AARHUS
UNIVERSITET

Informationssikkerhed

Informationssikkerhedspolitik og regler

Version 2.0

Dataklassifikation: Offentlig

AARHUS UNIVERSITET

Indholdsfortegnelse

AARHUS
UNIVERSITET

Rektors forord

Kære medarbejdere og studerende ved Aarhus Universitet.

Aarhus Universitet er en vidensvirksomhed. En stadig større del af vores viden skabes, behandles og gemmes på IT-systemer. Derfor skal alle, der har deres virke på AU, såvel forskere, undervisere og teknisk/administrativt personale som studerende have den størst mulige fokus på informationssikkerhed.

Informationssikkerhed betyder forskellige ting for forskellige mennesker. Denne håndbog prøver at komme rundt om alle væsentlige områder. Hvis du troede, at infomationssikkerhed bare er noget om vira og hackere, bør du studere politikken, reglerne og procedurerne nøje, der er langt flere aspekter.

Det systematiske infomationssikkerhedsarbejde hviler på 3 hovedsøjler - tilgængelighed, integritet og fortrolighed. At tilgængeligheden skal sikres bedst muligt er vist indlysende for alle. Et universitet - på linie med snart sagt alle moderne virksomheder - er nærmest paralyseret hvis IT-systemerne er nede. Tilsvarende er hele Universitetets virke baseret på vores integritet - der må ikke kunne stilles spørgsmålstegn ved den, så vores IT-systemer skal altid være retvisende. Og endelig må vi, selvom vi er sat i verden til at formidle viden, ikke være blinde for at betydelige dele af vores data indeholder følsomme eller fortrolige oplysninger som skal beskyttes. Det gælder f.eks. forskningsdata med følsomme personoplysninger eller fortrolige informationer til rådgivning og myndighedsbetjening

Så uanset hvad vores arbejde på Aarhus Universitet er - det være sig inden for forskning, uddannelse, overvågning, rådgivning, information eller administration - skal vi altid have øje for informationssikkerheden.

Informationssikkerhedshåndbogen for Aarhus Universitet udstikker spillereglerne for informationssikkerheden. Den udgør en integreret del af de regler og forordninger alle skal kende og overholde som betingelse for at være ansat eller indskrevet ved Universitetet.

Meget af det der står på disse sider er almindelig sund fornuft. Ting man godt ved i forvejen. Nu er det skrevet ned i en håndbog, som alle har pligt til at kende og efterleve.

Med venlig hilsen

Lauritz B. Holm-Nielsen

Rektor

AARHUS UNIVERSITET

Informationssikkerheds-politik for Aarhus Universitet

Indledning

Denne informationssikkerhedspolitik er den overordnede ramme for informationssikkerheden hos Aarhus Universitet. Som et led i den overordnede sikkerhedsstyring tager ledelsen på grundlag af den løbende overvågning og rapportering informationssikkerhedspolitikken op til revurdering minimum en gang om året.

Politikken omfatter Aarhus Universitets informationer, som er enhver information, der tilhører Aarhus Universitet herudover også informationer, som ikke tilhører Aarhus Universitet, men som Aarhus Universitet kan gøres ansvarlig for. Dette inkluderer fx alle data om personale, data om finansielle forhold, alle data, som bidrager til administrationen af Aarhus Universitet, samt informationer som er overladt Aarhus Universitet af andre, herunder forsøgs- og forskningsdata.

Denne politik omfatter alle Aarhus Universitets informationer, ligegyldigt hvilken form de opbevares og formidles på.

Formål

Informationer og informationsaktiver er nødvendige og livsvigtige for Aarhus Universitet, og informationssikkerheden har derfor stor betydning for Aarhus Universitets troværdighed og funktionsdygtighed.

Formålet med informationssikkerhedspolitikken er at definere en ramme for beskyttelse af Aarhus Universitets informationer og særligt at sikre, at kritiske og følsomme informationer og informationsaktiver bevarer deres fortrolighed, integritet og tilgængelighed.

Derfor har Aarhus Universitets ledelse besluttet sig for et beskyttelsesniveau, der er afstemt efter risiko og væsentlighed samt overholder lovkrav og indgåede aftaler, herunder licensbetingelser. Ledelsen vil oplyse medarbejdere og studerende om ansvarlighed i relation til Aarhus Universitets informationer og informationsaktiver.

Hensigten med informationssikkerhedspolitikken er endvidere at tilkendegive over for alle, som har en relation til Aarhus Universitet, at anvendelse af informationer og informationsaktiver er underkastet standarder og retningslinjer. På den måde kan sikkerhedsproblemer forebygges, eventuelle skader kan begrænses, og retablering af informationer kan sikres.

Omfang

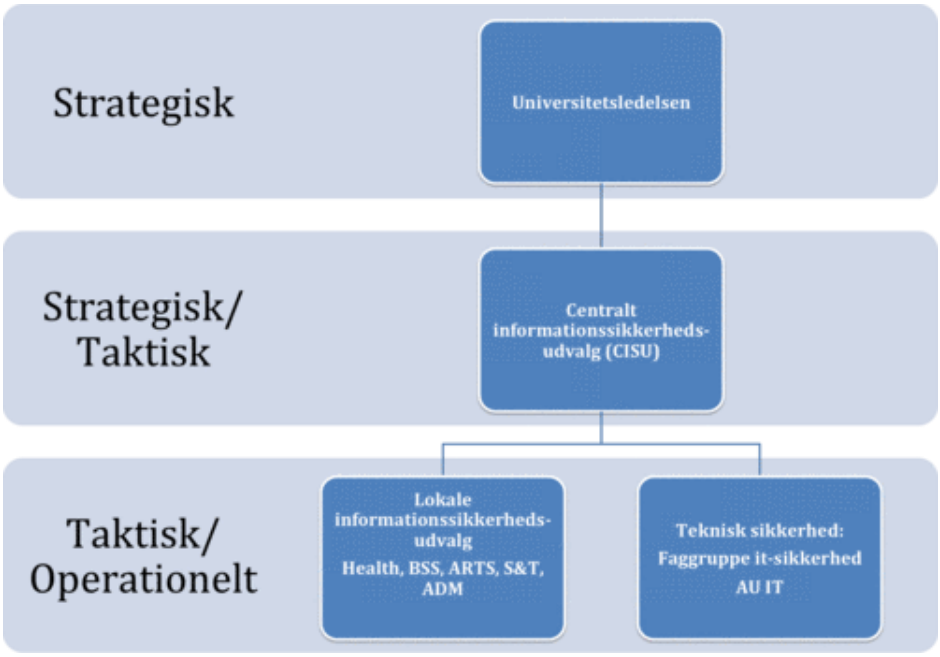
Denne politik gælder for alle ansatte uden undtagelse, både fastansatte og personer, som midlertidigt arbejder for Aarhus Universitet. Alle disse personer bliver her betegnet som medarbejderne.

Politikken gælder endvidere for studerende, der i forbindelse med deres studie anvender informationer og/eller informationsaktiver tilhørende Aarhus Universitet.

Ved udlicitering af dele af eller hele IT-driften skal det sikre, at Aarhus Universitets sikkerhedsniveau fastholdes, således at serviceleverandøren, dennes faciliteter og de medarbejdere, som har adgang til Aarhus Universitets informationer, mindst lever op til Aarhus Universitets informationssikkerhedsniveau.

Organisering af informationssikkerhedsarbejdet

Aarhus Universitet har organiseret sit informationssikkerhedsarbejde gennem en række informationssikkerhedsudvalg, jf. Figur 1.



Figur 1 - Organisering af informationssikkerhedsarbejdet

Det operationelle ansvar for den daglige styring af informationssikkerhedsindsatsen er placeret hos informationssikkerhedschefen. Denne sikrer i samarbejde med primært sikkerhedsudvalgene og sekundært vicedirektøren for it, at de aktiviteter, standarder, retningslinjer, kontroller og foranstaltninger, der er beskrevet i sikkerhedshåndbogen, gennemføres og efterleves. Ligeledes er det væsentligt, at informationssikkerhed integreres i alle forretningsgange, driftsopgaver og projekter.

De lokale informationssikkerhedsudvalg er ansvarlige for gennemførelsen af det arbejde som ligger i årshjulet, der er beskrevet i afsnit 1.8

Sikkerhedsniveau

Det er Aarhus Universitets politik at beskytte sine informationer og udelukkende tillade brug, adgang og offentliggørelse af informationer i overensstemmelse med Aarhus Universitets retningslinjer og under hensyntagen til den til enhver tid gældende lovgivning.

Aarhus Universitet fastlægger på baggrund af en risikovurdering et sikkerhedsniveau som svarer til betydningen af de pågældende informationer.

Der gennemføres mindst en gang årligt en risikovurdering, så ledelsen kan holde sig informeret om det aktuelle risikobillede. Der foretages ligeledes en risikovurdering ved større forandringer i organisationen, som har indflydelse på det samlede risikobillede.

Sikkerhedsniveauet fastlægges i det enkelte tilfælde under hensyntagen til arbejdets gennemførelse og økonomiske ressourcer. Målsætningen om et højt sikkerhedsniveau afvejes med ønsket om en hensigtsmæssig og brugervenlig anvendelse af it, samt det forhold at Universitetet har en samfundsrolle som leverandør af frit tilgængelig information.

Sikkerhedsbevidsthed

Informationssikkerhed vedrører Aarhus Universitets samlede informationsflow, og

gennemførelse af en informationssikkerhedspolitik kan ikke foretages af ledelsen alene. Alle medarbejdere og studerende har et ansvar for at bidrage til at beskytte Aarhus Universitets informationer mod uautoriseret adgang, ændring og ødelæggelse samt tyveri. Alle medarbejdere og studerende skal derfor løbende have information om informationssikkerhed i relevant omfang. Ansatte og studerende har ligeledes et ansvar for at behandle de informationsaktiver, der stilles til rådighed på en hensigtsmæssig måde.

Som brugere af Aarhus Universitets informationer skal alle medarbejdere og studerende følge informationssikkerhedspolitikken og de retningslinjer, der er afledt heraf. Medarbejderne og de studerende må kun anvende Aarhus Universitets informationer i overensstemmelse med det arbejde, de udfører for Aarhus Universitet, og skal beskytte informationerne på en måde, som er i overensstemmelse med informationernes klassifikation.

Brud på informationssikkerheden

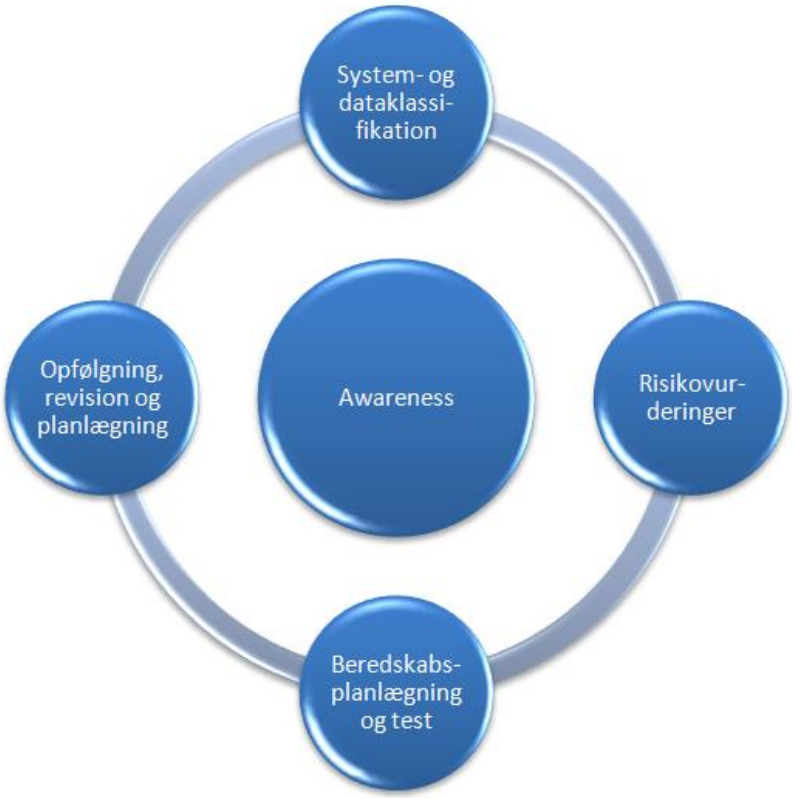
Såfremt en medarbejder eller en studerende opdager trusler mod informationssikkerheden eller brud på denne, skal dette meddeles til informationssikkerhedsafdelingen.

