Syddansk Universitet

IT-sikkerhedspolitik

IT-sikkerhedshåndbog

Universitetets regler for informationssikkerhed

Version 2010.4

17-11-2010

Indholdsfortegnelse

Generelt

1 Indledning

Hvad er informationssikkerhed?

Information er et aktiv, der i lighed med øvrige virksomhedsaktiver er væsentlig for universitetets forretningsaktiviteter og derfor skal beskyttes på passende vis. Dette er specielt vigtigt med den øgede digitale informationsudveksling, som har medført en forøgelse af både trusler og sårbarheder, jf. eksempelvis OECD guidelines.
Information kan eksistere i mange former. Det kan være skrevet på papir, lagret elektronisk, transmitteret via kabler eller gennem luften, ligge på en film eller være fremført i en konversation. Uanset formen skal information beskyttes i henhold til dens betydning for universitetet.
Informationssikkerhed defineres som den samlede mængde af beskyttelsesforanstaltninger, der skal sikre universitetets daglige drift, minimere skader, samt beskytte universitetets investeringer og sikre grundlaget for nye forretningsmuligheder.
Informationssikkerhed opnås ved at implementere, overvåge, revurdere og løbende ajourføre et passende sæt af beskyttelsesforanstaltninger bestående af politikker, praksis, procedurer, organisatoriske tiltag og system- eller maskintekniske funktioner.

Hvorfor er informationssikkerhed nødvendig?

Information og informationsbehandlingsprocesser, -systemer og -netværk ervæsentlige universitetsaktiver. At definere, etablere og vedligeholde en passende informationssikkerhed kan være afgørende for universitetets konkurrencedygtighed, rentabilitet, omdømme og efterlevelse af gældende lovgivning.
Informationssikkerhed er væsentlig både for den offentlige og private sektor og for at beskytte kritisk infrastruktur. En troværdig informationssikkerhed er en afgørende forudsætning for digital forvaltning og e-handel. Samtidigt giver det øgede antal adgangsmuligheder, fjernarbejdspladser og nye services for både studerende og medarbejdere en øget sårbarhed, da det ikke længere er muligt at forlde sig på traditionelle, centrale sikringsforanstaltninger.

Formulering af sikkerhedsbehov

Det er af afgørende betydning, at universitetet definerer sine sikkerhedsbehov. Man kan her tage udgangspunkt i tre hovedkilder:

- Universitetets egen risikovurdering baseret på universitetets forretningsstrategi og -målsætning. Her vurderes trusselsbilledet, universitetets sårbarhed og de forretningsmæssige konsekvenser, hvis et uheld skulle ske.
- Eksterne krav til universitetet, dets samarbejdspartnere og dens leverandører. Disse krav kan være lovgivning, bekendtgørelser, forordninger, samarbejdsaftaler eller hensyn til det omgivende samfund.
- Interne krav afledt af universitetets egne kvalitetskrav for at støtte en specifik forretningsmålsætning.

Opgørelse af sikkerhedsbehov

Sikkerhedsbehov identificeres ved en metodisk vurdering af sikkerhedsrisici. Udgifterne til sikringsforanstaltninger skal holdes op mod de forretningsmæssige tab herunder også de immaterielle tab som f.eks. dårligt omdømme ved en given sikkerhedsbrist. En risikovurdering kan gennemføres for den samlede virksomhed, for enkelte afdelinger eller for specifikke informationssystemer, systemkonponenter eller -ydelser. Resultatet af risikovurderingen indgår i universitetsledelsens risikostyring, hvor de enkelte risici prioriteres, og det besluttes, hvilke sikringsforanstaltninger der skal iværksættes. Det vil i mange tilfælde være nødvendigt at

gennemføre risikovurderingen i flere trin for at bevare det samlede overblik.
Endelig skal det understreges, at en risikovurdering skal gentages regelmæssigt og ved større organisatoriske eller teknologiske ændringer.

Valg af sikringsforanstaltninger

Når universitetets sikkerhedsbehov og risici er afdækket, og risiciene er prioriterede i henhold til deres væsentlighed, skal de basale sikringsforanstaltninger og relevante skærpede sikringsforanstaltninger udvælges og implementeres for at sikre, at risiciene bliver reduceret til et acceptabelt niveau. I enkelte specielle tilfælde kan det blive nødvendigt at udvikle og implementere yderligere foranstaltninger. Man skal dog være opmærksom på, at ingen sikringsforanstaltninger kan give fuldstændig sikkerhed. De skal altid suppleres med en ledelsesmæssig overvågning og en løbende ajourføring for at sikre deres effektivitet.

2 Termer og definitioner

Ordforklaring

Adgangskontrol - fysisk: Enhver fysisk sikringsforanstaltning mod uautoriseret adgang til et sikkerhedsområde.
Adgangskontrol - logisk: Enhver programmerbar sikringsforanstaltning mod uautoriseret anvendelse af universitetets informationsaktiver.
Adgangskontrolanlæg, elektronisk (ADK-anlæg): Et anlæg, der har til opgave at overvåge og kontrollere trafikken gennem en fysisk adgangsvej. Via en indlæseenhed foretages der en entydig identifikation, som sammenholdt med tid og sted legitimerer og åbner den pågældende adgangsvej.
Adgangskontrolliste: En liste over brugere og deres tildelte autorisationer og rettigheder til at anvende universitetets informationsaktiver.
Se også "autorisation" og "rettigheder".
Adgangskode (password): Kombination af tegn, som benyttes til verifikation af en brugers identitet.
Adgangskort: Et adgangskort er en identifikationsbærer, der fx er udformet som et "plastickort". Kortets dataindhold identificerer den person, kortet er udstedt til.
Aktiver: Alt, der har værdi for universitetet - således også immaterielle værdier som fx informationsbehandlingssystemer, data, procedurer og dokumentation.
Se også "informationsaktiver".
Anråb/svarsystem: En sikringsmekanisme, der validerer, hvorvidt en opkaldende brugers forsøg på at få tilladelse til at anvende et informationsbehandlingssystem kan godkendes. Inden godkendelsen gives, sender den opkaldte node et "anråb" til den opkaldende node med krav om et autenticitetsbevis. Kun, hvis det modtagne svar"svar"/autenticitetsbevis godkendes, gives der tilladelse. På engelsk kaldes det "Challenge/Respons"-system.
Applikationssystem: Se "informationsbehandlingssystemer".
Arbejdsstation/plads: Betegnelse på en PC, skærmterminal eller lignende, der benyttes af en enkelt bruger, og som er tilkoblet et netværk, der giver mulighed for at anvende fælles ressourcer og datakommunikation.
Arkiv (dataarkiv): Opbevaringssted, hvor man systematisk opbevarer data på maskinlæsbare medier.
Autenticitet: Egenskab, der sikrer, at en ressource eller person er den hævdede (anvendes fx ved log-on og elektronisk underskrift/digital signatur).
Autentificering/autentifikation: Verifikation af en afsenders eller en modtagers autenticitet.
Automatisk Brandalarmerings Anlæg (ABA-anlæg): Anlæg, udført i overensstemmelse med forskrift 232 fra Dansk Brandteknisk Institut, der overvåger mod brandkendetegn og alarmerer i tilfælde af ildebrand.

Automatisk Indbrudsalarmerings Anlæg (AIA-anlæg): Anlæg, udført i overensstemmelse med DS 471, der overvåger mod indbrud og alarmerer i tilfælde af indbrud.
Autorisation: Rettighed til at udføre specifikke funktioner samt tilladelse til at anvende på forhånd tildelte ressourcer.
Backup af data: Sikkerhedskopieringsaktivitet. Lagring af vigtige data og programmer på et eksternt lagermedie, der kan opbevares sikkert og anvendes i tilfælde af, at de originale data er gået tabt.
Backupansvarlig: Den person, der er ansvarlig for sikkerhedskopiering.
Barriere: Fysisk afgrænsning, der har til formål at danne en adskillelse mellem et bestemt område og omgivelserne. Afgrænsningen kan være reel (fx væg) eller eventuelt være symbolsk (fx malet linje på gulv suppleret af adgang forbudt skilt.
Basissystemer: Opdeles i operativsystem(er) og hjælpeprogrammer. Se også "informationsbehandlingssystemer".
Beredskabsplan: En skriftlig, opdateret dokumentation for, hvad der skal iværksættes af definerede redningsaktioner, og hvem der skal igangsætte disse, hvis der indtræder en forstyrrende afbrydelse af universitetets forretningsprocesser, der kræver en redningsplan.
Bibliotek (for data og programmer): Et system, der registrerer opbevaring af og fører kontrol med til- og afgang af fx basis- og netværksprogrammer, brugerprogrammer, udviklings- og testprogrammer, programkildekoder og data, samt hvilke brugere der har fået tilladelse til at anvende disse. De forskellige biblioteksdele holdes adskilt.
Brugerprogram/system: Se "informationsbehandlingssystemer".
"Blå blanket": Blanket, som benyttes til at anfordre oprettelse, ændringer og nedlæggelse af brugerkonti på IT-systemerne.
Bygningsskallen: Se "Skallen".
Celle: Et barrikaderet lokale inden for et sikkerhedsområde, der er beskyttet med yderligere sikring i form af bygningsmæssig adskillelse og med separat adgangskontrol.
Centralt udstyr: Informationsbehandlingsudstyr, hvor flere arbejdsstationer (klienter) er tilsluttet en server eller en samling af servere ("cluster").
Se også "informationsbehandlingsudstyr".
CE-mærke: Et mærke, der påføres elektrisk udstyr, og som derved garanterer, at EU-regler og -direktiver er overholdt med hensyn til personsikkerhed og EMC.
Chat: Snak eller diskussion mellem to eller flere personer over et netværk. Kommunikationen sker via tastaturet på pcen.
Data: En formaliseret repræsentation af kendsgerninger eller instruktioner.
Dataansvarlig: En person der er udpeget til at have sikkerhedsmæssigt ansvar for et system- og/eller data.
Se også "ejer".
Dataarkiv: Se "arkiv".
Dataintegritet: Se "integritet".
Datamedier: Fysiske lagringsmedier, hvorpå der ad elektronisk vej er lagret data, fx på disketter, bånd, diske, CD-ROM, EPROM, USB-lagringsenheder.
Dekryptering: Den modsatrettede proces af en kryptering.
Diagnoseport: Tilkoblingsstik i informationsbehandlingsudstyr til kommunikationsforbindelse med ekstern servicetjeneste. Via kommunikationsforbindelsen kan en service tekniker fra et andet geografisk sted registrere udstyrets driftstekniske data, statusinformationer og øvrige informationer samt foretage fejlrettelser, under forudsætning af at diagnoseporten er aktiv/åben.
Se også "port".

