensstemmelse

18.1 Overensstemmelse med lov- og kontraktkrav

18.1.1 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.

18.1.2 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.

18.1.3 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.

18.1.4 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.

18.1.5 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.

18.2 Gennemgang af informationssikkerhed

18.2.1 Uafhængig gennemgang af informationssikkerhed

Mindst en gang årligt skal der udføres systematisk opfølgning på overholdelse af informationssikkerhedspolitikken. Hver enkelt enhedsleder skal løbende sikre, at informationssikkerhedspolitikken bliver overholdt inden for eget ansvarsområde.

18.2.2 Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder

18.2.3 Undersøgelse af teknisk overensstemmelse

Sikkerhedstest af interne it-systemer
Mindst en gang årligt skal der udføres uddybende test af informationssikkerhedsniveauet i internt netværksudstyr og servere.

Sikkerhedstest af eksterne it-systemer
Mindst en gang om året skal der udføres sikkerhedstests af kontroller og netværksforbindelser for at identificere og undgå uautoriserede adgangsforsøg.