Overtrædelse af informationssikkerhedspolitikken, eller heraf afledte regler og retningslinier, indrapporteres til informationssikerhedsafdelingen, som i samarbejde med nærmeste leder og HR-afdelingen træffer afgørelse om eventuelle videre foranstaltninger. Det er lederens ansvar, at et eventuelt videre forløb sker i overensstemmelse med de almindelige fagretlige regler, herunder bl.a. at de relevante tillidsrepræsentanter inddrages. Hvis overtrædelsen er udført af en studerende, behandles sagen som enhver anden disciplinærsag.

Hvis overtrædelsen har karakter af strafferetlig, erstatningsretlig eller anden strafbar overtrædelse, vil der blive foretaget politianmeldelse.

Årshjul for informationssikkerhedsarbejdet

Aarhus Universitet har opstillet et årshjul som beskriver arbejdet med informationssikkerheden. Dette årshjul ser ud som følger:



Årshjulet omfatter 5 aktiviteter:

1. System- og dataklassifikation
2. Risikovurderinger
3. Beredskabsplanlægning og test
4. Opfølgning, revision m.v.
5. Awareness

Ansvaret for udførelsen af opgaverne ligger hos de lokale informationssikkerhedsudvalg på fakulteterne/administrationen. Informationssikkerhedsafdelingen kan facilitere processen, og stille relevante værktøjer til rådighed, men udførelsen ligger hos hovedområderne. Da det kræver et godt kendskab til de lokale forhold, anbefales det at arbejdet forankres på institutter og/eller forskningsgrupper m.v.

Alle aktiviteter i hjulet gennemføres en gang årligt, startende med system- og dataklassifikationen.

Awareness er en central del af arbejdet, som skal køre hele året. Denne del varetages af informationssikkerhedsafdelingen, i samarbejde med informationssikkerhedsudvalgene.

Informationssikkerhedsregler for Aarhus Universitet

Indledning

Baggrund for arbejdet med informationssikkerhed på AU	Aarhus Universitet skal i lighed med andre statslige organisationer overholde standarden DS484:2005, som definerer en række krav til informationssikkerheden på universitetet. Kravet om overholdelse af DS484:2005 trådte i kraft d. 1. januar 2007. Fremadrettet bliver kravet, at man overholder ISO27001 standarden, og AU er derfor ved at skifte fokus fra DS484:2005 til de standarder, der findes i ISO27000 serien.
Definition på Informationssikkerhed	Informationssikkerhed defineres som de samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og intregritet af universitetets informationer, aktiver og data.
Ordforklaringer	Bør: Ordet bør anvendes flere steder i denne håndbog. Generelt gælder det at bør = skal, medmindre der er givet dispensation herfor, eller omkostningerne ved gennemførelse overstiger gevinsten. Hvis man fraviger fra anbefalingen skal man således enten søge dispensation, eller godtgøre at det ikke kan betale sig. Arbejdsmæssig brug: Formuleringen "arbejdsmæssig brug", dækker, hvor intet andet er nævnt, også over studerendes studiemæssige brug. Det samme gælder for formuleringen "arbejdsrelateret brug". Outsoucing: Ordet outsourcing dækker over de tilfælde, hvor hele eller dele af it-understøttelsen drives af et eksternt firma. Outsourcing dækker således også over Cloud Computing, hvor man køber sig til ydelser hos 3.mand, fx email, webservere, regnekraft m.v. Mobile enheder: Mobile enheder anvendes som en samlet betegnelse for

	mobiltelefoner, smartphones, tablets o.lign. Bærbare pc'er, netbooks, laptops o.lign. er er ikke dækket af ordet mobile enheder, men benævnes i stedet bærbare pc'er. Informationsaktiver: Informationsaktiver er alle de systemer m.v. som indeholder, genererer eller bearbejder informationer. Det gælder fx pc'er, servere, mobile enheder, bærbare pc'er, frysebokse, kølerum, serverrum o.s.v.

1. Organisation og implementering

Placering af ansvar er nødvendigt for at sikre opmærksomhed på Universitetets informationsaktiver. Organisationsstrukturen på Universitetet og samarbejde med eksterne partnere er vigtig for at opretholde et tidssvarende sikkerhedsniveau. Kontrakter med partnere og andre aftaler er ligeledes et område, der har indflydelse på informationssikkerheden.

1.1 Risikobevidsthed

Risikoanalyse	Aarhus Universitet klassificerer sine systemer i A, B og C systemer. For type A systemer skal der udarbejdes både en risikoanalyse og en beredskabsplan, for type B systemer skal der udarbejdes en risikoanalyse, mens type C systemer ikke kræver hverken beredskabsplaner eller risikoanalyser. Alle identificerede informationsaktiver skal i forbindelse med registreringen gennemgå en klassificering. Systemklassifikationen bestemmes ud fra dataklassifikationen og betydningsvurderingen af det enkelte aktiv.
Konsekvensvurdering	Konsekvenser af hændelser i mod informationsaktiver skal løbende vurderes.
Overordnet risikovurdering	Der skal udføres en overordnet risikovurdering af trusselsbilledet for Universitetet. Den overordnede risikovurdering skal indeholde konsekvensvurdering og

	sårbarhedsvurdering. Risikovurderingen skal opdateres ved alle væsentlige ændringer i risikobilledet, dog mindst en gang om året.
Information om nye trusler, virus og sårbarheder	AU IT skal etablere en proces for identifikation af nye sårbarheder. Der skal udpeges en ansvarlig person eller gruppe for dette. AU IT skal holde sig orienteret om sikkerheden inden for de benyttede operativsystemer, samt de anvendte systemer og applikationer på både klient- og serversiden. AU IT skal gennem det centrale informationssikkerhedsudvalg informere relevante personer i ledelsen om nye trusler, som potentielt kan berøre de pågældende forretningsenheder med henblik på at tilpasse forretningsgange og tilvejebringe de fornødne ressourcer for at modvirke truslerne.
Håndtering af sikkerhedsrisici	Når risikovurderingerne afdækker sikkerhedsbehov, som ikke pt. honoreres af de tilgængelige sikringsmekanismer og procedurer skal informationssikkerhedschefen bringe emnet op i det centrale informationssikkerhedsudvalg. Såfremt der er tale om en væsentlig/kritisk risiko, kan informationssikkerhedsudvalget pålægge ejerne af det/de berørte aktiver, at identificere mulige løsningsmodeller, og om at opprioritere implementeringen. Ved ikke kritiske risici, skal løsningen indgå i den normale prioritering af opgaver og projekter på AU.

1.2 Informationssikkerhedspolitik

Dispensation for krav i sikkerhedspolitikken	Dispensation for efterlevelsen af sikkerhedspolitikkerne er kun muligt, hvis det er forretningsmæssigt velbegrundet, og de respektive system- og procesejere står inde for at det er forsvarligt.

	Dispensation gives af det centrale informationssikkerhedsudvalg. En dispensation er altid skriftlig, og med en tidsbegrænset varighed - typisk 1 år. Det er brugerens ansvar at sikre sig en evt. forlængelse af dispensationen. Informationssikkerhedschefen vedligeholder en oversigt over de givne dispensationer. Den relevante system- og/eller procesejer er ansvarlig for enhver sikkerhedshændelse, der sker som en direkte konsekvens af dispensationen.
Offentliggørelse af sikkerhedspolitik	Sikkerhedspolitikken skal offentliggøres og alle relevante interessenter, herunder alle medarbejdere og studerende, skal gøres opmærksomme på politikken.
Godkendelse af sikkerhedspolitik	informationssikkerhedspolitikken skal ved ændringer godkendes af Universitetsledelsen efter indstilling fra det centrale informationssikkerhedsudvalg.
Opfølgning på implementering af sikkerhedspolitikken	Hver enkelt leder skal løbende sikre, at sikkerhedspolitikken bliver overholdt inden for eget ansvarsområde.
Vedligeholdelse af sikkerhedspolitik	Universitetets informationssikkerhedspolitik, regler, procedurer og deraf afledt dokumentation skal vedligeholdes af informationssikkerhedschefen, i samarbejde med relevante parter, herunder AU IT, informationssikkerhedsudvalgene, de studerende og universitetsledelsen.

1.3 Sikkerhedsimplementering

Ledelsens rolle	Ledelsen skal støtte Universitetets informationssikkerhed ved at udlægge klare retningslinier, udvise synligt engagement samt sikre en præcis placering af ansvar.
Koordination af	Ansvaret for koordination af sikkerheden

informationssikkerheden	på tværs i organisationen varetages af informationssikkerhedschefen.

1.4 Outsourcing

Outsourcingpartnere	Sikkerhedsniveauet hos alle outsourcingpartnere skal være acceptabelt. Alle outsourcingpartnere skal af hensyn til AUs it-arkitektur og driftshensyn godkendes af Vicedirektøren for IT og informationssikkerhedschefen. Ved outsourcing af områder, der omhandler persondata, skal man være opmærksomme på kravene i persondataloven og retningslinjerne som udstikkes af datatilsynet.
Sikkerhed ved outsourcing	AUs sikkerhed må samlet set ikke ikke forringes af outsourcing. Ved outsourcing af IT-systemer skal der inden indgåelse af kontrakt indhentes information om sikkerhedsniveau fra outsourcingpartner, herunder dennes sikkerhedspolitik.
Overvågning af serviceleverandøren	Den aftale ansvarlige skal regelmæssigt overvåge serviceleverandøren. Det kan ske via rapportering og statusmøder, men ved større aftaler bør man forbeholde sig ret til at lave inspektion og revision af leverandøren. Ved outsourcing bør der stilles krav om en revisionserklæring, eller certificering efter DS484, ISO27001 e.lign.