Digital signatur: En digital signatur dannes ved en kryptografisk transformation af en hashværdi beregnet ved hjælp af meddelelsen, og som knyttes til denne. Bruges til verifikation af meddelelsens integritet og til verifikation af afsenderens autenticitet.
Downloade: At downloade betyder at kopiere data (fx programmer) fra en computer på Internettet til ens egen pc.
"Ejer": For manuelle systemer er der ofte i en virksomhed en naturlig forventning til, hvem der er "ejer" af et system og dets informationer, og at "ejeren" har såvel ansvar som rettigheder vedrørende informationerne. Bogholderen "ejer" de financielle informationer, salgslederen "ejer" de afsætningsmæssige informationer, og lagerforvalteren "jer" de beholdningsmæssige informationer. Ansvar for og rettigheder til systemer og informationer bliver ofte mere diffust, når et system digitaliseres. Derfor er det nødvendigt, at der gøres noget aktivt for at bibeholde dette ansvar. "Ejeren" bestemmer, hvilke brugere der kan anvende et system og dets informationer.
Engangskode: En logisk adgangskontrolmetode, hvorved den opkaldte parts valideringssystem er synkroniseret med en brugers transportable kodeomsætter (kan være elektronisk eller blot en udskrevet liste). Brugeren benytter et givet kodeord i omsætteren, der omsætter en engangskode ved hjælp af en indbygget algoritme eller ved simpelt tabelopslag. Den nye kode kan kun benyttes en gang. I visse systemer skal den benyttes øjeblikkeligt, idet den kun er gyldig i en kort periode.
Enhedschef: Den formelle chef for en enhed. Enhederne kan variere i de enkelte afsnit. Er der tale om universitetet er rektor enhedschef. Er der tale om fakulteter er dekanen enhedschef. For biblioteket er overbibliotekaren enhedschef og for fællesadministrationen er direktøren enhedschef. På institut- og afdelingsniveau er institutleder og afdelingsleder enhedschef.
Entitet: En uafhængig enhed, der har selvstændig eksistens, fx en node/en person.
Firewall: Se "logisk filter".
Fortrolige informationer: Informationer, som kun må være tilgængelige for autoriserede medarbejdere, fx følsomme personoplysninger, samarbejdspartneres forhold, oplysninger i relation til patenter m.v.
Fortrolighed: Egenskaben, at informationen ikke gøres tilgængelig eller kan afsløres for uautoriserede personer, entiteter eller processer.
Se også "konfidentialitet".
Funktionsadskillelse: Funktionsadskillelse er en sikringsforanstaltning, hvis hovedprincip er, at den samme person ikke både må udføre og godkende en given operation eller funktion.
Fysisk sikring: Sikringsforanstaltninger, der baserer sig på fysiske eller mekaniske foranstaltninger for imødegåelse af tyveri, indtrængning, hærværk, eller anden ødelæggelse af aktiver.
Se også "tyverisikring, mekanisk".
Fældeovervågning: En elektrisk tyverisikring fx i en passageåbning, der evt. kan supplere en rum- og skalovervågning.
Hacking: Betegner den ulovlige handling, at en ukendt og uautoriseret person i det skjulte anvender andres informationsbehandlingsudstyr, systemer, informationer eller data. Handlingen udføres fx ved hjælp af teknisk omgåelse af de logiske adgangskontrolsystemer.
Se også "penetrering".
Hashværdi: En gentagelig beregning med hjælp af bestemte algoritmer af fx et programs "tværsum" til verifikation af, at selve programmet ikke er ændret.
Hemmeligholdelse: Sikkerhed for, at indholdet af en meddelelse ikke kan afsløres af uvedkommende.
Hjælpeprogram: Standardbetegnelse for værktøjsprogrammer, der anvendes til fx editering, filkopiering, filsammenligning, fejlrettelser og optimering.
Identitetskort (ID-kort): Et kort eller lignende, der identificerer indehaveren, som legalt er i besiddelse af identifikationen (fx pas, betalingskort og kørekort).

Indbrudskriminalitet: Foreligger, når en person i berigelseshensigt har skaffet sig ulovlig fysisk adgang til aktiver.
Inddata: Alle data, der overføres til eller indrapporteres i et informationsbehandlingssystem.
Information: Den mening, der tillægges en mængde af data.
Se også data.
Informationsaktiver: De aktiver, der har tilknytning til og er nødvendige for virksomhedens informationsbehandling.
Informationsbehandlingssystemer: Betegnelsen for en samling programmer til løsning af en samlet mængde opgaver. Grundlæggende opdeles informationsbehandlingssystemer i to hovedgrupper:

- **Basissystemer**, der oftest er hardwareafhængige, består af **operativsystem**(er) og **hjælpeprogram** (mer). Basissystemer, ofte benævnt styre-, system- eller driftssystemer, er grundlaget for al informationsbehandling og skal være i funktion, før alle andre programmer kan anvendes.

  Operativsystemerne styrer kommunikationen mellem datamaskinen, andre datamaskiner, andet udstyr og brugerprogrammer og brugere.

  Hjælpeprogrammerne er værktøjer, der benyttes til fx at rette fejl i operativsystemet eller foretage optimering af driften på informationsbehandlingsudstyret.

- **Brugersystemer**, der er afhængige af det valgte basissystem, opdeles i **egenudviklede systemer** og **standardsystemer**.

  Egenudviklede systemer er unikke, specialudviklede programmer til specifikke opgaveløsninger eller sammenhængendeopgavekomplekser i en virksomhed eller mellem flere virksomheder. De udvikles som en specialopgaveaf en udvalgt programleverandør eller af en virksomheds egne programmører.

  Standardsystemer er universelle programmer til løsning af virksomheders generelle arbejdsopgaver som fx bogholderi,lønningsregnskab, ordre- og lagerstyring, kalkulation, tekstbehandling og illustrationstegning. Standardsystemeranskaffes fra mange forskellige lagerførende leverandører. De kan af den enkelte bruger ved at vælgemellem nogle indbyggede parametermuligheder tilpasses dennes ønsker om opsætning og de regelsæt, hvorefterstandardsystemet skal fungere. Ofte sammensættes flere af ovennævnte programtyper til en integreret programpakke/office suite.

Informationssikkerhed: Alle aspekter relateret til definering, gennemførelse og vedligeholdelse af fortrolighed, integritet, tilgængelighed, ansvarlighed, autenticitet og pålidelighed omkring informationsbehandlingssystemer.
Informationssikkerhedspolitik: Ledelsens overordnede retningslinjer for strategier, direktiver og forretningsgange, der regulerer, hvordan universitetets informationer, inklusive følsomme oplysninger, anvendes, styres, beskyttes og distribueres på universitetet og dets informationsbehandlingssystemer.
Integritet: Sikkerhed for, at indholdet af en meddelelse eller en post i et register er korrekt og komplet.
Interne informationer: Informationer om universitetets arbejdsgange, fx dokumentation af interne procedurer.
IT-sikkerhedskoordinator: Den person, der er ansvarlig for udarbejdelse af regler og procedurer for sikringsforanstaltninger for universitetets informationsbehandling.
IT-sikkerhedsrepræsentant: Den person i den enkelte enhed, der har det daglige ansvar for IT-sikkerheden i enheden og derudover repræsenterer enheden i IT-sikkerhedsudvalget.
IT-stamblad: IT-stambladet udarbejdes for såvel materiel (servere) som systemer (applikationer). IT-stambladet skal omfatte de data, der er nødvendige for den daglige drift, sikkerhedsregler og -opsætning, service, reparation samt genetablering af systemerne efter alvorlige fejl og/eller situationer, hvor anlægget skal nyanskaffes.
IT-revision: Aktivitet, der udføres til kontrol af, at den ønskede informationssikkerhed i henhold til universitetets politik for informationssikkerhed og forskrifter for informationsbehandling er til stede og efterleves. Revisionen

dokumenteres og forelægges virksomhedens ledelse.
ITG: Universitetets IT-sikkerhedsudvalg.
ITK: Universitetets IT-koordineringsgruppe.
ITS: IT-service i fællesområdet.
ITU: Universitetets IT-udvalg.
Junk-mail: Junk-mail kan oversættes til noget i retning af skraldespandspost. Det kan være på papir, på fax eller e-mail. Det er mest udbredt i e-mail, fordi det er let og billigt at sende til mange på én gang. Junk-mail er typisk uopfordrede og useriøse e-mails med tilbud om hvad som helst.
Karakter: Ethvert stort eller lille bogstav, tal eller tegn, der anvendes enkeltstående eller som en tilladelig sekvens.
Kildekode: Et informationsbehandlingsprogram, der er skrevet i et symbolsk og standardiseret programmeringssprog.
Klartekst: Ubeskyttet og umiddelbar læselig tekst.
Kompatibilitet: Den forenelighed, der skal være til stede, for at noget (et system) kan virke sammen med noget andet (andre systemer).
Konfidentialitet: Se hemmeligholdelse.
Kontrolspor: En specificeret udtrækning og samling af data, hvormed det kan konstateres, hvilke transaktioner der er udført, hvornår og af hvem, og hvilke direkte og indirekte konsekvenser de har haft på tidligere eller oprindelige data.
Kryptering: Omsætning (kodning) af læsbar klartekst, således at teksten ikke er læsbar for udenforstående, uden at de er i besiddelse af krypteringsforskriften og krypteringsnøglen.
Log-off: Er den afsluttende procedure for brugeren af et informationsbehandlingssystem, hvorved forbindelsen mellem en arbejdsstation og programmerne afbrydes.
Log-on: Er den nødvendige indledende procedure, hvormed en bruger etablerer sin tilladelse til at anvende informationsbehandlingsudstyr og -systemer.
Logisk bombe: En række destruktive programmer eller makroer, der er skjult i et i øvrigt normalt informationsbehandlingssystem, der regelmæssigt køres. Den destruktive kode aktiveres, når nogle forudsatte betingelser er opfyldt. Man kan fx tænke sig en logisk bombe indlagt i et firmas lønberegningssystem. Den logiske bombe udløses, når en medarbejder ikke længere er på lønningslisten. Bomben ødelægger fx vitale firmadata.
Logisk filter: Et filtreringssystem, fx en kombination af en router og nogle programmerede kontroller ved den grænse, hvorigennem datakommunikationen skal passere for at komme fra et netværk til et andet netværk. Ved grænsen bliver datakommunikationen tilladt, videredirigeret eller nægtet passage baseret på et sæt vedtagne regler.
Lokalnetværk (LAN): Et netværk, der benyttes til datatransmissioner mellem forskelligt informationsbehandlingsudstyr inden for samme virksomhed, og som i nogle tilfælde kobles sammen med andre interne og eksterne netværk, med offentlige netværk eller andre datakommunikationsforbindelser.
Se også netværk.
Makulering: Destruktion, opstrimling eller sønderrivning af læsbare medier i strimmel- eller flagestørrelser, der ikke kan gensammensættes til læsbare informationer.
Mikroprocessorenhed: Speciel form for identifikationsbærer baseret på fx et plastikkort eller en USB-enhed med indlagt datahukommelse og dataprocessor. Ud over at identificere ejeren kan kortet indeholde et stort antal data (evt. kryptograferet), der kan opdateres og regulere kortets anvendelsesmuligheder ved hjælp af specielle autorisationskoder og algoritmer, fx certifikater til digital signatur.
Netværk: Generel betegnelse, der dækker alle typer af sammenhængende datakommunikationsforbindelser mellem centralt udstyr, servere, arbejdsstationer og andet kommunikationsudstyr.

Netværksansvarlig: Den person, der har ansvaret for drift af og sikkerhed i netværket eller segmenter af netværket.
Node: Adresserbart punkt på et datanetværk (fx en arbejdsstation, printer, switch, netværksomskifter, router).
Objektkode: Et maskinlæsbart program, der umiddelbart kan afvikles på en datamaskine.
Offentlige informationer: Informationer der er underlagt bestemmelserne om offentlighed i forvaltningen.
Operativsystem: Et grundlæggende program eller programkompleks, der foretager den overordnede styring af alt, hvad der kan afvikles på informationsbehandlingsudstyr.
Opgradering: Udskiftning af hidtil anvendt informationsbehandlingsudstyr og -systemer med andet kompatibelt materiel, som kan yde mere eller muliggøre bedre rationel anvendelse.
Opkobling: Etablering af en datakommunikationsforbindelse.
Orm: Et selvstændigt program, der er i stand til at lave kopier af sig selv hele tiden uden at være afhængig af et andet program. Kan spredes via datanetværk og databærende medier m.v. til andet udstyr, hvor ormen starter sig selv og derved stjæler datakraft fra udstyret, som herved overbelastes.
Overvåget område: Et afgrænset område, der fx elektronisk tyveri- og brandovervåges af et automatisk alarmeringsanlæg.
Password: Se adgangskode.
Penetrering: At skaffe sig mulighed for ulovligt at anvende informationer, data eller datasystemer uden at have den fornødne autorisation og uden at blive opdaget.
Se også hacking.
Personaleansvarlig: En medarbejders nærmeste leder.
Piratkopiering: At foretage kopiering af et informationsbehandlingsprogram eller information i strid med lovgivningen om licensaftaler.
Port: Generel betegnelse for elektriske kredsløb, der virker som interface mellem informationsbehandlingsudstyr, arbejdsstation og andre ydre tilsluttede enheder via datakommunikationsforbindelser.
Privilegier: Betegnelsen for de rettigheder, som specificeres for en autoriseret bruger til legalt at anvende en vedtagen delmængde af informationsbehandlingsressourcer, herunder data, til sine arbejdsopgaver.
Protokoller: Regler, som er reguleret af standarder, normer, tekniske metoder og specifikationer, der er fastsat med det formål at kunne fortolke og udveksle data.
Public Key: Den del af det asymmetriske kryptograferingsnøglesæt, der er gjort offentlig tilgængelig for dem, der har fået tildelt deres egen specifikke kryptograferingsnøgle for at kunne transformere et kryptograferet dokument.
Pålidelighed: Egenskab, der sikrer, at den forventede opførsel og de forventede resultater opnås.
Rettigheder: Se privilegier.
Revision, økonomisk: En kontrol af, hvorvidt en virksomheds regnskaber, hvad enten de fremstilles manuelt eller elektronisk, udføres betryggende og i overensstemmelse med bogføringspligten, lovgivningen og virksomhedens bestemmelser og forretningsgange.
Risiko: Det beregnede eller konstaterbare resultat af en kombination af hyppigheden af en uønsket hændelse og omfanget af konsekvenserne (tabene).
Risikoanalyse: En detaljeret og systematisk procedure til at afdække virksomhedens trusler og sårbarheder samt konsekvenserne af uønskede hændelser.
Risikostyring: Den ledelsesmæssige styring af virksomhedens indsats for at imødegå forretningsmæssige risici.
Risikovurdering: En overordnet afvejning af virksomhedens risikobillede.
Sikkerhed: Resultatet af alle de sikringsforanstaltninger, der er foretaget for at imødegå de aktuelle trusler.