1.5 Sikkerhed i tredjeparts adgang

Samarbejdsaftaler	Der må ikke gives adgang mellem Universitetets og eksterne parters informationsaktiver, før der er indgået en samarbejdsaftale, der som minimum skal indeholde en fortrolighedserklæring.
Aftaler om informationsudveksling	Ved udveksling af følsomme eller fortrolige informationer og data imellem AU og evt.

	tredje part skal der foreligge en skriftlig aftale herom. Lovgivningen stiller desuden krav om en databehandler aftale, såfremt der er tale om behandling for personfølsomme oplysninger.
Indhold af fortrolighedserklæringerne	Definition af de informationer, der er omfattet. En fastlagt løbetid. Beskrivelse af hvad der skal ske, når aftalen udløber. Underskriverens ansvar for at undgå brud på den aftalte fortrolighed. Information om omfattede ophavsrettigheder. Beskrivelse af hvordan informationerne må anvendes, for eksempel hvilke brugsrettigheder til informationerne underskriveren får. Universitetets ret til overvågning af og opfølgning på overholdelse af fortrolighedspligten. Procedure for advisering og rapportering af brud på fortroligheden. Betingelser for returnering eller destruktion af informationsaktiver ved aftalens ophør. Sanktioner ved brud på fortrolighedspligten.
Sikkerhed ved samarbejde med partnere	Ved integration af AUs systemer og processer med tredjepart skal systemejeren sikre, at sikkerhedsrisici vurderes og dokumenteres.
Information til eksterne partnere	Det skal sikres, at tredjepart gøres opmærksom på det forventede sikkerhedsniveau, herunder adgang til beskrevne politikker.
Fortrolighedserklæring for studerende	Det skal sikres, at studerende, der tildeles adgang til Universitetets følsomme og/eller fortrolige data, afgiver en

	fortrolighedserklæring.

2. Identifikation, klassifikation og ansvar for aktiver

Informationsaktiver skal beskyttes, uanset om det er fysiske aktiver som dokumenter, der er udskrevet, produktionsudstyr eller it-systemer. Det er derfor nødvendigt at identificere, klassificere og placere ejerskab for alle aktiver.

2.1 Håndtering af informationer og aktiver

Accepteret brug af informationsaktiver	Systemejere skal lave retningslinier for accepteret brug af AUs informationsaktiver.
Opbevaring af følsomme eller fortrolige informationer på privat udstyr	Personligt ejet IT-udstyr som pc, tablet, bærbare harddiske, memorysticks, CD- eller DVD-brændere må ikke anvendes til opbevaring af følsomme eller fortrolige data.
Brug af bærbare medier til følsomme og fortrolige data	Følsomme og fortrolige informationer skal krypteres, når de opbevares eller transporteres på bærbare medier, fx USB-nøgler, tablets, mobiltelefoner, CD'er eller DVD'er.

2.2 Klassifikation af informationer og data

Kontrol med klassificerede informationer	Det centrale informationssikkerhedsudvalg er ansvarlig for at definere et fast sæt af egnede og relevante sikkerhedskontroller til beskyttelse af de enkelte informationskategorier. Vicedirektøren for IT skal sikre, at de nødvendige forholdsregler, procedurer og kontroller implementeres i IT-afdelingen. Den lokale ledelse, skal sikre, at de nødvendige forholdsregler, procedurer og kontroller implementeres på hovedområderne.
Ansvar for dataklassifikation	Det er ejeren, som har ansvaret for at dataklassificere det enkelte aktiv og tilse, at det sikres på behørig vis i overensstemmelse med klassifikationen.

Klassifikation af data og andre informationer	AUs data og informationer, i det følgende "data", skal klassificeres efter følgende skala: Offentlige data: Defineret som data, som alle, der udtrykker et ønske om det, har eller kan få adgang til. Det kan fx være data på offentlige hjemmesider, uddannelsesbrochurer m.v. Disse data kræver som udgangspunkt ikke nogen særlig beskyttelse, dog skal man sikre, at kun godkendte personer kan redigere i disse data. Interne data: Defineret som data, der kun må anvendes og kommunikeres internt, og som i den daglige drift er nødvendige for de brugere, der skal anvende dem. Det kan fx dreje sig om mødereferater, blanketter, fakturaer mv. Interne data kræver en vis grad af beskyttelse. Som minimum skal man sikre, at kun godkendte personer har adgang til både at læse og ændre data. Fortrolige data: Defineret som de data, som kun særligt betroede brugere kan få adgang til for at kunne udøve deres arbejdsfunktioner, og hvor et brud på fortroligheden kan være skadelig for AU eller vores samarbejdspartnere. Det kan fx dreje sig om ansøgninger, kontrakter, regnskabsdata mv. Fortrolige data kræver en høj grad af beskyttelse. Adgangen skal begrænses til godkendte personer, og anvendelse af kryptering bør overvejes, specielt ved overførsel til eksterne medier eller tjenester. Fortrolige data data må aldrig opbevares eller behandles på privat udstyr. Følsomme data: Defineret som data, der er omfattet af Lov om behandling af personoplysninger. Følsomme data kræver ekstra høj grad af beskyttelse. Adgangen skal begrænses til så få godkendte personer som muligt, og kryptering skal overvejes. Følsomme data må aldrig opbevares eller behandles på privat udstyr, og hvis data flyttes til eksterne

	medier, skal der anvendes kryptering. Vær også opmærksom på, at der kan være behov for indgåelse af databehandler aftaler og anmeldelse til datatilsynet. Se mere på datatilsynets hjemmeside. Relaterede Procedurer Klassifikation af data
Ansvar for betydningsvurderingen	Det er ejeren, som har ansvaret for at betydningsvurdere det enkelte informationsaktiv og tilse, at det sikres på behørig vis i overensstemmelse med dets betydning for AU.
Informationsaktiver skal betydningsvurderes	Informationsaktiver skal betydningsvurderes i henhold til den på AU gældende standard. Et aktiv skal altid vurderes som den højeste af værdi af de relevante kategorier. Relaterede Procedurer Betydningsvurdering af informationsaktiver

2.3 Ejere af systemer og data

Juridisk ejerskab	Det juridiske ejerskab til data på AUs computere (servere, stationære PCer, Bærbare PCer etc.) tilfalder som udgangspunkt Universitetet. Det gælder dog ikke i følgende tilfælde: - Der er lavet en skriftlig aftale - Det følger af gældende lovgivning, fx regler om ophavsret m.v. - Der er tale om private data, fx private digitale billeder - Der er tale om forskningsdata, som 3.mand stiller til rådighed for AU. Indholdet af studerendes netværksdrev anses som udgangspunkt for at være privat ejendom, medmindre den studerende har et ansættelsesforhold ved AU. Netværksdrev må kun anvendes til studiemæssig brug, og AU forbeholder sig

	retten til at overvåge brugen, og analysere på indholdet med henblik på at hindre misbrug.
Retten til at disponere over udstyr	Uanset om data ejes af AU, en medarbejder, eller 3. mand, kan AU frit disponere over eget udstyr. Dette betyder at AU må slette indholdet af en computer, et netværksdrev, en memorystick o.s.v hvis en medarbejder har forladt universitetet, uden at konsultere medarbejderen først. Tilsvarende må AU nulstille mobiltelefoner og tablets. AU kan ikke gøres ansvarlig for evt. tab som følge af ovenstående.
Udpegelse af administrativ ejer	Alle informationsaktiver skal have udpeget en administrativ ejer. Ejerskab defineres hos AU som en jobfunktion, som kan pålægges den enkelte medarbejder. Ejerskab i AU er hierakisk nedarvet fra Rektor gennem enten Dekanerne og Institut-/centerlederne, eller Universitetsdirektøren og Vicedirektørerne til de enkelte medarbejdere. Ved fratræden eller andet fravær tilbagegår ejerskabet altid til den foregående person i kæden, indtil en ny ejer er udpeget.
Persondata-ansvarlig	Systemejeren til aktiver som indeholder data, der er omfattet af persondataloven, er persondata-ansvarlig.
Ansvar for adgangsrettigheder	Aktivets ejer har ansvaret for at fastlægge og løbende revurdere adgangsrettigheder. Tildeling af adgang skal ske i overensstemmelse med gældende regler om fx password o.lign.
Administration af Internet-domœnenavne	Der skal forefindes en liste over AUs registrerede domœnenavne, status for brug, betalingsoplysninger og dato for fornyelse. Ansvaret for registrering af de primære

	domænenavne ligger hos AU IT. Ansvaret for projektorienterede domænenavne kan ligge decentralt, men domænerne skal være centralt kendt.
Ansvarlige for data på mobile enheder	På mobile enheder med en primær ejer er pågældende ansvarlig for data. På mobile enheder uden en primær ejer er seneste bruger ansvarlig for at data fjernes fra enheden efter brug. Brugere af Universitetets mobile enheder er ansvarlige for at beskytte de data, der behandles på disse, samt enhederne selv.

2.4 Dataintegritet

Opbevaring og behandling af data	Data skal altid opbevares og behandles således, at dataintegriteten bevares. Der kan være lovkrav e.lign. som stiller særlige krav til dokumentation af informationer/datas integritet.

2.5 Identifikation og registering af aktiver

Identifikation af informationsaktiver	Alle Universitetets informationsaktiver skal identificeres og klassificeres. Se afsnit 2.2

3. Personalesikkerhed og brugeradfærd

Informationssikkerheden i virksomheden afhænger i høj grad af medarbejderne. Det er nødvendigt at sikre virksomheden gennem ansættelse af de rigtige medarbejdere, uddanne medarbejdere i jobfunktioner og sikkerhed - samt sætte regler for, hvordan man skal agere i forhold til sikkerhedshændelser og -risici.

3.1 Ansættelses og fratrædelse

Baggrundscheck af ansatte	HR afdelingen skal i samarbejde med Vicedirektøren for IT tilse, at der sker forsvarligt baggrundscheck af IT-medarbejdere. HR afdelingen skal, i samarbejde med den ansættende enhed, tilse, at der sker forsvarligt baggrundscheck af medarbejdere i særligt betroede stillinger, herunder lederstillinger.

Baggrundscheck af medarbejdere bør minimum omfatte:	En personlig reference. Ansøgerens curriculum vitae. Uddannelser og professionelle kvalifikationer.
Returnering af aktiver ved fratrædelse	Medarbejderen skal aflevere alle de af AU udleverede aktiver ved ansættelsens ophør. Såfremt der indgås særlige aftaler, fx Emeritusordninger, kan de udleverede aktiver forblive hos medarbejderen indtil aftalens ophør.
Inddragelse af privilegier ved fratrædelse	HR skal i samarbejde med Vicedirektøren for IT lave og vedligeholde en procedure for inddragelse af privilegier i forbindelse med fratræden eller afskedigelse af personale. Proceduren skal gennemgås/opdateres minimum en gang om året. Proceduren for inddragelse af privilegier skal indeholde en liste over funktioner og personer, der skal informeres i forbindelse med fratrædelsen. Privilegier omfatter adgange til systemer, bygninger m.v., samt evt. rettigheder til at disponere på vegne af AU.

3.2 Funktionsadskillelse

Sikring af IT-systemer	IT-systemer skal beskyttes ved hjælp af funktionsadskillelse, således at risikoen for misbrug af privilegier minimeres.

3.3 Ledelsens ansvar

Ledelsens ansvar	Det er nærmeste leders ansvar, at alle medarbejdere: Er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med sikkerhed, før de tildeles adgang til Universitetets systemer og data. Er gjort bekendt med nødvendige retningslinier, således at de kan leve op til

	AUs informationssikkerhedspolitik. Opnår et opmærksomhedsniveau i spørgsmål vedrørende informationssikkerhed, der er i overensstemmelse med deres roller og ansvar hos Universitetet.

3.4 Uddannelse

Sikkerhedsuddannelse for IT-medarbejdere	Alle IT-medarbejdere skal uddannes i sikkerhedsaspekterne i deres job. For eksempel for at mindske risiko for hændelser i forbindelse med deres eventuelle privilegerede adgang.
Kendskab til klassificering af informationer	Alle ansatte bør have kendskab til, hvorledes data og dokumenter klassificeres. Systemejere, dataejere og systemansvarlige skal holde sig opdateret omkring klassifikation.
Kendskab til sikkerhedspolitikken	Nærmeste leder er sammen med AU HR ansvarlig for, at nye medarbejdere gøres bekendt med AUs informationssikkerhedspolitik. Som minimum skal nye medarbejdere have udleveret folderen "Informationssikkerhed for ansatte på Aarhus Universitet". Alle relevante brugere modtager løbende instruktioner i overholdelse af AUs informationssikkerhedspolitik. Eksisterende studerende og medarbejdere hos Aarhus Universitet, har pligt til at holde sig informeret om de gældende regler på informationssikkerhed.au.dk Nye studerende ved Aarhus Universitet skal gøres bekendt med nødvendige retningslinjer inden de starter på Universitetet. Ansvaret herfor ligger hos studieadministrationen.

3.5 Logning og overvågning

Generelle regler for logning	AU IT har lov til at logge al information som vedrører sikkerhed, driftsstabilitet og fejlretning. Ovenstående omfatter adgang eller forsøg

	på adgang til systemer, hændelser, der kan påvirke fortroligheden, tilgængeligheden eller integriteten af AUs systemer eller infrastruktur, netværksforbindelser og aktivitet på AUs netværk, e-mail trafik og brug af forskellige programmer. Logningen giver potentielt mulighed for at spore en enkelt persons handlinger på AUs udstyr og/eller netværk.
Anvendelse af logfiler	Det er ikke tilladt at bruge log-filerne til at spore enkeltpersoners handlinger, medmindre der er tale om henvendelser vedr. ulovlige handlinger, alarmer fra antivirus/antispam eller lignende sikkerhedssystemer, eller ved mistanke om ikke tilladt adfærd. AU IT udarbejder således ikke oversigter over den enkelte brugers aktiviteter og foretager ingen vurdering af om enkeltpersoners aktiviteter er relevante for den pågældendes arbejde på AU. Såfremt der er behov for at spore en enkelt bruges adfærd, skal der først indhentes tilladelse hos personen selv (fx ved opfølgning på alarmer), eller ved dennes nærmeste chef (fx ved mistanke om ikke tilladt adfærd, jf. politikker, lovgivning m.v.). AU IT må gerne bruge logfiler til følgende formål: - Statistik over fx mail-, internet- og netværkstrafik til og fra AU. - Statistik om anvendelse af fx visse programmer eller visse typer af netværkstrafik. - Statistik relateret til mindre udsnit af AU, fx et institut/center eller et vicedirektørområde, sålænge man ikke kan udlede enkeltpersoner ud fra materialet. - Fejlfinding og alarmering. - Opfølgning på sikkerhedshændelser.

3.6 Adfærdsregler

Omgåelse af sikkerhedsforanstaltninger	Det er ikke tilladt at forsøge at omgå sikkerhedsmekanismer.

	Det er ikke tilladt at foretage uautoriseret afprøvning af sikkerheden.
Tavshedspligt	AUs medarbejdere er omfattet af tavshedspligt. IT-medarbejdere med privilegerede adgange til informationer skal udvise særlig omhu for at sikre, at oplysninger som de i forbindelse med deres arbejde måtte få kendskab til, ikke gives videre.
Ytringsfrihed	AUs medarbejdere har, som alle borgere i Danmark ytringsfrihed, som kun begrænses af straffelovens paragraffer om injurier, racisme el. lign. AU følger Justitsministeriets Vejledning om offentligt ansattes ytringsfrihed (September 2006). Relaterede Procedurer Vejledning om offentligt ansattes ytringsfrihed

3.6.1 Adfærdsregler for brug af adgangskode

Brug af kodeordsbeskyttet pauseskærm	Som bruger bør du aktivere kodeordsbeskyttet skærmlås, når du forlader din arbejdsstation, således at den er uden for din synsvidde. Alle pc'er, servere og mobile enheder skal automatisk aktivere skærmlås efter 10 minutters inaktivitet.
Genbrug af kodeord	Medarbejdere og studerende må ikke genbruge kodeord til AUs infrastruktur til adgang til tredjeparts systemer som fx websteder og netbanker. Brug af samme kodeord på tredjeparts systemer øger sandsynlighed for, at kodeordets fortrolighed krænkes.
Overdragelse af kodeord	Midlertidige/engangskodeord kan overdrages verbalt efter sikring af modtageres identitet. Det er tilladt at sende midlertidige/engangskodeord via SMS, efter sikring af modtageres identitet. Det er tilladt at sende engangskodeord pr.

	mail, efter sikring af modtagers identitet. Når man sender et password pr. SMS eller email, må det ikke fremgå, hvor passwordet kan bruges.
Kodeord er strengt personlige	Kodeord er strengt personlige og må ikke deles med andre, heller ikke it-medarbejdere.

3.6.2 Adfærdsregler for brug af internet

Blokering af netadgang	AU IT forbeholder sig ret til at spærre brugerkonti og foretage omgående frakobling af en given brugers computer, såfremt det skønnes nødvendigt for at opretholde netværkssikkerheden eller på anden måde at sikre driften.
Download af filer og programmer fra Internettet	Filer må downloades fra Internet til arbejdsmæssig brug, og i rimeligt omfang til privat brug, jf. reglerne om privat anvendelse af Internetforbindelsen. Det er tilladt at hente programmer fra Internet til arbejdsmæssig brug, forudsat sikkerhedspolitikken og alle licensbetingelser i øvrigt overholdes, og at der ikke er et lokalt forbud mod installation af tredjepartsprogrammer på den pågældende maskine. Det er tilladt at hente programmer fra Internettet i rimeligt omfang til privat brug, forudsat sikkerhedspolitikken i øvrigt overholdes, og alle licensbetingelser overholdes. Vær opmærksom på, at man som ved alle andre køb, skal overholde gældende indkøbsregler.
Kriminelle aktiviteter - Internetadgang	Brug af Internetforbindelsen til kriminelle aktiviteter af enhver art, herunder (men ikke begrænset til) hackning, download eller distribution af børnepornografi, download eller distribution af pirat-software, -musik, -film eller anden omgåelse af lov om ophavsret, er forbudt. Forsøg på at omgå AUs

	sikkerhedsmekanismer er forbudt. Tilsvarende er ethvert forsøg på at omgå andres sikkerhedsmekanismer fra AUs Internetforbindelse forbudt.
Andre begrænsninger - Internetadgang	Begrænsninger i adgangen til visse applikationer kan også gælde arbejdsrelaterede opgaver (fx overførsel af store mængder forskningsdata), hvor AU IT fx kan vurdere, at disse aktiviteter om muligt skal foretages uden for almindelig arbejdstid. Dette meldes i givet fald ud via e-mail og/eller intranettet.
Kommerciel brug - Internetadgang	AUs Internetforbindelse må ikke benyttes til private kommercielle aktiviteter. Studerende og medarbejdere, der har eget firma udenfor AU må gerne tilgå services i dette firma fra Universitetets netværk, såfremt det ikke udgør en sikkerhedsrisiko for AU, og såfremt eksisterende tekniske foranstaltninger tillader dette. Der kan ikke gives tilladelse til at åbne fx firewall porte e.lign. for at give adgang til private formål. Studerende og medarbejdere må under ingen omstændigheder drive private firmaer fra udstyr der befinder sig på AUs netværk, således at firmaet derved kan associeres med AU.
Agtpågivenhed - Internetadgang	AU IT gør deres bedste for at sikre nettrafikken ved hjælp af antivirusprogrammer, Firewall-regler samt sikkerhedsopdateringer på PC'erne, men disse sikringsmekanismer kan i visse tilfælde være utilstrækkelige, og alle brugere skal derfor orientere sig om, og udvise agtpågivenhed overfor trusler mod IT-sikkerheden fra Internettet.
Begrænset netadgang fra visse maskiner	Vær opmærksom på, at der for visse maskiner (fx, men ikke begrænset til servere, styringscomputere til laboratorie- og klinisk udstyr mv.) bør være begrænsninger i netværksadgangen. Fx bør denne type udstyr ikke bruges til at

	surfe på internettet o.lign.
Ansvarsfraskrivelse - Internetadgang	Vælger man at benytte sin arbejds-PC til at udføre privatøkonomiske transaktioner (Netbank, PC-bank og lignende) over AUs Internetforbindelse skal man være opmærksom på, at AU er uden ansvar for fejl og tab af enhver art.
Adgang og identitet - Internetadgang	Computere tilsluttet AUs lokalnetværk har adgang til Internettet - og vil der sædvanligvis optræde med identiteter, som henviser til au.dk eller et andet af AUs domæner. Det påhviler derfor den enkelte bruger at sikre, at hans eller hendes færden på Internettet hverken kompromitterer sikkerheden eller AUs anseelse.
Anvendelse - Internetadgang	Adgang til WWW og andre net-tjenester er primært forbeholdt aktiviteter i direkte forbindelse med arbejde/studier, men det er tilladt at bruge AUs netforbindelse til private formål. Private aktiviteter må under ingen omstændigheder have et omfang, der kan genere andre medarbejderes eller studerendes legitime arbejds- eller studierelaterede aktiviteter.

3.6.3 Adfærdsregler for brug af e-mail

Adgang og identitet	Alle ansatte og studerende ved AU har en e-mail adresse og har adgang til at sende og modtage elektronisk post. E-mail adressen omfatter AUs navn ved at indeholde “au.dk” eller et andet af AUs domæner. Det påhviler den enkelte bruger at sikre, at hans eller hendes brug af e-mail er i overensstemmelse hermed, dvs. ikke kan skade AUs anseelse.
Anvendelse	Brugen af e-mail er primært forbeholdt aktiviteter i direkte forbindelse med arbejde/studier, men det tillades at bruge e-mail til private formål.