Sikkerhedsmiljø: Det samlede sæt af sikringsforanstaltninger og kontroller, virksomheden har etableret for at sikre, at sikkerhedspolitikken bliver efterlevet.
Sikkerhedsområder: Alle universitetets bygninger på de forskellige campusser er opdelt i forskellige sikkerhedsområder. De enkelte sikkerhedsområder og deres karakteristika er nærmere definerede herunder:

- Et *offentligt* sikkerhedsområde er karakteriseret ved, at der er fri, ukontrolleret adgang til området det meste af døgnet. Et område kan således godt være *offentligt* i brugsmæssig og sikkerhedsmæssig betydning, selv om det er aflåst om natten; det gælder fx visse parkområder.
- Et *halvprivat* sikkerhedsområde er karakteriseret ved, at det kun i begrænset omfang er muligt at kontrollere personers adgang. Typisk er der tale om indgangspartier, forhaller, trappeopgange og lignende.
- Et *privat* sikkerhedsområde er karakteriseret ved, at det er muligt at føre kontrol med adgang til og opholdsmuligheder i sikkerhedsområdet. Typisk for denne kategori er kontorer, opholdslokaler, lagerrum, værksteder og øvrige arbejdslokaler.
- Et *særligt* sikkerhedsområde er karakteriseret ved, at det udover at være privat har særlige forhold, der skal tages IT-sikringsmæssige hensyn til. Typisk stilles der skærpede krav til begrænsning af adgangsforhold og opholdsmuligheder, herunder til begrænsning af, hvilke personalekategorier der kan få adgang. *Særlige* sikringsområder er fx lokaler, der inddeles i separate funktionsadskilte celler til fx driftsafvikling og overvågning, servere, kontorer med arbejdsstationer og printere, rum til teleudstyr og krydsfelter samt dataarkiver.

Sikkerhedsrevision: Se IT-revision.
Sikkerhedsstyring: En løbende proces, hvor ledelsen gennem en systematisk rapportering om ændringer i risikobilledet, observerede svagheder samt konkrete hændelser til stadighed kan revurdere den fastlagte sikkerhedsstrategi og foretage de fornødne justeringer for at fastholde det ønskede sikkerhedsniveau.
Sikret område: Et område, hvis afgrænsninger er mekanisk/fysisk indbrudssikrede.
Sikringsforanstaltning: En praksis, procedure eller mekanisme, der reducerer sårbarheden. Dvs. alle de bestræbelser, forholdsregler og foranstaltninger, der tages i anvendelse for at modvirke såvel utilsigtede som tilsigtede fejl, tab og misbrug af data samt sikring af tilgængelighed for de autoriserede brugeres anvendelse af udstyr og data.
Single sign-on-procedure: Log-on-procedure, der bevirker, at det ikke er nødvendigt efter den første log-on-procedure at foretage selvstændige log-on til flere specifikke systemer.
Skallen: Samtlige de bygningsdele, som ud fra et indbrudssikringsmæssigt synspunkt danner begrænsning for et rumligt afgrænset område.
Skalovervågning: En elektronisk indbrudsovervågning af bygningsdele i skallen.
Skalsikring: En mekanisk indbrudssikring af bygningsdele i skallen.
Skrivebeskyttelse: Sikringsforanstaltning, der har til formål at forhindre utilsigtede tilføjelser, ændringer eller sletninger af eksisterende data på datamedier.
Social engineering: En form for svindel, hvor den person der udfører social engineering, prøver at narre brugernavne og kodeord fra autoriserede brugere, fx ved at udgive sig for at være en IT-supporter, der forsøger at løse et problem på brugerens arbejdsstation. De afslørede brugernavne og kodeord bruges derefter af svindleren til at få uautoriseret adgang til systemerne.
Spam-mail: Misbrug af e-mail. At spamme betyder populært sagt, at man sender uønskede mails, typisk i reklameøjemed.
Se også "junk-mail".
Standardsystem: Se informationsbehandlingssystemer.
Systemadministrator: Den person, der har ansvaret for drift af og sikkerhed i et eller flere IT-systemer.

Systemrevision: Se IT-revision.
Sårbarhed: Mangel på sikkerhed, som kan medføre uønskede hændelser.
Test: Verifikation af kvaliteten af et givet system og/eller program.
Tilgængelighed: Egenskaben at være tilgængelig og anvendelig ved anmodning fra en autoriseret entitet.
Transaktionsspor: Se kontrolspor.
Trojansk hest: Et program, der ser ud og virker som et almindeligt program, men som indeholder en eller flere uautoriserede programkommandoer eller programsekvenser.
Trussel: En potentiel årsag til en uønsket hændelse, som kan forvolde skade på virksomheden.
Tyverisikring, elektrisk: Sikringsforanstaltning til overvågning af områder eller genstande ved hjælp af et AIA-anlæg.
Tyverisikring, mekanisk: Hensigtsmæssig anvendelse af bygningsdele, låseenheder mv., således at tyveri og utilsigtet gennembrydning eller oplukning vanskeliggøres. Bygningsdele kan fx være specielt udformede eller forstærkede.
Uafviselighed: En procedure, der beviser, at en specifik bruger på et givet tidspunkt har sendt en anden specifik bruger en bestemt meddelelse.
Uddata: Alle data, der efter endt behandling i informationsbehandlingsudstyret enten placeres i et baggrundslager eller et eksternt datamedie eller overføres til en printer for udskrift.
Uønsket adfærd, eksempler på: Det er blandt andet ikke tilladt at:

- forsøge at læse, slette eller kopiere andres e-mail,
- forfalske e-mail-adresse,
- afsende generende, obskøne eller truende meddelelser til andre brugere,
- afsende junk-mail, kædebreve, spam-mail eller lignende former for meddelelser,
- anskaffe eller bibeholde brugernavn (bruger-id) under falske forudsætninger,
- udlåne eller dele "bruger-id/password" med andre. Sker det, er indehaveren personlig ansvarlig for alle handlinger, der udføres af låneren,
- slette, gennemse, kopiere eller modificere andres data uden på forhånd opnået godkendelse,
- forsøge på at snyde eller modificere ressourcetildelinger, privilegier m.v.,
- bruge netværk og/eller dertil knyttede systemer til at opnå uautoriseret adgang til andre tilsluttede systemer,
- forsøge at dekryptere system- eller brugerpasswords,
- forsøge at kopiere normalt utilgængelige systemfiler,
- forsøge at bryde sikkerhedssystemer (hacking),
- indlægge edb-virus eller andre former for programmer, der kan afbryde eller ødelægge driften af såvel interne som eksterne systemer,
- påvirke fortroligheden af data,
- oprette dial-in adgang til IT-systemer via telefonnettet eller tilsvarende systemer uden forudgående godkendelse fra SDUs IT-sikkerhedsansvarlige organisation,
- oprette trådløse net med direkte adgang til SDUs net uden forudgående godkendelse fra SDUs IT-sikkerhedsansvarlige organisation,
- kopiere tredieparts materiale uden tilladelse fra ejeren eller uden legal licens,
- distribuere ulovligt programmel, film, musik m.v.,
- fortsætte med uhæmmet forbrug af systemressourcer, der generer andre legale brugere, efter at der er gjort opmærksom på forholdet,
- forsøge at standse IT-systemer eller ødelægge deres funktioner,
- foretage skanninger af netværk efter adresser, porte, services m.v.,

- downloade og/eller videresende musik- og videofiler med mindre dette har en undervisnings- og/eller forskningsmæssig begrundelse.

Validering: Kalkulation og kontrol af, at indrapporterede datas værdi eller et givet tegn eller ord er indeholdt i et forudbestemt gyldigt værdiinterval, fx er datoen den 30. gyldig for januar men ikke for februar måned.
Virus: En programkode, der er skjult og udfører handlinger, som brugeren ikke har tiltænkt. Handlingen har typisk en skadende eller ødelæggende virkning på data eller programmer. En virus laver kopier af sig selv og kan sprede sig selv til harddiske og netværk eller til andet udstyr via netværk og flytbare datalagringsmedier.
Åbent net: Et netværk, som er umiddelbart og offentligt tilgængeligt for alle, der har indgået en anvendelsesaftale, og som har det nødvendige udstyr, fx internet og telefonnettet.

3 Formål

Det er dette dokuments formål at:

- Udgøre et generelt grundlag for universitetets sikkerhedsmålsætning med henblik på udvikling, implementering, indførelse og effektiv styring af sikkerhedsmæssige kontroller, forholdsregler og sikringsforanstaltninger baseret på kravene i DS484:2005, Standard for informationssikkerhed.
- Være generel referenceramme for universitetets interne og eksterne brug af informationsteknologiske faciliteter.
- Skabe grundlag for tillid til universitetets informationsbehandling både internt og eksternt.
- Være referenceramme ved anskaffelse og kontrahering af informationsteknologiske produkter og tjenesteydelser.

Regler

4 Risikovurdering og -håndtering

Der skal være forståelse for de trusler, institutionen kan blive udsat for og for institutionens sårbarheder.

Overordnet risikovurdering

Som grundlag for ajourføring af SDU's tekniske og organisatoriske IT-sikkerhedsforanstaltninger foretager IT-sikkerhedsudvalget en gang årligt en overordnet risikovurdering.Vurderingen baseres blandt andet på:• Det generelle trusselsbillede, som det beskrives af sikkerhedseksperter i dags- og fagpressen, ved konferencer m.v.,• ny og ændret lovgivning, der medfører krav om sikkerhedsforanstaltninger,• SDU's kommunikationsbehov og særlige forhold som forsknings- og uddannelsesinstitution,• sikkerhedsmæssige hændelser på SDU i det forløbne år.Vurderingen skal også belyse sandsynligheden for at IT-aktiverne udsættes for trusler, omfattende tilfældige, forsætlige og uforsætlige hændelser som f.eks.:• Destruktion af informationer, data og andre faciliteter,• modifikation af informationer og data,• tyveri, fjernelse eller tab af informationer, data eller andre ressourcer,• uautoriseret afsløring af informationer og data,• afbrydelse af driftsafvikling og netværkskommunikation.Risikovurderingen skal foreligge indenfor den termin, der er angivet i SDU's ISMS og forelægges ledelsen, der træffer beslutning om eventuelle ændringer af sikkerhedspolitikken og andre sikkerhedstiltag.

Risikoanalyse

Der skal udarbejdes en detaljeret risikoanalyse for alle forretningskritiske systemer, dvs. systemer der er klassificeret i kategori A eller B.

Analysen skal belyse sandsynligheden for at IT-aktiverne udsættes for trusler, herunder tilfældige, forsætlige og uforsætlige hændelser som f.eks.:Destruktion af informationer, data og andre faciliteter,modifikation af informationer og data,tyveri, fjernelse eller tab af informationer, data eller andre ressourcer,uautoriseret afsløring af informationer og data,afbrydelse af driftsafvikling og netværkskommunikation.Risikoanalysen for hvert enkelt system består af en konsekvensvurdering, som foretages af systemejerne (repræsenterer de forretningsmæssige krav) og en sandsynlighedsvurdering, som foretages af de system- og driftsansvarlige.Analyserne samles i en risikorapport, som skal foreligge indenfor den termin, der er angivet i SDU's ISMS og forelægges ledelsen, der på baggrund af vurderingens anbefalinger træffer beslutning om eventuelle ændringer af systemkonfiguration, sikkerhedspolitik og andre sikkerhedstiltag. Ledelsen kan også beslutte at justere de forretningsmæssige forventninger til systemerne.