	Private mails bør tydeligt sorteres/mærkes, således at de kan skelnes fra arbejdsmæssige/studierelaterede mails. Der bør laves en folder der hedder Privat/Private til opbevaring af privat e-mail korrespondace. Hvis man ønsker større sikkerhed for afsendte emails, kan man markere udgående mails med ordet "privat"/"private" i emnefeltet. Private aktiviteter må under ingen omstændigheder have et omfang, der kan genere andre medarbejderes eller studerendes legitime arbejds- eller studierelaterede aktiviteter, og private e-mails må ikke fylde AUs posthuse op.
Brevhemmelighed	E-mail er omfattet af brevhemmeligheden, jf. straffelovens §263, stk. 1-3. Hvis en medarbejder forlader AU, forbeholder AU sig ret til at tilgå den pågældende persons postkasse. Ved en sådan adgang må man alene læse og kopiere arbejdsrelaterede e-mails og aftaler. Privat post og private aftaler må ikke åbnes. Hvis ikke emails og aftaler er mærket som private, kan andre ved vanvare komme til at åbne en privat e-mail eller aftale. Såfremt det sker, skal man straks lukke e-mailen/aftalen - det er ikke tilladt at læse indholdet.
Adgang til andres postkasser	Indholdet i medarbejdernes postkasse anses på lige fod med øvrige data som AUs ejendom. Det gælder dog ikke evt. privat korrespondance, som derfor bør sorteres/mærkes som beskrevet under afsnittet anvendelse. Indholdet af studerendes postkasser anses som udgangspunkt for at være privat, og AU har derfor ikke ret til at åbne en studerendes postkasse, medmindre der foreligger en aftale herom, eller det er nødvendigt af tekniske hensyn, som beskrevet nedenfor. Såfremt det sker af tekniske hensyn, må indholdet i

	postkassen ikke læses af medarbejderne. AU IT kan skaffe sig adgang til alle e-postkasser på AUs posthuse. Dette kan være nødvendiggjort af tekniske nedbrud (fx mail-loops, der fylder en fraværende medarbejders/studerendes postkasse op), eller et tvingende behov for at skaffe sig adgang til en besked, der vides sendt til en fraværende medarbejder. Hvor AU IT er nødt til at skaffe sig en sådan adgang, skal det altid ske efter aftale med den pågældende medarbejder/studerende selv, eller hvis dette ikke er muligt, med medarbejderens chef/Vicedirektøren for studieområdet. Ved adgang til medarbejderes postkasser, bør man inddrage den relevante tillidsmand. Den pågældende medarbejder/studerende skal hurtigst muligt orienteres om episoden. De enkelte afdelinger kan aftale, at medarbejderne giver hinanden eller fx en sekretær læseadgang til postkasserne, eller dele der af. Sådanne aftaler træffes i åbenhed af afdelingerne selv. I tilfælde af at en medarbejder rejser, eller bliver afskediget, har AU ret til at tilgå den pågældende bruges postkasse, med henblik på at få adgang til forretningsrelevant korrespondance. Det anbefales at man laver en aftale om adgangen inden personen forlader AU, og at man giver personen en mulighed for at rydde op i sin private korrespondance inden adgangen gives.
Forward af email	AUs medarbejdere bruger i vid udstrækning mail- og kalendersystemet som et værktøj i forbindelse med sagsbehandling. Det betyder, at der i de mails, der cirkulerer på AU, potentielt befinder sig følsomme og fortrolige personoplysninger, og vi er derfor forpligtede til at overholde Persondatalovgivningen, herunder sikkerhedsbekendtgørelsen. Medarbejdere må derfor ikke automatisk videresende

	mails fra AU til mail uden for AU som fx G-mail og Hotmail. Ovenstående gælder alene for medarbejdere på AU. AU sender ikke personlig post via mail til de studerende, og studerende må derfor gerne videresende deres post.
Behandling af fratrådte medarbejderes e-mail konti	AU følger datatilsynets retningslinjer for behandling af en fratrådt medarbejders e-mail konto. Hvis der er specielle behov, som ikke kan imødekommes af datatilsynets retningslinjer, kan AU indgå en aftale med den fratrædende medarbejder omkring behandlingen. En sådan aftale skal være skriftlig, og underskrevet af begge parter. Relaterede Procedurer E-mail - behandling af en fratrådt medarbejders e-mail konto
Blokering af e-mail konti	AU IT har ret til at spærre konti og foretage omgående frakobling af en given brugers computer, såfremt det skønnes nødvendigt for at opretholde sikkerheden eller på anden måde at sikre driften.
Agtpågivenhed	AU IT sikret e-mail trafikken bedst muligt ved hjælp af filtre mod virus, malware og spam samt via løbende sikkerhedsopdateringer på PC'erne, men disse sikringsmekanismer kan være utilstrækkelige, og alle brugere skal derfor orientere sig om og udvise agtpågivenhed over for e-mail bårne trusler mod informationssikkerheden.
Kriminelle aktiviteter	Brug af e-mail til kriminelle aktiviteter af enhver art, herunder (men ikke begrænset til) distribution af pirat-software, -musik, -film eller anden omgåelse af lov om ophavsret, er forbudt. E-mail må ikke ligeledes ikke benyttes til ulovlige aktiviteter som udsendelse af SPAM mv.

Kommerciel brug	E-mail kontiene må ikke benyttes til private kommercielle aktiviteter. Godkendte kommercielle aktiviteter (fx datterselskaber under AU) skal have eget postdomæne, og der skal udarbejdes klare retningslinier, som sikrer, at de enkelte medarbejdere skal afsende e-mail fra den rigtige konto, således at sammenblanding af roller undgås.

3.6.4 Adfærdsregler for brug af trådløse netværk

Forbindelse til fremmede trådløse netværk	Som bruger bør man udvise forsigtighed, når man forbinder sig til fremmede trådløse netværk. Man kan ikke stole på at det er sikkert. Det anbefales, at man anvender en VPN-forbindelse ovenpå det trådløse netværk. På smartphones, tablets o.lign. skal man være ekstra påpasselig, da der ikke er en intern Firewall. Man bør så vidt muligt anvende en VPN forbindelse ovenpå det trådløse netværk.
Installation af trådløst udstyr	Medarbejdere, studerende og gæster må kun benytte de officielle trådløse netværk. Man må ikke installere eller ibrugtage udstyr, der giver anden trådløs netadgang til AUs produktionsnetværk.

3.6.5 Adfærdsregler for databeskyttelse

Sikkerhedskopiering (backup)	Som medarbejder skal man sikre arbejdsrelaterede data ved regelmæssig sikkerhedskopiering (backup), fx ved at anbringe data på et af universitets netværksdrev. Derved sikrer man at data kan rekonstrueres, hvis de er blevet slettet eller overskrevet, en disk er fejlet, eller en computer stjålet.
Anvendelse af servere og netværksdrev	AUs servere og netværksdrev er omfattet af backup, og som udgangspunkt bør alle data lagres på AUs servere.

Forholdsregler når data ikke kan lagres sikkert on-line	Hvis data ikke umiddelbart kan lagres på sikrede servere (fx data som indsamles i felten, eller mens beregninger pågår), er man som medarbejder hos AU forpligtet til at sikre, at lagring finder sted ved først givne lejlighed. Indtil lagring kan finde sted bør man sikre sig, at der er flere uafhængige kopier af data.

3.6.6 Adfærdsregler for brug af sociale netværkstjenester

Universitetets informationer på sociale netværk	Sociale netværk som fx Facebook, Twitter, Google+ m.v. er ikke lukkede og ikke sikre. Kun informationer, som kan stilles til rådighed på AUs offentlige hjemmesider (dvs i laveste klassifikations kategori), må distribueres via sociale netværk.
Misbrug af oplysninger på sociale netværkstjenester.	IT-kriminelle udnytter i vid udstrækning sociale netværk til at skaffe sig oplysninger om en given virksomhed. Vær derfor opmærksom på, hvilke oplysninger du offentliggør om AU på de sociale netværk, specielt om de kan bruges i forbindelse med kriminelle handlinger.

3.6.7 Adfærdsregler for overholdelse af licensregler

Kommerciel brug - licenseret software	Mange af de programmer, AU anvender, er anskaffet under særligt gunstige vilkår, fordi AU er en forsknings- og uddannelsesinstitution. Disse programmer vil være underlagt restriktioner i forhold til kommerciel anvendelse. Er du i tvivl om en given anvendelse er tilladt, bør du rådføre dig med AU ITs licens-faggruppe.
Eksterne parter - licenseret software	Mange af AUs IT-systemer er licenseret alene til AUs eget brug. Det er derfor sædvanligvis nødvendigt at tilkøbe yderligere licenser, hvis et system skal anvendes af eksterne parter – i særdeleshed fx hvis et system stilles til rådighed bredt via Internettet. I tvivlstilfælde kan man rådføre sig med AU ITs licens-faggruppe.

Hjemlån og privat brug - licenseret software	Nogle af de programmer, som AU har licens til, tillader samtidig installation på flere maskiner, fx en arbejds-PC i AUs lokaler, en bærbar PC og/eller en PC i medarbejderens hjem. Som hovedregel er licensen imidlertid bundet til arbejdsrelaterede aktiviteter, dvs. den dækker ikke privat brug, og slet ikke brugerens familiemedlemmer. Er man i tvivl om, en privat aktivitet er acceptabel, skal man rådføre sig med AU ITs licens-faggruppe først. Den enkelte bruger har også pligt til at overholde licensreglerne på dette område og har i særdeleshed pligt til at slette al AU-leveret software på private PC'er i hjemmet i forbindelse med fratræden.
Distribution og installation - licenseret software	AU IT er behjælpelige med distribution og installation af licenseret software via automatiske udrulningsystemer. Den enkelte bruger har derfor ret til at antage, at såfremt AU IT installerer programmet automatisk, så findes der en licens for vedkommendes brug. Andre programmer, som kun én eller ganske få skal anvende, bliver distribueret på anden vis, fx ved lån af installationsmedier fra AU IT, eller projekternes egne indkøb af licens og medier. Brugen heraf er ofte personlig og/eller bundet til en given maskine. Man må således normalt ikke "låne" licenser til/af andre brugere. Medarbejdere hos AU må ikke downloade eller uploade software, som søger at omgå licenskontrol. Installation af demo-versioner af software, fx i forbindelse med identifikation af nye værktøjer, er tilladt. Det er forbudt at søge at omgå demo-versionernes restriktioner i funktionalitet og/eller løbetid.
Installation af programmer på arbejdsstationer	Brugerne skal i videst muligt omfang benytte de programmer, som tilbydes gennem de automatiske

	installationsmekanismer. Selvinstallerede programmer på Universitetets arbejdsstationer skal overholde alle licensbetingelser. Brud på licensbetingelser mv. kan resultere i disciplinære sanktioner.

3.6.8 Adfærdsregler for mobile enheder

Synkronisering af mail og kalender til mobile enheder	Det er tilladt at synkronisere sin mail og kalender til mobile enheder som tablets og telefoner som stilles til rådighed af AU. Det er tilladt at synkronisere sin mail og kalender til private mobile enheder som tablets og telefoner. Hvis man ønsker at synkronisere sin mail og kalender til mobile enheder som tablets og telefoner skal man acceptere at følgende politik bliver lagt på enheden (både AU ejede og private): - Der skal anvendes en pin-kode på minimum 4 tegn. - Enheden sletter sig selv, hvis man taster pin-koden forkert mere end 25 gange. - Pin-koden aktiveres automatisk efter 10 minutters inaktivitet.
Ansvarlige for data på mobile enheder	På mobile enheder med en primær ejer er pågældende ansvarlig for data. På mobile enheder uden en primær ejer er seneste bruger ansvarlig for at data fjernes fra enheden efter brug. Brugere af Universitetets mobile enheder er ansvarlige for at beskytte de data, der behandles på disse, samt enhederne selv.

3.6.9 Adfærdsregler for brug af cloud tjenester

Anvendelse af cloud tjenester	Offentlige cloud tjenester som fx Dropbox, Gmail, GoogleDocs, Office365, Skydrive o.s.v. kan være nyttige samarbejdsværktøjer for medarbejdere og studerende på AU. Desværre er

	sikkerheden ikke altid i orden for disse tjenester, og det er derfor vigtigt at man bruger tjenesterne med omtanke. Generelt skal tjenesterne betragtes som et supplement til de tjenester som AU stiller til rådighed. Derfor bør man som medarbejder have en opdateret kopi af data på sit netværksdrev på AU. Som studerende bør man altid have en kopi af data lokalt. Følsomme data må ikke overføres til cloud tjenester, medmindre AU har indgået en databehandleraftale med den pågældende udbyder. Fortrolige data må kun overføres til cloud tjenester, efter aftale med dataejeren. Fortrolige data bør krypteres inden de overføres til en cloud tjeneste.

4. Fysisk sikkerhed

Fysisk sikkerhed og adgangsregler for gæster er naturlige elementer i Universitetets sikkerhedspolitik. Fysisk sikkerhed omfatter blandt andet døre, vinduer, alarmer - samt tyverisikring af Universitetets fysiske aktiver, eksempelvis it-udstyr. Systemer til adgangskontrol er ligeledes et element af fysisk sikkerhed, der sikrer, at kun personer med legalt ærinde får adgang til Universitetets område.