5 Overordnede retningslinier.

5.1 Informationssikkerhedsstrategi

5.1.1 Formulering af informationssikkerhedspolitik

Det overordnede ansvar for SDUs IT-sikkerhed er fastlagt i SDUs overordnede IT-sikkerhedspolitik.
Opnåelse af optimal sikkerhed afhænger primært af, at følgende forudsætninger er til stede:

- Ledelsen udviser et uforbeholdent engagement i IT-sikkerheden og medvirker til dens gennemførelse.
- Sikkerhedsmål og -aktiviteter er baseret på og i overensstemmelse med den vedtagne IT-sikkerhedspolitik.
- Der er forståelse for de trusler, institutionen kan blive udsat for og for institutionens sårbarheder.
- Medarbejdere og studerende er bekendt med reglerne for den interne IT-sikkerhed.
- Klare retningslinier for IT-sikkerhedspolitik og -standard fordeles til alle berørte persongrupper, herunder eksterne samarbejdspartnere, gæster m.fl..

I forbindelse med justering af sikkerhedspolitikken og sikkerhedsforanstaltningerne udarbejdes en handlingsplan for hvordan og hvornår ændringerne implementeres og hvorledes de forskellige aktiviteter prioriteres.

Offentliggørelse af IT-sikkerhedspolitik	IT-sikkerhedspolitikken skal offentliggøres og kommunikeres til alle relevante interessenter, herunder alle medarbejdere og studerende.
Godkendelse af IT-sikkerhedspolitik	IT-sikkerhedspolitikken skal hvert år godkendes af ledelsen.
Sprog for IT-sikkerhedspolitik	IT-sikkerhedspolitikken skal kun eksistere på dansk, som er hovedsproget i organisationen.
Omfang af IT-sikkerhedspolitik	Informationssikkerhed defineres som de samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet. Foranstaltninger inkluderer tekniske, proceduremæssige, lov- og regelmæssige kontroller.

5.1.2 Løbende vedligeholdelse

Ongoing maintenance of information security policy.

Revision af IT-sikkerhedspolitik	På basis af risikovurderingen og den overordnede IT-sikkerhedspolitik ajourføres nærværende beskrivelse af IT-sikkerhedsforanstaltningerne - om nødvendigt - årligt indenfor den termin, der er angivet i SDUs ISMS.
Vedligeholdelse af IT-sikkerhedspolitik	IT-sikkerhedskoordinatoren har ansvaret for at universitetets sikkerhedspolitikker, regler, procedurer og tilhørende dokumantation bliver vedligeholdt.

6 Organisering af informationssikkerhed

Placering af ansvar er vitalt for at sikre opmærksomhed på universitetets informationsaktiver. Organisationsstrukturen på universitetet og samarbejde med eksterne partnere er yderst vigtigt for at opretholde et tidssvarende sikkerhedsniveau. Kontrakter med partnere og andre aftaler er ligeledes et område der har indflydelse på informationssikkerheden.

6.1 Interne organisatoriske forhold

Ansvarsplacering, udmøntning af de generelle retningslinier i specifikke forretningsgange og instruktioner samt den løbende opfølgning pålægges IT-sikkerhedsudvalget og skal indgå i sikkerhedsimplementeringen. IT-sikkerhedsudvalget skal endvidere vurdere brud på sikkerheden, nye trusler og sårbarheder samt nye muligheder for sikringsforanstaltninger, samt påse, at disse informationer tilgår ledelsen og indgår i den løbende ajourføring af den overordnede risikovurdering.

Ledelsens rolle	Ledelsen skal støtte universitetets informationssikkerhed ved at udlægge klare retningslinier, udvise synligt engagement samt sikre en præcis placering af ansvar.
Koordination af informationssikkerheden	Sikkerhedsforanstaltninger planlægges og aftales med ledelsen på overordnet niveau i forbindelse med den årlige planlægning. Grundlaget for dette er et oplæg til det kommende års sikkerhedsarbejde fra IT-sikkerhedskoordinatoren og chefen for IT-service.Det tværorganisatoriske samarbejde foregår dels i IT-styringskomiteen, IT-koordinationsgruppen og IT-sikkerhedsudvalget.Regler og planer på sikkerhedsområdet drøftes i IT-koordinationsgruppen og IT-sikkerhedsudvalget.
Sikkerhedsorganisation	SDU's IT-sikkerhedsudvalg er universitetets forum for informationssikkerhed, der har ansvar for at sikre at strategien for informationssikkerhed er synlig, koordineret og i overensstemmelse med universitetets mål. IT-service's IT-sikkerhedsgruppe, herefter benævnt ITS-sikkerhedsgruppen, er Fællesadministrationens forum for informationssikkerhed og har ansvaret for den operationelle sikkerhed på de fælles IT-systemer.

Ansvarsplacering

Alle SDU's IT-aktiver skal have udpeget en sikkerhedsansvarlig. Der skal forefindes et ajourført register over institutionens kritiske fysiske IT-aktiver og deres sikkerhedsansvarlige. For flerbrugersystemer påhviler ansvaret for sikkerheden som hovedregel den person, der har ansvaret for de data, som systemet indeholder. Enhedschefen har ansvaret for at der udpeges en sikkerhedsansvarlig for hvert flerbrugersystem. For arbejdsstationer gælder som hovedregel, at den registrerede bruger er ansvarlig for sikkerheden af disse systemer.

For hver enkelt IT-system skal der defineres de flg. profiler, som dog godt kan være den samme person:Dataejeren, som er ejer af de data, der findes på systemet og dermed bestemmer hvordan data må tilgås og af hvilke brugere. F.eks. er Stads-kontoret ejer af STADS systemet.Systemejeren, som enten benytter eller er leder af den afdeling, der benytter systemet. Det vil typisk være systemejeren, der skal foretage konsekvensvurderingen i forbindelse med systemets årlige risikovurdering.Den IT-sikkerhedsansvarlige, som har ansvaret for systemets data og de applikationer, der håndterer disse data.Den IT-systemansvarlige, som har ansvaret for installation og konfiguration af systemet.Den IT-driftsansvarlige, som har ansvaret for den daglige drift af systemet.For hver enkelt system udarbejder og vedligeholder den IT-systemansvarlige et IT-stamblad for alle IT-systemer der ejes og/eller administreres af IT-service. IT-stambladet indeholder blandt andet en klassificering af systemet.

Fagligt samarbejde med grupper og organisationer

IT-sikkerhedsudvalget har ansvaret for at holde sig orienteret om den generelle udvikling på IT-sikkerhedsområdet og for at videregive relevant information inden for SDU. IT-sikkerhedsudvalget kan til dette formål oprette personlige og faglige kontakter til andre organisationer, men må i den forbindelse ikke viderebringe oplysninger om sikringsforhold og andet, der kan misbruges til angreb på SDU's IT-sikkerhed.

Periodisk opfølgning

IT-sikkerhedsudvalget har ansvaret for at igangsætte og koordinere følgende aktiviteter:Ajourføring af den overordnede risikovurdering: Årligt, skal være afsluttet indenfor den termin, der er angivet i SDUs ISMS.Ajourføring af nærværende beskrivelse af IT-sikkerhedsforanstaltninger: Årligt, skal være afsluttet indenfor den termin, der er angivet i SDUs ISMS.Forslag til ajourføring af sikkerhedspolitik: Årligt, skal være afsluttet indenfor den termin, der er angivet i SDUs ISMS.Adhoc forslag til ajourføring af IT-sikkerhedspolitikken efter behov, hvis eksterne hændelser eller krav giver anledning til dette.IT-sikkerhedsarbejdet i SDUs forskellige fakulteter, institutter m.v. indgår i den årlige planlægning og opfølgning på lige fod med andre sikkerhedsaktiviteter.

Kontakt med relevante myndigheder

Ved brud på sikkerheden skal der være etableret en procedure for håndtering af bevismateriale og eventuelt kontakt med relevante myndigheder.

Forsikring mod hændelser

SDU er en statslig selvejende institution som er selvforsikret.

Fortrolighedserklæring ved ansættelse	Alle it-medarbejdere skal senest ved ansættelsestidspunktet gøres opmærksom på at Straffelovens §152 gælder under ansættelsen og efter ansættelsesforholdets ophør.

6.2 Eksterne samarbejdspartnere

SDU vil i fornødent omfang benytte ekstern assistance.

Fortrolighedserklæring for tredjepart	I de tilfælde, hvor der benyttes ekstern assistance og hvor rådgiveren formodes at få adgang til interne informationer, indgås formel aftale indeholdende en fortrolighedserklæring.
Sikkerhed ved samarbejde med tredjepart	Eksternt service- og rådgivningspersonale pålægges tavshedspligt i henhold til den underskrevne fortrolighedserklæring. Eksternt personales fysiske tilstedeværelse i maskinstuer, serverrum, netrum og lignende, hvor der forefindes systemer i klasse A, skal være overvåget af en ansat IT-medarbejder, med mindre, der er etableret andre særlige sikkerhedsregler, f.eks. video overvågning. Der kan dog dispenseres fra dette krav for eksternt personale med særlig tilknytning til SDU. IT-aktiver, der indeholder fortrolige data må ikke flyttes ud af SDU's bygninger, med mindre dataene er sikret mod uvedkommendes aflæsning. Såfremt eksternt servicepersonale får tilladelse til at medtage sådant udstyr til reparation, skal der udstedes en kvittering for udleveringen og afgives en fortrolighedserklæring. Ved bortskaffelse af brugte PC'er til grøn IT, skal servicepartneren skriftligt dokumentere at harddiskene er renset vha. godkendt slettesoftware.
Sikkerhed ved samarbejde med partnere	Det kan udgøre en risiko at give en samarbejdspartners medarbejdere adgang til interne faciliteter og informationer, blandt andet fordi samarbejdspartnerens styring af sikkerhed kan være utilstrækkelig. Samarbejdspartneren skal skriftligt tilkendegive at vedkommendes IT-sikkerhed er tilstrækkelig, evt. i form af en RS3411 revisionsrapport.Kontrakten skal færdigbehandles og underskrives før det tekniske og kontrolmæssige indhold implementeres. Enhedens IT-sikkerhedsansvarlige har ansvaret for at IT-sikkerhedsrelaterede emner bliver behandlet og inkluderet når kontrakten udarbejdes.
Samarbejdsaftaler	For at sikre at universitetets sikkerhedsmålsætning ikke kompromitteres skal ethvert formaliseret eksternt samarbejde være baseret på en samarbejdsaftale. Denne samarbejdsaftale skal leve op til de krav, der er beskrevet i ”Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning”, i daglig tale kaldet sikkerhedsbekendtgørelsen.

Aftaler om informationsudveksling

Inden datakommunikationsforbindelse etableres til en samarbejdspartners IT-systemer, skal der udføres en risikovurdering. Den skal mindst omfattehvilke typer data der skal gives adgang til,nødvendige sikringsforanstaltninger,hvilke personalegrupper, der skal gives adgang til og privilegier til data.Inden der åbnes for adgang til SDUs IT-aktiver, skal der i hvert enkelt tilfælde udarbejdes en skriftlig aftale, der pålægger samarbejdspartneren at overholde SDUs IT-sikkerhedsregler.I tilfælde hvor en konsulent eller lignende via fjernadgang skal udføre systemarbejde skal vedkommende underskrive en fortrolighedsaftale inden adgangen åbnes.

Der skal indgås skriftlig aftale om al rutinemæssig dataudveksling, dvs. udveksling af indkøbsordrer, fakturaer, betalingsordrer o.s.v., med eksterne partnere. Sikringsforanstaltningerne skal afstemmes med karakteren af de udvekslede data, herunder brug af vpn, ftp, kryptering mv.

Gæstekonti

SDU tillader fremmede (d.v.s. personer, der ikke har nogen formel tilknytning til SDU) at få adgang til netværket, når deres behov er relevant for SDU's virke.

Gæstekonti er personlige. Den enkelte bruger skal identificeres på tilfredsstillende måde inden udlevering af gæstekonti.