4.1 Tekniske sikringsforanstaltninger

Brandsikring	Serverrum skal sikres med veldimensioneret brandmelde- og brandslukningsudstyr. Serverrum må ikke benyttes som lager for brændbare materialer. Farlige eller brandfarlige materialer skal lagres i behørig afstand fra sikre områder.
Køling	Lokaler med væsentlige mængder af IT-udstyr skal sikres med køling.
Nødstrømsanlæg	Alle server-systemer skal beskyttes med nødstrømsanlæg med kapacitet til mindst 15 minutters uafbrudt drift, således at nedlukning kan ske forsvarligt. Dette omfatter også hjælpesystemer som fx

	tilhørende køleanlæg. Forretningskritiske systemer og tilhørende køleanlæg bør desuden være tilsluttet nødstrømsanlæg som kan opretholde driften ved længere nedbrud, fx dieselgeneratorer.

4.2 Beskyttelsesanlæg

Miljømæssig sikring af serverrum	Serverrum, hovedkrydsfelter og tilsvarende områder skal på forsvarlig vis sikres mod miljømæssige hændelser som brand, vand, eksplosion og tilsvarende påvirkninger.

4.3 Sikre områder

Overvågning i sikre områder	AU IT skal sikre, at 3. parts arbejde i serverrum og andre sikre it-områder så vidt muligt overvåges. Den område ansvarlige leder skal sikre at 3. parts arbejde i andre sikre område, fx laboratorier overvåges, såfremt der behandles følsomme eller fortrolige data.
Oplysninger om sikre områder	Oplysninger om sikre områder og deres funktion skal alene gives ud fra et arbejdsbetinget behov.
Adgang for serviceleverandører	Serviceleverandører må kun få adgang til sikre områder, når dette er påkrævet.
Aflåsning af hovedkrydsfelter og lignende teknikrum	Alle krydsfelter og andre teknikrum skal være aflåste. Der skal være adgangskontrol til hovedkrydsfelter og lignende rum, således at det er muligt at kontrollere, hvem der har været i rummet på et givet tidspunkt.
Adgang til serverrum og hovedkrydsfelter	Adgang til serverrum og hovedkrydsfelter tillades kun med tilladelse fra AU ITs ledelse, eller ved overvåget adgang af betroede medarbejdere fra AU IT. Det er Vicedirektøren for ITs ansvar, at kun

	betroede personer har adgang til serverrum og krydsfelter.

4.4 Udstyrssikkerhed

Afskaffelse eller genbrug af udstyr	Når udstyr genbruges, skal databærende medier overskrives, så data ikke kan genskabes. Defekte eller udtjente harddiske, eller andre databærende medier fra servere, kopimaskiner, computerer, mobile enheder o.s.v., skal enten overskrives eller destrueres så data ikke kan genskabes.
Vedligeholdelse af udstyr og anlæg	AU IT skal vedligeholde udstyr efter leverandørens anvisninger. Alle informationer, som ikke er klassificeret som offentlige, skal slettes fra udstyr, der repareres eller vedligeholdes uden for AU.
Sikring af kabler	Faste kabler og udstyr skal mærkes klart og entydigt. Dokumentation skal opdateres, når den faste kabelføring ændres.
Placering af udstyr	Udstyr skal placeres eller beskyttes, så risikoen for skader og uautoriseret adgang minimeres. Udstyr, der benyttes til at behandle følsomme/fortrolige informationer, skal placeres, så informationerne ikke kan ses af uvedkommende.
Tyverimærkning af IT-udstyr	Alt udstyr med en anskaffelsespris på over 3.000 kr. skal være tydeligt mærket for at minimere risikoen for tyveri. AU IT skal i samarbejde med de primære leverandører, arbejde på at få udstyr mærket ved levering. Det gælder også for mobiltelefoner, selv om de ikke er over beløbsgrænsen beskrevet ovenfor.
Sikring af mobile enheder og bærbare computere	Adgang til data på bærbare computere skal beskyttes med et login password.

	Udstyr med følsomme eller fortrolige informationer skal anvende harddisk kryptering. Smartphones og lignende mobile enheder skal låses med PIN kode e.lign, som er forskellig fra SIM kort koden.
Brug af mobile enheder	Mobile enheder og bærbare pc'er skal medbringes som håndbagage under rejser.
Opbevaring af bærbare computere	Bærbare computere skal fjernes, låses inde eller på anden måde sikres mod tyveri efter arbejdstidens ophør.

4.5 Gæster

Gæsters adgang	Værten har ansvaret for gæsters færden på AU.

5. It- og netværksdrift

Vedligeholdelse og opdatering af it-systemer er nødvendig for at opretholde et passende sikkerhedsniveau for Universitetet. 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 Universitetet. Den trussel, som uautoriseret adgang indebærer, gør det nødvendigt med klare regler for brugen af Universitetets netværk samt overvågning af infrastrukturen.

5.1 Daglig administration

Beskyttelse af systemdokumentation	Adgangsrettigheder til systemdokumentation skal holdes på et minimum. AU IT skal opbevare systemdokumentation passende sikkert.
Sikring af servere	Servere skal konfigureres så kun de nødvendige services er tilgængelige. Ovenstående bør ske ved at deaktivere de funktioner, der ikke er nødvendige, samt evt. benytte en indbygget firewall, til at begrænse adgangen.
Sikring af arbejdsstationer	Alle arbejdsstationer skal sikres inden brug.

inden ibrugtagning	Minimum sikring inkluderer installation af seneste sikkerhedsrettelser for operativsystem og programmer samt et opdateret antivirus-program.
Systemer til styring af adgangskoder	Adgangskontrolsystemet skal låse en brugerkonto i 15 minutter, hvis brugeren har overskredet det tilladte antal af adgangsforsøg.
Overvågning af procedurer for sikkerhedskopiering	Muligheden for at retablere data fra backup systemer skal regelmæssigt aftestes i et testmiljø. Endvidere skal retablering testes efter system- eller procesændringer, der kan påvirke backup rutiner.

5.2 Håndtering af datamedier

Beskyttelse af følsomme og fortrolige data på datamedier	Alle datamedier, fx USB-nøgler, der indeholder følsomme eller fortrolige data, skal være krypterede.
Virusscanning af datamedier	AUs antivirus-løsning scanner automatisk ethvert nyt medie. Brugeren behøver ikke at foretage sig noget, medmindre IT-systemet giver en specifik advarsel eller opfordring.
Afskaffelse og genbrug af medier	Alle datamedier, for eksempel harddiske, cd, dvd, bånd og hukommelsesenheder, skal sikkerhedsslettes eller destrueres inden bortskaffelse.

5.3 Operationelle procedurer og ansvarsområder

Adskillelse af udvikling, test og drift	Udviklings- og testmiljøer skal være systemteknisk eller fysisk adskilt fra driftsmiljøet.
Sikkerhedskopiering af data på serversystemer	AU IT er ansvarlige for sikker lagring og backup af data på serverudstyr. Planlægning skal ske i samarbejde med systemejerne.

Driftsafviklingsprocedurer	Driftsafviklingsprocedurer for type A systemer skal være dokumenterede, ajourførte og tilgængelige for driftsafviklingspersonalet og andre med et arbejdsbetinget behov.
Antivirusprodukter på servere	Der skal være installeret antivirus beskyttelse på alle systemer, hvor dette er muligt.
Softwareopdateringer generelt	AU IT skal holde sig informeret om programrettelser til de programmer, der anvendes i driften af Universitetets IT. AU IT skal installere disse på alle computere, fx servere og arbejdsstationer, når det vurderes, at rettelserne er nødvendige for at opretholde en tilfredsstillende sikkerhed, eller hvis opdateringerne vurderes at have en positiv effekt på stabiliteten af driftsmiljøet.
Dokumentation	AU IT skal sikre, at alle væsentlige systemer og IT-relaterede forretningsgange er dokumenterede, fx ved at samarbejde med systemejere og procesejere omkring dokumentationen.

5.4 Systemplanlægning

Kapacitetsplanlægning	IT-systemernes dimensionering skal afpasses efter kapacitetskrav, og jævnligt tilpasses behovet.
Sikkerhed i systemplanlægning	Ved planlægning af systemer skal sikkerhedsbetragtninger altid medtages i overvejelserne. IT-sikkerhedskrav skal tages i betragtning ved design, aftestning, implementering og opgradering af nye IT-systemer og ved systemændringer.

5.5 Overvågning af systemer

Kapacitetsovervågning	Alle serversystemer med kritiske informationer skal løbende overvåges for

	tilstrækkelig kapacitet til at sikre pålidelig drift og tilgængelighed. Alle serversystemer skal løbende overvåges for tilstrækkelig kapacitet til at sikre pålidelig drift og tilgængelighed. Overvågningen skal afspejle systemets klassifikation.
Overvågning af tilgængelighed	AU IT skal løbende overvåge alle IT-systemer. Overvågningen bør give mulighed for at kunne dokumentere tilgængeligheden af vigtige systemer. Et systems vigtighed afgøres ud fra systemets klassifikation.
Registrering af driftsstatus	AU IT skal registrere væsentlige forstyrrelser og uregelmæssigheder i driften af systemerne.

5.6 Styring af ændringer - Change Management

Definition på change	En change er enhver ændring i en service eller et system, der kan medføre et kald til helpdesk, eller en ændring som kan medføre tab af fortrolighed, tilgængelighed eller integritet.
Change Management - it-systemer	AU IT skal have en proces for håndtering af ændringer i infrastrukturen. Processen bør støtte sig op ad anerkendte metoder som fx ITIL, COBIT, ISO 20000 e.lign.
Change Management - andre områder	Ansvarlige for andre aktiver (systemer, anlæg og processer) bør have en procedure for håndtering af ændringer, som sikrer at alle relevante parter bliver informeret om ændringerne.

5.7 Beskyttelse mod skadelige programmer

Antivirusprodukter på arbejdsstationer	Der skal installeres et antivirusprogram på alle arbejdsstationer. Programmet skal sikre mod vira, orme og trojanske heste mv. Opdatering af signaturfiler mv. skal

	være muligt, selv om arbejdsstationen ikke har forbindelse til AUs netværk.
Opdateringer	AU IT stiller antivirus software, sikkerhedsopdateringer og andre beskyttelsesmekanismer til rådighed, og man er som medarbejder og studerende ved AU forpligtet til at sikre, at ens egen PC er opdateret. Sædvanligvis er ens stationære PC omfattet af automatisk opdatering, men man skal regelmæssigt checke, at fx antivirusprogrammet er aktivt og opdateret, og i forbindelse med brugen af bærbare PCer hviler der et særligt ansvar for at sikre, at alle opdateringerne er foretaget. AU IT udarbejder vejledninger herom og står altid til rådighed for at hjælpe med databeskyttelse.

5.8 Indholdsfiltrering

Automatisk indholdsfiltrering	Al indkommende email skal scannes for spammail og phishing. Mail der markeres som spam eller phishing skal enten sættes i karantæne, eller flyttes til brugernes spam folder.