Såfremt en person får udleveret et antal gæstekonti til fordeling blandt nogle brugere, skal denne person som minimum identificeres med billedlegitimation.

Gæstekonti skal have en løbetid på maximalt 1 måned og skal derefter automatisk nedlægges/spærres.

Gæstekonti udleveres af enten Konferencesekretariatet, IT-service eller andre funktioner, som IT-sikkerhedskoordinatoren har givet tilladelse dertil.

Gæste udstyr

Der kan være specielle situationer hvor gæster som f.eks. gæsteforskere kan få deres maskiner på SDU's interne netværk. For at dette er tilladt skal enhedens it-sikkerhedsansvarlige give tilladelse, og maskinen skal efterses for vira, at den bliver holdt automatisk opdateret, og at der er installeret antivirus software, som bliver vedligeholdt automatisk. Derudover skal maskinnavnet og MAC-adressen registreres.

Outsourcing

Outsourcing

Ved outsourcing af it-systemer skal enhedens IT-sikkerhedsansvarlige inden indgåelse af kontrakt indhente information om sikkerhedsniveau fra outsourcingpartner og godkende at universitetets sikkerhed samlet set ikke forringes af outsourcing.

Outsourcing-partnere

Inden indgåelse af aftaler, skal sikkerhedsniveauet ved partneren afklares og sammenlignes med de krav der stilles i sikkerhedspolitikken. Outsourcing-partneren skal skriftligt tilkendegive at vedkommendes IT-sikkerhed er tilstrækkelig, evt. i form af en RS3411 revisionsrapport.

Ekstern revision af outsourcing-partnere	Outsourcing-partnere skal sørge for ekstern revision mindst en gang om året.

7 Styring af informationsrelaterede 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.

7.1 Identifikation af og ansvar for informationsrelaterede aktiver

7.1.1 Fortegnelse over informationsaktiver

IT-aktiver skal identificeres. Der skal for alle SDUs kritiske IT-aktiver udpeges en ansvarlig ejer.

Når omfanget af sikringsforanstaltninger for IT-aktiverne er fastlagt, besluttes det, hvordan sikringsforanstaltningerne administreres og hvordan beskyttelsen revurderes og justeres i overensstemmelse med løbende ændringer.

Registrering af it-udstyr	SDU's kritiske fysiske IT-aktiver skal identificeres og klassificeres. Der skal træffes foranstaltninger til sikring af disse aktiver i henhold til deres klassifikation. Ejer af aktivet har ansvar for implementering af sikringsforanstaltningerne.Der skal udarbejdes opgørelser over hvert enkelt IT-systems væsentligste IT-aktiver, både fysiske aktiver, programaktiver og informationsaktiver.Det skal dokumenteres, hvilke sikringsforanstaltninger der skal beskytte IT-aktiverne, hvilke regler ejeren og andre skal følge, for at sikringen er effektiv, og hvorledes der følges op med kontrolforanstaltninger.Det skal dokumenteres, hvorledes sikringsforanstaltningerne implementeres, revurderes og vedligeholdes. Tab af programmer og data i forbindelse med tyveri, hærværk, teknisk sammenbrud eller anden ødelæggelse af IT-udstyret skal modvirkes ved sikkerhedskopiering. Sikkerhedskopier skal opbevares adskilt fra det udstyr, der sikres. Ved konkret vurdering i hvert enkelt tilfælde kan der udføres supplerende sikringsforanstaltninger mod uautoriseret fjernelse f.eks. mekanisk- og/eller elektronisk tyverisikring. Udstyr skal afmeldes i henhold til bestemmelserne i: "Internt cirkulære vedr. registrering og udskiftning / afhændelse af apparatur m.m.".
Arbejdspladsudstyr	Alt udstyr over et vist minimumsbeløb, herunder IT-udstyr, der anskaffes af SDU, bliver registreret i Apparaturregistret. Hovedformålet med denne registrering er at kunne udføre beholdningskontrol, jfr. "Internt cirkulære vedr. registrering og udskiftning / afhændelse af apparatur m.m." i regelsamlingen. I forbindelse hermed registreres brugeren, der har ansvaret for udstyret.

7.1.2 Ejere af systemer og data

Sikkerhedsansvar for informationsaktiver

Enhedens IT-sikkerhedsansvarlige har ansvar for at der bliver udarbejdet og vedligeholdt af en liste over enhedens informationssystemer. Listen angiver henholdsvis dataejer, systemejer, den IT-sikkerhedsansvarlige, den IT-systemansvarlige og den IT-driftsansvarlige for hvert enkelt system.

Ansvar for sikkerheden på it-platforme

For alle IT-systemer, der er klassificeret som enten A eller B systemer, udarbejdes endvidere det i afsnit 6.1 omtalte IT-stamblad. Registreringen af systemerne i IT-stambladet skal omfatte de data, der er nødvendige for den daglige drift, sikkerhedsklassificering og -opsætning, service, reparation samt genetablering af systemerne efter alvorlige fejl og/eller situationer, hvor IT-systemer skal nyanskaffes.

Den IT-systemansvarlige for hver enkelt system skal sikre, at IT-stambladet holdes ajour og at sikkerhedsforanstaltningerne løbende holdes opdateret. For klasse A systemer udskrives der en papirkopi af IT-stambladet efter hver ændring af IT-stambladet. Disse papirkopier opbevares fysisk adskilt fra systemerne. Den IT-sikkerhedsansvarlige for hver enkelt system skal godkende opgraderinger og konfigurationsændringer på systemet, mens den IT-systemansvarlige skal sikre at de udføres.

Ejere af data på mobile enheder

Brugere af universitetets bærbare pc'er og andre mobile dataenheder er ansvarlige for at beskytte de data der behandles på disse, samt enhederne selv.

Ansvar for adgangsrettigheder

Enhedschefen har ansvaret for at den enkelte medarbejder tildeles netop de brugerprivilegier, som medarbejderens stilling og arbejdsopgaver berettiger til. Proceduren for tildeling af rettigheder afhænger af klassificeringen af det enkelte IT-aktiv. Den ansvarlige for aktivet fastsætter regler for tildeling af privilegier.

Administration af internet-domænenavne

Ansvaret for registrering af domænenavne ligger hos enhedens IT-chef, eller en af IT-chefen udpeget funktion.

7.1.3 Adfærdsregler

Adfærdsregler for brug af SDUs IT-udstyr

SDU har generelt den holdning, at universitetets IT-udstyr skal anvendes så meget som muligt, men indenfor visse rammer. Dette betyder, at SDUs medarbejdere må have en professionel holdning til brugen af IT og det udleverede udstyr, hvilket bl.a. indebærer at:Udstyret behandles på en forsvarlig måde, så der så vidt muligt ikke opstår hardwarefejl pga. håndteringen.Der ikke ændres på udstyrets sikkerhedsmæssige opsætning, medmindre dette er aftalt, f.eks. i forbindelse med programudvikling.Der ikke installeres nogen form for programmel på udstyret af brugeren, medmindre dette er aftalt, f.eks. i forbindelse med programudvikling.Udover ovenstående henvises til reglerne i afsnit 10, "Styring af netværk og drift".

Adfærdsregler for brug af internet

Adgang til surfing på internet	Retningslinier for brug af Internettet er angivet i Personalepolitiske retningslinier.
Medarbejderes private brug af internetadgang	Universitetets internetadgang må også anvendes til privat formål, såfremt sikkerhedspolitikken i øvrigt overholdes, og såfremt arbejdsrelateret brug ikke generes på nogen måde.
Sikkerhedsindstillinger i web-browser	Når der besøges web-sites på internettet, skal browserens sikkerhedsindstillinger reflektere, at Internettet pr. definition er usikkert. Dette gælder uanset hvilken browser der anvendes. Brugerne må ikke forsøge at omgå eller bryde sikringsforanstaltningerne.
Afvikling af programmer i forbindelse med Internetsurfing	Det er tilladt at afvikle browserbaserede programmer forudsat at disse er digitalt signerede, således at programleverandøren tydeligt fremgår.
Brug af messenger-programmer	Det er tilladt at bruge messenger-programmer på netværket.
Download af filer fra internet	Der må ikke hentes filer fra internet, med mindre de specifikt scannes for virus umiddelbart efter nedhentning og inden de åbnes.
Terminalsessioner til fjernstyring	Det er tilladt at benytte krypterede sessioner, for eksempel Secure Shell (SSH).

Adfærdsregler for brug af e-mail

Ejerskab	SDU betragter alle e-mails som universitetets ejendom.
Medarbejderes private brug af e-mail	Universitetet tillader brug af e-mail-systemer også til privat brug, såfremt sikkerhedspolitikken i øvrigt overholdes. Reglerne for medarbejdernes private brug af universitetets e-mail system er beskrevet i "Personalepolitiske retningslinier".
Vedhæftede filer	Det tilrådes at medarbejderne udviser forsigtighed med vedhæftede filer og ikke ukritisk åbner disse.
Fortrolig mail	Ved afsendelse af E-mails med følsomt indhold skal reglerne i dokumentet "Sikkerhedsklassificering af data på SDU" overholdes. Hvis e-mail bruges til bindende aftaler skal de underskrives med en digital signatur.

Elektronisk udveksling af post og dokumenter

Al e-mail skal indeholde tydelig identificerbar afsender.

Medarbejderne skal udvise forsigtighed med deres brugeridentitet i forbindelse med videregivelse af eksempelvis mailadresser, samt i forbindelse med modtagelsen af uønskede e-mails.

Brugere af e-mail gøres opmærksom på, at e-mail lagres under forsendelse fra afsender til modtager på forskellige servere.

Der accepteres en maksimal e-mail størrelse på 20Mb incl. vedhæftede filer. Dette gælder både ind- og udgående e-mail.

E-mailens kuvert (headeren), men ikke indholdet, registreres af transmissionssystemerne af hensyn til efterspring af e-mail, fejlanalyse m.v.

E-mail kan endvidere af sikkerhedsårsager blive sikkerhedskopieret både under vejs i forsendelsen og på den server, hvorfra brugeren henter sin e-mail.

Automatisk viderestilling af mails må ikke ske, hvis der kan opstå risiko for at de videresendte informationer kan skade SDU. Det vil bl.a. sige, at der skal udvises agtpågivenhed om, hvor information sendes hen, og det skal sikres, at information ikke går SDU af hænde.

Det er ikke tilladt at foretage masseudsendelse af mails. Hvis en studerende har et studierelevant behov for dette, kontaktes Helpdesk, som i samarbejde med enhedens IT-sikkerhedsansvarlige vil vurdere anmodningen og evt. forestå masseudsendelsen.

Systemadministratorer og netværksansvarlige kan i tilfælde af driftsproblemer og sikkerhedshændelser have behov for at læse brugernes E-mails. For at undgå at private E-mails i disse tilfælde bliver læst, skal de tydeligt markeres med ordet: "privat" i emnefeltet.

Systemadministratorer og netværksansvarlige har adgang til mailsystemets registre, servere og sikkerhedskopier.

Systemadministratorer og netværksansvarlige har tavshedspligt, så længe der ikke konstateres misbrug.

Opbevaring og sletning af e-post

E-mail der indeholder personhenførbare oplysninger, skal behandles i overensstemmelse med persondataloven.

Adfærdsregler for trådløse netværk

Installation af trådløst udstyr

Det er ikke tilladt at installere eller ibrugtage uautoriserede "access-punkter", dvs. udstyr der giver trådløs netadgang på SDU's netværk.

IT-service har ansvaret for netværket og skal derfor forhåndsgodkende evt. dispensationer fra ovenstående, f.eks. til forskningsbrug. Et sådant trådløst net må under ingen omstændigheder konflikte med driften af det normale trådløse net.

SDUs brugere skal være opmærksomme på, at SDUs trådløse netværk er ukrypteret og derfor undgå at sende fortrolig information over dette.

Forbindelse til fremmede trådløse netværk

SDUs brugere må forbinde deres mobile udstyr til fremmede trådløse netværk, forudsat at godkendt firewall er i brug.

7.2 Klassifikation af informationer og data

7.2.1 Klassifikation

Klassifikation af IT-systemer

Systemerne klassificeres efter det hovedprincip, at det er systemets data som afgør systemets klassifikation. Dette sker ved at data tildeles en score for konsekvenserne af brud på hvert af de tre områder fortrolighed, integritet og tilgængelighed. Denne score lægges sammen og summen angiver systemet kritikalitet og dermed også dets klassificering. Scorekortet kan for hvert af områderne tildeles de følgende værdier:Store konsekvenser giver en værdi på 4.Middelstore konsekvenser giver en værdi på 2.Små eller ingen konsekvenser giver en værdi på 1.Systemerne kategoriseres på baggrund af deres score i de følgende klasser:Klasse A: systemer som er forretningskritiske for hele SDU har en score på 7 og derover.Klasse B: systemer som er forretningskritiske for en af SDUs enheder har en score på 5 eller 6.Klasse C: Mindre væsentlige systemer har en score på 4 eller derunder.De organisatoriske enheders IT-afdelinger træffer afgørelse om klassifikationen, dog kan systemejeren altid hæve klassifikationen et niveau, forudsat at dette godkendes af enhedens IT-sikkerhedsansvarlige. Alle klasse A og B IT-systemer skal efterfølgende gennemgå en risikovurdering.

Klassifikationsmærkning

SDU's informationer og data klassificeres i henhold til "Lov om offentlighed i forvaltningen" samt til SDU's Journalvejledning, som beskrevet i dokumentet "Sikkerhedsklassificering af data på SDU".

Informationer og data skal klassificeres som følger:

I relation til nærværende forskrift kan SDU's informationer klassificeres i følgende grupper:Offentlige informationer, d.v.s. informationer der er underlagt bestemmelserne om offentlighed i forvaltningen.Interne informationer som f.eks. arbejdspapirer m.v.Følsomme forskningsdata, som generelt omhandler forskningsdata, hvor dataejeren sammen med enhedens IT-sikkerhedsansvarlige afgør hvorledes informationerne skal håndteres.Fortrolige informationer, herunder følsomme personoplysninger, samarbejdspartneres forhold, oplysninger i relation til patenter m.v.

7.2.2 Håndtering af informationer

Procedurer for informationsudveksling

De retningslinier og procedurer, der definerer hvorledes SDUs data skal håndteres, er beskrevet i dokumentet "Sikkerhedsklassificering af data på SDU".

Social Engineering

Medarbejdere skal når de behandler fortrolige informationer være passende opmærksomme på begrebet "social engineering" eller "kunsten at aflure fortrolige informationer uden at blive opdaget". For eksempel kan denne form for bedrag udføres via e-mail, telefon og/eller messenger-programmer.

8 Medarbejdersikkerhed

Menneskelige fejl samt misbrug, berigelse, bedrageri og lignende udgør generelt den største trussel mod IT-sikkerheden. Disse risici skal imødegås ved anvendelse af formålstjenlige procedurer ved ansættelse af personale inklusive vikarer, ved uddannelse i IT-sikkerhed, ved funktionsadskillelse og gennem regler for servicepersonales adgang til IT-aktiver. De personer, der færdes på SDU kan inddeles i 4 grupper (ansatte herunder vikarer, studerende, eksternt servicepersonale samt gæster). Alle disse persongrupper er pligtige til at overholde IT-sikkerhedsreglerne , men sanktionerne ved overtrædelse er forskellige for de enkelte grupper.

8.1 Sikkerhedsprocedure før ansættelse

Ansættelsesproceduren følger SDUs normale procedurer.

Fortrolighedserklæring ved ansættelse	Alle it-medarbejdere skal senest ved ansættelsestidspunktet gøres opmærksom på at Straffelovens §152 gælder under ansættelsen og efter ansættelsesforholdets ophør.
Baggrundscheck af medarbejdere	Den ansættende enhed skal tilse, at der sker forsvarligt baggrundscheck af medarbejdere med ansvar for forretningskritiske arbejdsområder. Personalekontoret bistår om nødvendigt den ansættende enhed med opgaven. Sikkerhedsgodkendelse i øvrigt af personale finder ikke sted.
Baggrundscheck af medarbejdere skal omfatte:	Identitetskontrol - Ansøgeren skal identificere sig ved hjælp af pas, kørekort eller anden fotolegitimation. Ansøgerens curriculum vitae - Eventuelle huller i ansøgerens curriculum vitae skal kunne forklares tilfredsstillende. Uddannelser og professionelle kvalifikationer - Eksamensbevisers ægthed og værdi skal verificeres.
Straffeattest	Ved ansættelse af systemadministratorer og andet personale, der ved arbejdet kan skaffe sig adgang til og overblik over SDU's data og/eller er i stand til at påvirke eller skade driften af SDU's IT-aktiver, bør det i hvert enkelt tilfælde overvejes, om der skal der indhentes straffeattest. Hvis der skal indhentes straffeattest, skal dette fremgå af stillingsopslaget.
Ansættelses aftalen skal indeholde og uddybe:	Fortrolighedserklæring. Medarbejderens ansvar i forbindelse med informationsbehandling. Ansvarsplacering når der arbejdes udenfor Universitetets egne områder eller udenfor normal arbejdstid, f.eks. i forbindelse med arbejde hjemmefra.
Ansvar for sikkerhed	IT-medarbejdere skal i forbindelse med deres ansættelse underskrive en erklæring om, at de er bekendt med og vil overholde nærværende retningslinier.

8.2 Ansættelsesforholdet

Ledelsens ansvar	Det er ledelsens 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 universitetets informationssikkerhedspolitik.Er motiverede til at leve op til universitetets informationssikkerhedspolitik og retningslinier.Opnår et opmærksomhedsniveau i spørgsmål vedrørende informationssikkerhed, der er i overensstemmelse med deres roller og ansvar på universitetet.

Uddannelse

Uddannelse i sikkerhedspolitikken	Alle nye medarbejdere modtager ved tiltrædelsen universitetets informationssikkerhedspolitik. Alle medarbejdere skal have træning i universitetets informationssikkerhedspolitik og baggrundsviden omkring denne. Alle it-brugere modtager løbende instruktioner i overholdelse af universitetets informationssikkerhedspolitik. Chefen for den ansættende enhed har ansvaret for at nyansatte medarbejdere ved oprettelsen som bruger instrueres i SDUs regler for IT-sikkerhed og konsekvenserne - for SDU og for medarbejderen - af brud på sikkerhedsreglerne.
Uddannelse i klassificering af informationer	De ansatte skal modtage instruktioner om, hvorledes data og dokumenter klassificeres.
Sikkerhedsuddannelse for it-medarbejdere	Alle it-medarbejdere skal specifikt uddannes i sikkerhedsaspekter for at minimere risikoen for sikkerhedshændelser. It-medarbejdere skal løbende gennemgå produktspecifik sikkerhedsuddannelse, for de it-produkter der er mest udbredte på Universitetet.

Sanktioner

Overtrædelse eller forsøg herpå af reglerne for IT-sikkerhed kan medføre disciplinære foranstaltninger. Disciplinære foranstaltninger iværksættes efter en samlet vurdering af overtrædelsens omfang og karakter. Der kan i visse tilfælde ligeledes blive tale om politianmeldelse og eventuelt erstatningskrav for forvoldt skade.

Ansatte	Overtrædelsen behandles i overensstemmelse med SDU's personalepolitiske retningslinier og almindelige ansættelsesretlige regler.Der kan blive tale om anvendelse af sanktionerne: Påtale, advarsel, afskedigelse og ved særlig grov pligtforsømmelse bortvisning.Personalekontoret skal altid konsulteres inden der tages stilling til de disciplinære foranstaltninger. Der henvises i øvrigt til punkt 4.4. i de personalepolitiske retningslinier, der findes på personalekontorets hjemmeside.

Studerende, eksternt servicepersonale og gæster	Overtrædelsen kan medføre anvendelse af sanktionerne: Mundtlig påtale, skriftlig advarsel, inddragelse af brugerrettigheder i kortere eller længere perioder, hel eller delvis bortvisning fra SDU. Beslutning om sanktioner træffes normalt af den lokale IT-ansvarlige. For studerendes vedkommende dog efter konsultation med rektor. Der henvises til "Regler om disciplinære foranstaltninger overfor studerende ved Syddansk Universitet". Beslutning om bortvisning fra SDU træffes dog af rektor efter indhentet udtalelse fra ovennævnte.

8.3 Ansættelsens ophør

Returnering af aktiver ved aftrædelse	Medarbejderen skal aflevere alle udleverede virksomhedsaktiver ved samarbejdets ophør.
Inddragelse af privilegier ved fratrædelse	Der skal forefindes en opdateret procedure for inddragelse af privilegier i forbindelse med fratræden eller afskedigelse af personale. Proceduren for inddragelse af privilegier skal indeholde en liste over funktioner og personer der skal informeres i forbindelse med fratrædelsen. Enhedschefen træffer beslutning om, hvornår fratrådte medarbejdere skal udelukkes fra - fysisk og logisk - at anvende SDU's IT-aktiver. Udelukkelsen skal dog ske indenfor maksimalt 3 måneder, medmindre medarbejderen stadig har arbejdsopgaver for SDU. Udelukkelsen sker vha. den "blå blanket". Når en systemadministrator eller lignende fratræder, skal der omgående skiftes kodeord på alle systemer, som den pågældende havde adgang til.
Fortrolighedserklæring ved fratrædelse	Ved fratrædelse skal der gøres opmærksom på gældende fortrolighedsaftaler.

9 Fysisk sikkerhed

Fysisk sikkerhed og adgangsregler er naturlige elementer i universitetets sikkerhedspolitik. Fysisk sikkerhed omfatter blandt andet døre, vinduer, alarmer - samt tyverisikring af universitetetets 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 private og særligt sikrede områder.

9.1 Sikre områder

Det skal vurderes, hvordan en bygning og dens omgivelser hensigtsmæssigt kan opdeles i sikkerhedsområder i relation til IT-funktionernes forskellige sårbarhed. Indretning og placering af IT-funktioner skal tilrettelægges således, at de forskellige personalekategorier kan færdes i bygningen, uden at de sikringsmæssige regler tilsidesættes. Med udgangspunkt i en lokaleregistrering kan bygningen inddeles i sikkerhedsområder. Et sikkerhedsområde kan yderligere inddeles i separate, funktionsadskilte celler (lokaler). Inddelingen har betydning for sikkerhedsplanlægningen. Vurderingen skal dokumenteres i form af en plan over, hvordan IT-anlæg, -udstyr, -installationer og -funktioner samles eller separeres i en eller flere celler inden for et defineret sikkerhedsområde. Det skal forhindres, at den normale IT-driftsafvikling sættes ud af spillet ved bevist eller utilsigtet indgreb eller uheld.

Offentlige områder	SDU's bygninger er som undervisningsinstitution åbne og tilgængelige uden kontrol i en stor del af døgnet.Bygningerne må derfor, i relation til standarden DS 484:2005, betragtes som halvprivat sikkerhedsområde d.v.s. "at det kun i begrænset omfang er muligt at kontrollere personers adgang".Bygningsskallen er i princippet aflåst i tidsrummet hverdage kl. 20:00 - 07:00 samt i week-end, helligdage, men som følge af forskellige retningslinier på SDU's lokationer, arrangementer om aftenen og i week-ends må bygningsskallen generelt betragtes som ikke aflåst i relation til nærværende sikkerhedsforskrift.Når bygningerne er aflåst, foregår adgang for autoriserede brugere enten via ADK-systemet eller med nøgle.
Adgang til serverrum og hovedkrydsfelter	Placering af de administrative IT-systemer og netværkskomponenter er vist i bilag A1. Telefonhovedcentraludstyr er placeret i Odense på Campus. Derudover findes telefonundercentraler på SDU's større lokationer, jfr. bilag A1. Adgang til serverrum og hovedkrydsfelter tillades kun autoriserede IT-medarbejdere, eller ved overvåget adgang af IT-medarbejdere. Bygningsskallen med tilhørende adgangsåbninger omkring lokaler, hvor der foregår IT-driftsafvikling, skal sikres i henhold til klassifikationen i bilag A2.
Adgang til maskinstuer og it-klargøringsrum	Adgangen beskyttes med kodelås, der styres af ADK-systemet med individuelle koder for de enkelte medarbejdere. Sikre områder skal placeres så gennemgang gennem et højere klassificeret rum ikke er nødvendig for at nå til et mindre klassificeret rum. IT-chefen er ansvarlig for godkendelse af personale der har adgang til sikre områder. Private og særlige sikkerhedsområder (klasse A og B) skal med adgangskontrol eller overvågning beskyttes mod uautoriserede personers tilstedeværelse. Risikoen fra de trusler, IT-systemer og -aktiver kan blive udsat for, skal minimeres ved hjælp af sektionering og strategisk placerede barrierer. IT-aktiver skal beskyttes mod risiko for ødelæggelse og forstyrrelser fra omgivelserne herunder i hvilket omfang barrierer og/eller sektionering kan minimere truslerne fra ild, røg, vandskade, støv, vibrationer, kemiske påvirkninger, forstyrrelser i infrastrukturen eller elektromagnetisk stråling. Fysiske barrierer etableres afhængig af IT-aktivernes værdi og klassifikation. Reserveanlæg, udstyr eller datamedier med sikkerhedskopier skal opbevares i sikker afstand fra hovedanlæg, adskilt med barrierer.
Aflåsning af hovedkrydsfelter og lignende teknikrum	Krydsfelter skal placeres i aflåste skabe eller i private eller særlige sikkerhedsområder.