5.9 Styring af netværk

Opdeling af netværk	AU IT skal segmentere netværk for at etablere en passende adskillelse imellem forskellige tjenester, brugergrupper eller systemer.
Sikring af netværk	AU IT har det overordnede ansvar for at beskytte AUs netværk, efter AUs fælles retningslinier.
Beskyttelse af diagnose- og konfigurationsporte	Fysisk og logisk adgang til diagnose- og konfigurationsporte bør kontrolleres.
Fjernstyring og administration	Værktøjer til fjernadministration tillades, hvis adgangen er krypteret ved hjælp af teknologier som fx SSH, VPN eller SSL/TLS, og hvis der er indhentet tilladelse fra AU IT. Det er ejeren af det pågældende udstyr,

	der er ansvarlig for evt. brud på sikkerheden i forbindelse med fjernadministration.
Tilslutning af udstyr til netværk	Det er ikke tilladt at koble udstyr som fx servere, netværksharddiske, printere e.lign. til AUs produktionsnetværk, uden forudgående aftale med AU IT. Selv om der er indhentet tilladelse, kan AU IT kræve udstyret frakoblet, hvis det forstyrrer den normale drift. Uautoriseret udstyr på AUs produktionsnetværk konfiskeres.
Installation af netværksudstyr	Det er ikke tilladt at installere netværksudstyr uden forudgående sikkerhedsgodkendelse. Dog er det tilladt, i samarbejde med AU IT, midlertidigt at tilslutte en switch til deling af et netværksstik i forbindelse med demonstrationer, møder eller lignende, såfremt disse alene giver adgang til Internettet. Standardværdier, eksempelvis administrator-login, skal ændres, før et system installeres på netværket. Det er tilladt at bruge netværksudstyr til undervisningsbrug, såfremt det er aftalt med AU IT.
Adgang til aktive netværksstik	Netværksstik i offentligt tilgængelige områder, hvor der ikke kræves validering, må kun give Internetadgang. For at få adgang til AUs interne netværk, skal der benyttes en VPN forbindelse.
Routing og netservices	Medarbejdernes computere må aldrig agere router mellem forskellige netværk eller udbyde netværksservices uden forudgående tilladelse fra AU IT.

5.10 Trådløse netværk

Gæsters brug af Universitetets trådløse	Gæstenetværket kan og må kun anvendes til Internetadgang, ikke til direkte adgang til interne systemer, med

netværk	undtagelse af services specielt beregnet til gæster.
Brug af trådløse lokalnetværk	AU stiller trådløst netværk til rådighed for både ansatte og studerende. Ukrypterede og/eller uvaliderede trådløse netværk giver kun adgang til internet og evt. print. For at få adgang til AUs interne netværk fra et sådant skal der anvendes en VPN forbindelse.

5.11 Forbindelser med andre netværk

Overordnet politik for fjernadgang	AU stiller en VPN-forbindelse til rådighed for alle ansatte på universitetet. Dermed har medarbejderne mulighed for at arbejde hjemmefra, eller mens de er på farten. Såfremt man anvender udstyr, der er udleveret og styret af AU IT, har man fuld adgang til AUs netværk. Hvis man anvender andet udstyr, fx en privat pc eller en pc indkøbt uden om AU IT, må man forvente at adgangen på nogle områder vil være begrænset. Det er ikke tilladt selv at opsætte udstyr eller programmer, der gør det muligt at etablere fjernadgang til AUs netværk, eller maskiner på AUs netværk. Ved specielle forskningsmæssige behov, som ikke kan dækkes af den normale VPN forbindelse, kan der laves en aftale med AU IT og informationssikkerhedschefen. Der kan stilles en VPN-adgang til rådighed for ekstene partere, fx konsulenter o.lign. En sådan forbindelse skal i videst muligt omfang begrænses til de relevante systemer. Eksterne parter skal altid udfylde en skriftlig aftale om VPN adgang, som skal indeholde udførlig beskrivelse af de systemer, der kan tilgås, den/de tilladte metode(r) til fjernadgang, brugerens underskift på at overholde AUs IT-sikkerhedsregler og underskrift fra den ansvarlige leder på AU, som indestår for

	brugerens fjernadgang. Studerende bør ikke have en fuld VPN-adgang, men alene have adgang til de services der er relevante, fx netværksdrev og mail- og kalendersystemet.
Autentifikation	Der skal altid benyttes to-faktor autentifikation ved fjernadgang. Den ene faktor er brugernavn og password, mens den anden faktor er afhængig af hvem man er, og hvorvidt man benytter udstyr, der er privat eller ejet af AU.

5.12 Overvågning af systemadgang og brug

Opbevaring af opfølgningslog	AU IT skal opbevare log for sikkerheds- og fejlhændelser på ethvert system i mindst 3 måneder.
Tidssynkronisering	Alle computersystemer, herunder netværksudstyr, i AU skal benytte korrekt tid. Systemer, som kan benytte automatisk tidssynkronisering skal gøre dette. Andre skal regelmæssigt kontrolleres og sættes.
Fejllog	Fejl skal logges og analyseres, og nødvendige udbedringer og modforholdsregler skal gennemføres.
Administratorlog	Der skal foretages logning af alle handlinger udført af personer med administratorrettigheder i forbindelse med systemkomponenter (inklusive netværksudstyr).
Beskyttelse af logoplysninger	Logfaciliteter og logoplysninger skal beskyttes mod manipulation og tekniske fejl.
Opfølgningslogning	AU IT skal logge sikkerhedshændelser på AUs systemer. En sikkerhedshændelse er alle hændelser, der påvirker enten fortrolighed, tilgængelighed eller integritet.

Hændelseslogning	Alle produktionssystemer skal logge information om adgang og forsøg på adgang for at kunne spore uautoriseret aktivitet.

5.13 Mobile arbejdspladser og hjemmearbejdspladser

Sikkerhedskontroller overfor fjernopkoblet udstyr.	Bærbare computere skal altid sikres med antivirus, firewall og adgangskontrolsystemer. Disse foranstaltninger skal opdateres løbende. Mobile enheder skal anvende antivirus software, såfremt trusselsbilledet tilsiger det.
Adgang til data på AUs netværk	Ved fjernadgang til data på Universitetets netværk skal man være opmærksom på, at følsomme og fortrolige oplysninger ikke må gemmes på privat udstyr. Ved fjernadgang bør man så vidt muligt arbejde på AUs netværksdrev, frem for en lokal kopi. Dermed undgås problemer med versionering, og man er sikker på, at der er en sikkerhedskopi af data. Hvis det ikke er muligt at arbejde på AUs netværksdrev, bør man kopiere sit arbejde tilbage til AUs netværksdrev snarest muligt.
Adgang til applikationer på AUs netværk	Fjernadgang til AUs applikationer er normalt begrænset til standard kontor-applikationer som mail, tekstbehandling, regneark og lignende. Yderligere adgang til applikationer begrænses /gives af de respektive systemejere

5.14 Netværkstjenester med login

Beskyttelse af login	Alle websider, der giver mulighed for login skal benytte SSL. Alle services der kræver login skal benytte kryptering. Telnet, FTP o.lign. er således ikke tilladt. I stedet skal der anvendes SFTP, SSH e.lign. Såfremt transaktioner foregår på et internt lukket netværk kan der

	dispenseres for ovenstående.

5.15 Brug af kryptografi

Brug af kryptering i forbindelse med opbevaring af data	Følsomme og fortrolige informationer skal altid være krypteret, når de opbevares på transportabelt udstyr, fx på bærbare computere, håndholdte computere, usb-sticks m.m. Såfremt det ikke er muligt at anvende kryptering, fx på mobile enheder som tablets og smartphones, bør man undlade at behandle følsomme eller fortrolige data på enheden. Adgangskoder o.lign. må aldrig opbevares ukrypteret, hverken på mobilt eller stationært udstyr. Krypteringen af passwords bør ske via anvendelse af en anerkendt krypteringsteknologi.
Brug af kryptering i forbindelse med dataudveksling	E-mail og data, der indeholder fortrolige informationer, skal altid krypteres under transmission over åbne netværk.

6. Adgangskontrol og metoder

Adgangen til at udføre handlinger på Universitetets it-systemer beskyttes af autorisationssystemer. Systemerne har til formål at sikre mod uautoriserede ændringer, ordrer, fejl og svindel. Medarbejdere og studerende er medvirkende til beskyttelse af informationsaktiverne gennem korrekt brug af autorisationssystemerne.

6.1 Adgangskontrol til operativsystemer

Ændring af administrative kodeord	Administrative kodeord skal ændres, hvis udenforstående får kendskab til disse, eller hvis fx administratorer forlader Universitetet. Administrative kodeord, som kun bruges i nødstilfælde, eller som sjældent bruges (fx Enterprise Admin) skal opbevares i AU ITs brandskab. Disse password skiftes efter hvert brug, og skal være minimum 20 karakterer lange.

Servicekonti	Til opgaver, hvor man ikke ønsker at skifte password, skal der så vidt muligt anvendes servicekonti. Password til servicekonti skal opbevares i AU ITs brandboks, og skal være minimum 20 karakterer lange. Password til servicekonti skal skiftes, såfremt brugere med kendskab til passwordet forlader AU. Servicekonti må ikke bruges af medarbejdere til dagligt arbejde, eller som erstatning til almindelige brugerkonti.

6.2 Adgangskontrol for applikationer

Begrænset adgang til informationer	Adgang for brugere og hjælpepersonale til brugersystemers funktioner og informationer skal begrænses i overensstemmelse med de fastlagte forretningsbetingede krav og informationernes klassifikation.

6.3 Logisk adgangskontrol

Krav til længde af kodeord	Passwords skal indeholde mindst otte karakterer. Længere passwords kan kræves for privilegeret adgang, ved adgang til følsomme informationer eller til forretningskritiske systemer.
Retningslinier for kodeord	Ved brugeroprettelse eller nulstilling af kodeord skal brugere tildeles en sikker, midlertidig adgangskode, som skal ændres umiddelbart efter første anvendelse. Midlertidige kodeord skal være unikke og opfylde de almindelige krav til kodeord.
Krav til skift af kodeord	Kodeord skal skiftes efter højst 180 dage.
Krav til indhold af kodeord	Kodeord skal indeholde kombinationer fra mindst tre af følgende kategorier: Store bogstaver, små bogstaver, tal og specialtegn.

Valg af sikre kodeord	Brugerne bør følge retningslinjerne for oprettelsen af gode passwords. Relaterede Procedurer Sådan laver du et sikkert password

6.4 Administration af adgangskontrol

Udvidede adgangsrettigheder	Udvidede adgangsrettigheder, fx systemadministratorer eller superbrugere i de administrative systemer, må kun tildeles i begrænset omfang og alene ud fra et arbejdsbetinget behov. De udvidede adgangsrettigheder skal registreres. Der skal benyttes særlige brugeridentiteter til de udvidede rettigheder af hensyn til overvågning og opfølgning.
Retningslinier for adgangsstyring	AU IT har i samarbejde med systemejerne det overordnede ansvar for at etablere og vedligeholde procedurer for adgangsstyring.
Gennemgang af brugerprofiler	Alle brugerprofiler i AUs IDM system (og de afledte directory services) skal automatisk gennemgås mindst en gang i kvartalet for at identificere inaktive profiler eller tilsvarende, der skal fjernes eller ændres.
Medarbejderes omplacering	Ved omplacering af medarbejdere skal alle rettigheder for pågældende bruger revurderes.

6.5 Adgangskontrol til netværk

Autentificering ved adgang til netværket	To-faktor autentifikation skal benyttes ved fjernadgang til det interne netværk.
Retningslinier for brug af netværkstjenester	Brugere skal kun have adgang til de tjenester, de er autoriseret til at benytte.

7. Udvikling, anskaffelse og vedligeholdelse

Indkøb, udvikling og implementering af nye systemer på Universitetet skal foregå kontrolleret for at undgå en unødvendig forøgelse af risiko for informationssikkerheden. Når løsninger implementeres, skal sikkerhedsovervejelser altid indgå som en integreret del af processen.

Anskaffelsesprocedurer	Rekvirenten skal sikre, at nyanskaffelser ikke giver anledning til konflikt med eksisterende krav i sikkerhedspolitikken. Anskaffelser må ikke give anledning til forøget risiko for sikkerhedshændelser, med mindre at ledelsen accepterer den øgede risiko. Ethvert nyt system skal klassificeres og der skal laves en risikovurdering og evt. en beredskabsplan, såfremt systemet klassificeres som henholdsvis type A eller B.

7.1 Sikkerhedskrav ved anskaffelser

Sikkerhedskrav til informationsbehandlingssystemer	Universitetets ønsker til nye såvel som bestående systemer skal indeholde krav til sikkerheden med udgangspunkt i en risikovurdering.
Anskaffelser	IT-udstyr skal anskaffes i overensstemmelse med gældende indkøbsaftaler og/eller udbudsregler.
Specifikation af sikkerhedskrav	Sikkerhedskrav skal være dokumenteret i forbindelse med enhver væsentlig IT-system-nyanskaffelse eller IT-systemopgradering.
Systemudvikling udført af ekstern leverandør	For systemudvikling udført af en ekstern leverandør skal følgende indgå i overvejelserne: Har AU behov for at overvåge udviklingsprocessen? Skal der være en afleveringstest? Hvordan sikres dokumenteret løbende kvalitetssikring? Skal AU kræve deponering af kildekoden?

	Skal AU kræve ophavsrettighed på kildekoden?

7.2 Sikkerhed i softwareudviklingsmiljø

Aarhus Universitet anvender en bred vifte af systemer. Nedenstående regler er derfor ikke en "onesize fits all", men skal fortolkes ud fra systemets vigtighed, og klassifikationen af data i systemet.

Sikring af testdata	Data til test skal udvælges, kontrolleres og beskyttes omhyggeligt og i henhold til deres klassifikation. Testdata skal evt. anonymiseres. Det skal formelt godkendes af dataejeren, inden data fra driftsmiljøet kopieres til et testmiljø. Kopiering og brug af data fra driftsmiljøet til test skal logges for at sikre kontrolsporet. Produktionsdata må ikke benyttes direkte fra udviklings- eller testmiljøet.
Kontrolleret adgang til kildekode	Kildekoden til udviklingsprojekter skal sikres mod uautoriseret adgang. Ændringer skal kontrolleres for at sikre integritet. Kildekode må ikke opbevares i driftsmiljøet. Scriptkode som fx PHP, JavaScript, Coldfusion m.v. som først fortolkes ved afvikling, er undtaget fra denne regel.
Migreringsstyring	Migrering fra udvikling til produktion skal undergå test og kontrol for at tilsikre driftsniveau, sikkerhedsniveau og brugbarhed inden implementering. Derudover skal godkendt software sikres mod efterfølgende uønskede ændringer. Hvis muligt, skal kun objekt-kode, ikke kildetekster, migreres til produktionssystemer.
Sikkerhed i applikationsudvikling	Sikkerhed skal inkluderes som en integreret del af alle udviklingsprojekter.

7.3 Integritet for programmer og data

Validering af data	Data, der sendes ind i systemerne, skal valideres for korrekthed. Databasesikkerhed, integritetsstyring og datavalidering bør anvendes for at reducere muligheden for kompromittering af integriteten.

8. Styring af sikkerhedshændelser

Ansvar og forretningsgange for sikkerhedshændelser	Ledelsen skal placere ansvar for at fastlægge forretningsgange, der sikrer en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud.

8.1 Opdagelse og rapportering af hændelser

Rapportering af programfejl	Brugere, der observerer programfejl, skal rapportere dette til deres lokale AU IT helpdesk.
Rapportering af formodede sikkerhedshændelser	Ved konstatering af brud eller formodede brud på IT-sikringsforanstaltninger skal rapportering straks ske til den lokale AU IT helpdesk.
Rapportering af sikkerhedshændelser	AU IT eller eventuelle outsourcingpartnere skal en gang i kvartalet rapportere om hændelser af betydning for sikkerheden i væsentlige systemer. Rapporteringen bør omfatte et overblik over brud på fortroligheden, integriteten og tilgængeligheden. Type A og Type B systemer anses som væsentlige systemer. Endvidere opfattes systemer med følsomme data som væsentlige systemer.

8.2 Reaktion på sikkerhedsmæssige hændelser

Kontrol og opfølgning på sikkerhedsbrud	Brud på sikkerheden, uautoriseret adgang og forsøg på uautoriseret adgang til systemer, informationer og data skal registreres.

Proces for reaktion på hændelser	Informationssikkerhedsafdelingen skal definere telefonnumre, e-mail-adresser og elektroniske formularer til indrapportering af sikkerhedshændelser. Informationssikkerhedsafdelingen skal etablere og vedligeholde en procedure, der sikrer et passende svar til personer, som rapporterer en mulig sikkerhedshændelse.

8.3 Opfølgning på hændelser

Vurdering af tidligere hændelser	Mindst en gang om året skal informationssikkerhedsafdelingen og AU IT gennemgå den forgangne periodes hændelser og på denne baggrund anbefale hvorvidt IT-sikkerhedssystemet kan forbedres eller præciseres.
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.
At lære af sikkerhedsnedbrud	Informationssikkerhedsafdelingen skal opsamle og præsentere hændelserne, så andre kan drage læring af dem.
Information om sikkerhedshændelser	AU skal på faktuel vis informere berørte parter internt og eksternt om eventuelle sikkerhedshændelser. Informationssikkerhedschefen og/eller vicedirektøren for IT, bør godkende alle eksterne meddelelser.
Opfølgning på rapporterede sikkerhedshændelser	Informationssikkerhedschefen er ansvarlig for at opsamle statistik for rapporterede sikkerhedshændelser.

9. Beredskabsplanlægning og fortsat drift

Risikostyring og katastrofeplanlægning har til formål at mindske risikoen for og effekten af uforudsete hændelser. Nødplaner skal være med til at opretholde driften, således at skaderne for Universitetet minimeres.

9.1 Beredskabsplaner

Typer af beredskabsplaner	AU har to typer af beredskabsplaner. En overordnet beredskabsplan for it-driften, samt mere systemspecifikke beredskabsplaner for type A systemer. Ansvaret for de overordnede beredskabsplaner ligger hos teamlederne i AU IT. Ansvaret for de systemspecifikke beredskabsplaner ligger hos systemejerne.
Afprøvning af beredskabsplaner	Afprøvning af en beredskabsplan skal som minimum omfatte en skrivebordstest af de forskellige scenarier samt med jævne mellemrum en simulering af en beredskabssituation med henblik på at træne deltagerne i håndtering af deres roller.
Vedligeholdelse af beredskabsplaner	De generelle beredskabsplaner skal opdateres to gange årligt for at sikre, at de er tidssvarende og effektive. Ansvaret ligger hos teamlederne. De systemspecifikke beredskabsplaner, skal gennemgås og evt. opdateres ved ændringer i de berørte systemer.
Retablering af forretningskritiske systemer på ny lokation	For type A systemer, bør beredskabsplanerne afspejle muligheden for at de fysiske lokationer kan være utilgængelige eller ødelagt, og at man derfor bør kunne etablere nøddrift på andre lokationer.
Uddannelse i beredskabsplaner	Systemejeren har ansvaret for, at der foregår tilstrækkelig uddannelse af medarbejdere i de aftalte beredskabsprocedurer, inklusive krisehåndtering.
Aktivering af beredskabsplanen	Det skal være klart defineret, hvem der har ansvaret for aktivering af beredskabsplaner. Medarbejdere, der udgør en del af beredskabsplaner, skal være informeret

	om dette ansvar. Alle medarbejdere skal være informeret om beredskabsplanernes eksistens.

9.2 Sikkerhedskopiering

Procedure for sikkerhedskopiering	AU IT skal have en overordnet backup og restore strategi, som følges for alle systemer, hvis ikke andet er aftalt eller fremgår af systemdokumentationen. Backup og restore strategien, skal sikre at der løbende foretages restore test af væsentlige systemer. For systemer, hvor en komplet restore ikke er praktisk, skal man lave stikprøver med tilfældige data, for at sandsynliggøre at hele systemet kan genetableres. Såfremt der er særlige krav til backup, fx specielle arkiveringskrav e.lign. er det systemejeres ansvar af aftale dette med AU IT.
Opbevaring af sikkerhedskopier og redundante systemer	Backup, sikkerhedskopier og redundante systemer skal placeres således at uheld på den primære lokation ikke kan forplante sig til den sekundære lokation.

10. Lovgivning, kontrakter og etik

Mange aspekter af Universitetets virke kan være omfattet af lovgivning. Det er nødvendigt, at Universitetet overholder gældende lovgivning og regler, der gælder for statens virksomheder, samt at man foretager indrapportering som foreskrevet til offentlige myndigheder.

10.1 Overholdelse af lovmæssige krav

Identifikation af relevant lovgivning	Ledelsen er ansvarlig for at identificere lovgivning der er relevant for AUs drift, eller udpege en person der er ansvarlig for denne opgave.

10.2 Ophavsret

Retningslinier for ophavsrettigheder	Ledelsen har det overordnede ansvar for, at AU fastholder en passende

	opmærksomhed på ikke at krænke tredje parts ophavsrettigheder. Brugere må ikke kopiere, konvertere eller udtrække information fra billed- og lydfiler eller tilsvarende ressourcer med mindre dette specifikt tillades fra rettighedshaveren, eller såfremt der ligger en aftale med interesseorganisationer som fx CopyDan. Brugere må ikke kopiere bøger, artikler, rapporter eller andre dokumenter, helt eller delvist, med mindre dette specifikt tillades fra rettighedshaveren, eller såfremt der ligger en aftale med interesseorganisationer som fx CopyDan e.lign.

10.3 Identificerede love og regelsæt

Regulering på kryptografiområdet	Kryptografiske produkter reguleres i mange lande. Hvis kryptografi benyttes, skal disse forhold derfor undersøges nøjere ved samarbejde med udenlandske partnere, rejser eller import/eksport.

10.4 Kontrol, revision og afprøvning

Sikkerhedstest	Mindst fire gange om året skal der udføres sikkerhedstest af sikkerhedsniveauet i eksternt tilgængeligt netværksudstyr og servere. Sikkerhedstesten bør være en kombination af automatiske og manuelle test. Mindst 2 gange årligt skal der foretages en sikkerhedstest af interne sikkerhedsforanstaltninger, restriktioner, begrænsninger og netværksforbindelser. Sikkerhedstesten kan omfatte både automatiske scanninger og manuelle inspektioner. Evt. sårbarheder skal evalueres og risikovurderes. Håndtering af sårbarhederne indgår herefter i den normale opgave prioritering.

Revision af sikkerhedspolitik	Informationssikkerhedsafdelingen skal kontrollere at sikkerhedspolitikken er indarbejdet i AU ITs daglige arbejde, og at regler og procedurer bliver overholdt. Kontrollen skal foretages årligt, og resultatet skal rapporteres til det centrale informationsikkerhedsudvalg og Universitetsledelsen.