Indbrudsalarmer	Universitetet skal anvende tilstrækkelige alarmsystemer i alle lokaler med IT-udstyr der indeholder fortrolige informationer.
Overvågning i sikre områder	IT-afdelingerne skal sikre, at arbejde i sikre områder så vidt muligt bliver overvåget.
Optageudstyr i sikre områder	Uautoriseret optageudstyr er ikke tilladt i sikre områder.
Oplysninger om sikre områder	Oplysninger om sikre områder og deres funktion skal alene gives ud fra et arbejdsbetinget behov.
Sikring af kontorer, lokaler og udstyr.	Vinduer i lokaliteter hvori der foregår IT-driftsafvikling, skal lukkes med lukkebeslag, når lokalerne forlades uden overvågning. Hvor en risikovurdering angiver det, skal sikringen af vinduer i de underste etager suppleres med mekanisk beskyttelse. Elektronisk overvågning er ikke en sikringsmetode, der kan stå alene, da den ikke i sig selv forhindrer indbrud og tyveri, men den registrerer, når en person uautoriseret er ved at skaffe sig adgang til et sikret område. Registreringen af indbrud skal udløse en reaktion, som er afstemt efter IT-aktivernes værdi og de foreliggende mekaniske sikringsforanstaltninger. Elektronisk overvågning kan opbygges af fire forskellige overvågningstyper:Skalovervågning,Rumovervågning,Fældeovervågning, Objekt- eller punktovervågning.SDUs elektroniske overvågning baseres generelt på skalovervågning og rumovervågning. Den elektroniske overvågning skal give alarm til (vagt)personale, der kan reagere på alarmen døgnet rundt.
Brug af personlige adgangskort	Personers adgang til og ophold i sikkerhedsområder ((halv)private, private og særlige) skal registreres og kontrolleres i henhold til reglerne i SDUs ISMS. Medarbejdere skal bære deres id-kort eller adgangskort synligt på Universitetets områder. Nøgle og/eller adgangskort skal udleveres mod kvittering og modtageren skal instrueres om at det kun er til eget personligt brug og at bortkomst af det udleverede straks skal meldes. Der skal ske en registrering af de personer, der får udleveret nøgle og/eller adgangskort. Personale, der fratræder, skal have deres adgangsmuligheder inddraget.
Miljømæssig sikring af serverrum	Serverrum, krydsfelter og tilsvarende områder skal på forsvarlig vis sikres mod miljømæssige hændelser som brand, vand, eksplosion og tilsvarende påvirkninger.

Aflåsning af lokaler og bygninger

Trods hensigtsmæssige fysiske sikringsforanstaltninger kan tab efter ulykker ikke helt undgås, men skadeomfanget kan reduceres ved fornuftig planlægning. Således skal IT-anlæg, IT-funktioner, installationer og udstyr til energiforsyning, telekommunikation og sikringsanlæg beskyttes mod sikkerhedstrusler og ulykker fra omgivelserne og mod uautoriseret adgang.

Nøgle- og låsesystemer skal være konstruerede så de yder beskyttelse mod uautoriseret adgang til lokaliteter med adgangsbegrænsning og systemerne skal overholde kravene i DS 471.

Ansvar for den fysiske adgangskontrol

IT-sikkerhedskoordinatoren har det overordnede ansvar for administration af den fysiske adgangskontrol, f.eks. nøgleadministration, til kontorer og it-områder, men opgaven er typisk uddelegeret til SDUs organisatoriske enheder. Dette er nærmere beskrevet i SDUs ISMS.

IT-sikkerhedskoordinatoren er ansvarlig for at kontrollere fysisk adgang til universitetets faciliteter. Dette ansvar delegeres til betroede medarbejdere i organisationen, f.eks. sikkerhedsvagter.

Gæster

Gæsters adgang

Gæster må færdes frit på universitetets offentlige områder.

Gæster må ikke få adgang til de sikre zoner, medmindre de er ledsaget af en autoriseret IT-medarbejder.

9.2 Beskyttelse af udstyr

Placering af udstyr

Udstyr skal placeres eller beskyttes så risikoen for skader og uautoriseret adgang minimeres.

Arbejdsstationer, der viser følsomme eller fortrolige data, bør opstilles således, at uvedkommendes mulighed for at aflæse skærmbilleder forhindres.

Der skal foretages regelmæssig manuel overvågning af alle tekniske anlæg, som har betydning for driften af IT-systemer.

Systemer søges fordelt på flere maskinstuer, således at et alvorligt uheld i et rum ikke standser al IT-aktivitet. Centralt netværksudstyr er i et vist omfang dubleret og fordelt i flere netrum.

Automatisk overvågning af maskinstuer skal etableres til registrering af forsyningssvigt så tidligt som muligt for at minimere generne på IT-udstyr.

Opsyn med mobile enheder

Mobile enheder, som f.eks. bærbare computere, PDAer og mobiltelefoner, må ikke efterlades uden opsyn i uaflåste rum.

Adgang til data på bærbare computere skal beskyttes med et login kodeord. Udstyr med klassificerede informationer skal anvende harddisk kryptering.

Sikring af kabler

Kabler og tilhørende udstyr til el-forsyning og datakommunikation skal så vidt muligt installeres som "skjult" installation, således de ikke er umiddelbart synlige og tilgængelige for uautoriserede personer uden anvendelse af stige eller værktøj.

Forbindelserne i krydsfelterne skal være tydeligt afmærkede, så fejlopkobling kan undgås eller let kan afsløres. Der skal forefindes en veldokumenteret topologisk beskrivelse over alle kabelforbindelser og krydsfelter.

Forsyningssikkerhed

Det skal sikres, at leverandørens krav til omgivelseskonditioner (temperatur, luftfugtighed, støvindhold m.v.) for IT-systemer overholdes. Om nødvendigt skal der installeres ventilations- og/eller køleanlæg.

SDU's datakommunikation såvel internt som eksternt skal så vidt det er muligt inden for økonomiske og tekniske rammer sikres mod bevidst ødelæggelse ved dubleret udstyr og linier, alternative føringsveje m.v.

Sikringer, afbrydere, omskiftere og lignende skal så vidt muligt placeres inden for det sikkerhedsområde de betjener. Alternativt skal uautoriseret tilgang forhindres ved aflåsning.

Stophaner til vandforsyning og afbrydere til el-forsyning skal være tilgængelige og kendte af autoriseret personale.

Tilslutning af IT-udstyr må ikke kunne afbrydes ved uheld i forbindelse med rengøring og trafik omkring udstyret.

Leverandørens krav til spændingskvalitet og jordforbindelse skal opfyldes.

IT-udstyr i klasse A og B skal el-forsynes fra egen gruppe.

Beskyttelse mod udstråling

Alt IT- og telekommunikationsudstyr skal være CE-mærket i det omfang, det kræves for at overholde gældende lovgivning.

Der er ikke truffet særlige forholdsregler mod elektromagnetisk aflytning.

Kameraer

Der må ikke fotograferes i universitetets særlige sikkerhedsområder uden tilladelse fra IT-chefen eller IT-driftschefen.

Fjernelse af udstyr fra Universitetet

Udstyr må kun fjernes fra Universitet, hvis der foreligger en underskrevet aftale.

Udstyr der indeholder fortrolige data, må kun fjernes efter behørig godkendelse fra pågældende dataejer.

Udlån af udstyr skal så vidt muligt være tidsbegrænset.

Sikring af udstyr uden for universitetets overvågning

Eksternt placeret IT-udstyr f.eks. hjemmeudstyr, transportable arbejdsstationer, PDA'er m.v., der anvendes til kommunikation med SDU's IT-systemer via datakommunikation skal sikkerhedsmæssigt behandles på samme måde, som hvis det var placeret på en af SDU's lokationer. Sikringsniveauet afhænger af det system, der kommunikeres med.

Sikker bortskaffelse eller genbrug af udstyr

Alt IT-udstyr, der indeholder lagermedier f.eks. fastmonterede harddiske i arbejdsstationer og servere, skal kontrolleres før fjernelse for at sikre, at alle følsomme og fortrolige data tillige med licenserede og egne brugerprogrammer er slettet. Der henvises endvidere til Lov om personoplysninger.

For beskadigede datamedier, der indeholder følsomme eller fortrolige data, skal dataejeren afgøre, hvorvidt datamediet skal destrueres totalt eller repareres.

Ved reparation af udstyr med datamedier indeholdende følsomme eller fortrolige data, skal der indhentes tavshedserklæring fra reparatøren.

Skal der ske reparation i udlandet af datamedier, der jfr. Lov om personoplysninger indeholder fortrolige eller følsomme data, skal Datatilsynet være orienteret, inden der foretages forsendelse ud af Danmark.

Kasserede (flytbare) datamedier skal destrueres under opsyn af en dertil betroet medarbejder.

Vedligeholdelse af udstyr og anlæg

IT-udstyr skal vedligeholdes for at sikre dets tilgængelighed og pålidelighed.

Udstyr, herunder både IT-udstyr, sikrings- og overvågningsudstyr, skal vedligeholdes i overensstemmelse med leverandørens forskrifter, serviceintervaller og specifikationer.

Reparation og servicering skal udføres af kvalificeret personale.

Vedligeholdelse af IT-udstyr sker ved:Komplette reserveenheder.Reservedele.Servicekontrakter med en reaktionstid, der afhænger af det enkelte IT-systems klassificering.Service telefon- og kontraktnumre skal være anført i det enkelte systems IT-stamblad.

Brandsikring

Serverrum skal sikres med veldimensioneret brandslukningsudstyr.

Serverrum må ikke benyttes som lager for brændbare materialer.

Farlige eller brandfarlige materialer skal lagres i sikker afstand fra sikre områder.

Gennembrydning mellem brandceller skal sikres med godkendt brandtætning.

SDU's bygninger er i overvejende grad forsynet med ABA-anlæg.

Hvor der er etableret ABA-anlæg, er den tilhørende varsling udført i henhold til forskrifterne.

Brandslukningsanlæg skal som minimum findes i form af håndslukningsanlæg, der placeres let tilgængeligt, så en begyndende brand hurtigt kan slukkes.Typen på håndslukkere (kulsyre, pulver, vand, inertgas) skal tilpasses slukningsformålet. Håndslukkere skal være godkendt og mærket i henhold til Dansk Standard.Slukningsudstyret skal kontrolleres regelmæssigt.Personalet skal informeres om udstyrets tilstedeværelse og instrueres i brugen af det.

SDU har ikke etableret lynbeskyttelse.

Tyverimærkning af it-udstyr	Alt IT-udstyr skal beskyttelsesmærkes med en permanent mærkning med SDU som ejer.
Køling	Serverrum skal sikres med veldimensionerede airconditionanlæg. Anlæggene skal vedligeholdes og serviceres, så de er funktionsduelige. Lokaler, hvor der er installeret ventilations- og/eller køleanlæg bør overvåges med alarmeringsanlæg der giver akustisk og visuelt signal ved konditioner, der ligger uden for grænseværdierne.
Nødstrømsanlæg	IT-udstyr i klasse A skal el-forsynes via nødstrømsanlæg (UPS). IT-udstyr i klasse B bør overvejes forsynet via nødstrømsanlæg.

10 Styring af netværk og drift

Vedligeholdelse og opdatering af it-systemer er nødvendigt 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 vedligehold 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. Driftsafvikling skal ske korrekt og kompetent og skal planlægges som al anden produktion. En række faktorer har indflydelse på omfanget af denne planlægning. Væsentlige faktorer er enhedens størrelse, dens organisation og det udstyr og de IT-systemer, den benytter. Andre faktorer er afhængigheden og sensitiviteten af de programmer og data, som benyttes til afvikling af de daglige opgaver og de indførte sikringsforanstaltninger.

10.1 Operationelle procedurer og ansvarsområder

Enhedschefen har ansvaret for at driftsafvikling på IT-systemer og netværk er styret og defineret. Styringen skal understøttes af driftinstruktioner og reaktionsprocedurer til imødegåelse af uønskede hændelser. Funktionsadskillelse skal gennemføres, så vidt det er hensigtsmæssigt og muligt, for at reducere risici på grund af skødesløshed eller overlagt misbrug. Der skal gennemføres rutinemæssige procedurer for sikkerhedskopiering af data samt drifts-, hændelses- og fejllogning. Hvor procedurerne foreskriver det, skal udstyr og lokale m.m. overvåges.

10.1.1 Driftsafvikling

Driftsafviklingsprocedurer	Det skal være aftalt, hvordan og hvornår driftsafvikling skal foregå. Driftsafviklingspersonalet skal instrueres og trænes i driftsafvikling af de enkelte IT-systemer og eventuelle tilsluttede netværk. Driftsafviklingspersonalet skal instrueres i, hvad der skal sikkerhedskopieres, hvor ofte det skal ske, hvor kopierne skal opbevares og for hvilken periode, samt hvilke genstarts- og reetableringsprocedurer der skal tages i anvendelse, hvis der opstår fejl i driftsafviklingen. Der skal forefindes driftsafviklingsprocedurer for alle klasse A IT-systemer, som drives af SDU.

Driftsansvar	De enkelte enheders IT-medarbejdere er ansvarlige for drift, administration og sikkerhed på netværket og de fælles IT-systemer. Herunder efterlevelsen af sikkerhedspolitikker, regler og procedurer.
Dokumentation	De enkelte enheders IT-medarbejdere skal sikre at alle systemer og IT-relaterede forretningsgange er dokumenterede.
Indkaldelse af medarbejdere i vagtordning og ekstra personale	For SDUs alle kritiske IT-systemer skal der forefindes retningslinier for tilkald af relevant personale i tilfælde af behov for ekstraordinær drift, sikkerheds hændelser og lignende.
Deaktivering af beskyttelsesmekanismer	Det er under ingen omstændigheder tilladt at deaktivere eller omgå universitetets beskyttelsesmekanismer, herunder anti-virus produkter.

10.1.2 Styring af ændringer

Retningslinier for ændringer	Der opstår jævnligt behov for at basisprogrammel til operativ- og netværkssystemer ændres f.eks. med opdatering til en ny udgave eller der er behov for at tilføje nye programmer eller systemer til støtte for driftsafvikling, netværk og brugersystemer. Når der sker sådanne ændringer skal det kontrolleres, at der ikke optræder nogen forringelse af IT-sikkerheden for de enkelte brugersystemer.For det enkelte driftsafviklingsanlæg skal der forefindes en opdateret fortegnelse (IT-stamblad) over:De operativsystemer og andre programmer, som driftsafviklingen anvender til styring og kontrol. Fortegnelsen kan indeholde en henvisning til de respektive leverandørers dokumentationer af programmer og de tilhørende dokumentationer af driftsinstrukser.de brugersystemer og netværk, som driftsanlægget styrer og kontrollerer, inklusive opdaterede henvisninger til de respektive driftsinstrukser. Information omkring udførte ændringer skal formidles til interessenter. Den IT-systemansvarlige, jf. afsnit 6.1 har ansvaret for at al basisprogrammel er afprøvet og godkendt inden det sættes i drift.Den IT-systemansvarlige, jf. afsnit 6.1 har ansvaret for at systemets IT-stamblad bliver ajourført.Ud fra IT-stambladene dannes en oversigt, der benyttes:Ved den IT-systemsansvarliges vurdering af CERT's og andre sikkerhedsorganisationers og leverandørers anbefalinger til sikkerhedsrettelser af det kørende basisprogrammel.Ved den IT-sikkerhedsansvarliges vurdering af CERT's og andre sikkerhedsorganisationers og leverandørers anbefalinger til sikkerhedsrettelser af de kørende applikationer.Enhver opgradering og sikkerhedsrettelse skal være aftalt mellem den IT-systemansvarlige og den IT-sikkerhedsansvarlige for at sikre at der ikke er evt. kompatibilitets problemer mellem nye versioner af basisprogrammel og applikationer.

Planlægning, test og godkendelse af ændringer	Ændringer skal planlægges og så vidt muligt afprøves inden de sættes i drift. Ændringernes konsekvenser skal vurderes inden drift. Ændringer skal igennem en formaliseret godkendelsesprocedure inden drift. Enhedschefen kan opstille krav til og kriterier for nye systemers godkendelse, inden de tages i brug. Der skal foretages formålstjenlig afprøvning, før nye systemer godkendes - og det gælder ikke blot nyt maskinel, men også nye operativsystemer, hjælpesystemer og brugersystemer.
Styring af ændringer hos serviceleverandøren	SDU skal sikre, at ændringsstyring af serviceleverandørens ydelser følger samme retningslinier som universitetets egne.
Ændringer i forretningskritiske systemer	Alle ændringer i forretningskritiske systemer udføres efter godkendt procedure. Alle procedurer skal indeholde en alternativ plan til reetablering af det forretningskritiske system. Vilkårene for aktivering af den alternative plan skal ligeledes fremgå af proceduren.
Sikring af serversystemer	Servere skal konfigureres i henhold til SDUs gældende sikkerheds standarder.
Sikring af arbejdsstationer inden ibrugtagning	Alle arbejdsstationer skal sikres inden brug. Minimum sikring inkluderer installation af seneste sikkerhedsrettelser for operativsystemet og anti-virus program. SDUs arbejdsstationer opdateres løbende vha. centralt administrationssoftware. Der tages ikke backup af arbejdsstationerne, men der tages daglige sikkerhedskopier af alle brugerdata, som er lagrede på universitetets etablerede filservere.
Softwareopdateringer generelt	SDUs IT-medarbejdere skal holde sig informeret om alle programrettelser til alle programmer, der anvendes på universitetet og snarest installere disse på alle de computere, som de har ansvaret for, når det vurderes at rettelserne har positiv indflydelse på den samlede sikkerhed.

10.1.3 Funktionsadskillelse

Funktionsadskillelse er en sikringsforanstaltning, hvis hovedprincip er, at den samme person ikke både må udføre og godkende en given operation eller funktion. Funktionsadskillelse implementeres efter vurdering af enhedens kritiske systemer eller hvis lovgivningen kræver det.

Adgang til produktionsdata	Systemadministratorers adgang til fortrolige oplysninger skal registreres.
Sikring af forretningskritiske systemer	Forretningskritiske systemer skal beskyttes ved hjælp af funktionsadskillelse, således at risikoen for misbrug af privilegier minimeres. Hvor funktionsadskillelse ikke er muligt, skal der implementeres kompenserende tiltag.

10.1.4 Adskillelse mellem udvikling, test og drift

Adskillelse af udvikling, test og drift

Kritiske systemers test-, ændrings- og udviklingsaktiviteter skal så vidt muligt adskilles fra driftsaktiviteter.

Til A klassificerede IT-systemer er der oprettet separate udviklings-/testmiljøer, hvor nyudviklede/nyanskaffede faciliteter samt fejlrettelser kan afprøves forinden overførsel eller installation på produktionsmiljøer. Systemer, hvor der ikke kan opsættes realistiske testmiljøer, skal afprøves indenfor de aftalte service-vinduer.

10.2 Ekstern serviceleverandør

Overvågning af serviceleverandøren

Risici ved brug af eksterne serviceleverandørers styring af driftsafvikling skal identificeres og sikkerhedsforanstaltninger skal aftales og fremgå af driftsservicekontrakten. Anvendelsen af ekstern databehandler skal ske med respekt for Persondatalovens retningslinier.

Sikkerhedsregler skal i hvert enkelt tilfælde aftales med eksterne serviceleverandører. Hvis de skal have adgang til systemerne, skal de underskrive SDU's godkendte fortrolighedsaftale.

10.3 Styring af driftsmiljøet

Sikkerhed i systemplanlægning

SDU's IT-systemer afvikles fortrinsvis på servere dedikeret til den enkelte applikation, evt. i form af en virtuel server.

Inden ibrugtagning skal driftsafviklingssystemer, netværk og brugersystemer afprøves. Testen skal godkendes af både systemets ejer og den IT-sikkerhedsansvarlige.

Ved anskaffelse af nye og ved større ændringer af kritiske systemer udarbejdes en kravspecifikation som grundlag for en evt. tilbudsgivning/udbudsforretning. Der etableres en projektorganisation for gennemførelsen af tilbud/udbudsforretningen, samt efterfølgende test, godkendelse og implementering. Systemer SDU har anskaffet i fællesskab med andre institutioner (f.eks. økonomi, løn og studieadministration) gennemføres styring, test og implementering i et samarbejde med disse institutioner. Ved systemændringer og -opdateringer sker afprøvning som hovedregel ved en grundig afprøvning af et testsystem med samme funktionalitet som produktionssystemet i henhold til kravene i systemets klassificering. Afprøvning sker i samarbejde mellem dataejer og den IT-sikkerhedsansvarlige. Produktionssystemerne ændres/opgraderes og afprøves med så få ulemper for brugerne som muligt.

Kapacitetsplanlægning	It-systemernes dimensionering skal afpasses efter kapacitetskrav. Belastning skal overvåges således, at opgradering og tilpasning kan finde sted løbende. Dette gælder især for virksomhedskritiske systemer. I forbindelse med den årlige planlægning vurderes kapacitetsbehov for netværk og maskinel. Reservekapacitet skal koordineres og kravene til reservekapacitet skal med fastlagte tidsrum revurderes.
Integration af informationssystemer	Hvis integration af informationssystemer resulterer i en forøget risiko så skal denne vurderes og godkendes af IT-sikkerhedsudvalget.

10.4 Skadevoldende programmer og mobil kode

IT-systemer er sårbare over for uautoriserede indgreb eller ændringer. Derfor skal de beskyttes mod indvirkninger fra ondsindede programmer (trojanske heste, orme, logiske bomber, virus) i daglig tale gående under fællesbetegnelsen vira. Beskyttelse mod vira hviler grundlæggende på brugernes opmærksomhed på sikkerheden. Det vil sige, at brugerne skal instrueres om at beskyttelse er den primære sikringsforanstaltning. Ejere af IT-aktiver skal være på vagt over for vira. Især skal behovet for sikringsforanstaltninger, som kan beskytte og opdage vira, overvejes. Flytbare datamedier af fremmed oprindelse skal - ligesom data modtaget via eksterne netværk - kontrolleres for virus, inden de anvendes på systemerne. Eneste undtagelse er data fra IT-systemer, der med sikkerhed vides at være fri for virus. Strategien er dels at forhindre vira i at komme i udbrud, dels at forhindre spredning af virusbefængte filer.
Virusbekæmpelsesplanen består af følgende elementer:

- Al elektronisk post til og fra SDU skal åbnes og skannes for virus og spam i SDUs centrale mailgateway eller lignende. Hvis et vedhæng er befængt, konfiskeres det og gemmes i et særligt karantæneområde, hvorfra det evt. kan desinficeres med henblik på udlevering af en brugbar rest.
- Alle arbejdsstationer og lokale servere har, hvor det er muligt, beskyttelsesprogrammel (antivirusprogrammel), der for arbejdsstationernes vedkommen giver en aktiv beskyttelse, idet alle filer automatisk skannes idet de åbnes og blokeres i tilfælde af fare for smitte. På såvel arbejdsstationer, som lokale servere kan foretages skanning af de permanente filer. Der findes et virusberedskab, der dagligt administrerer overvågningssystemet og analyserer alle alarmer fra virusbeskyttelsen.

Antivirus produkter på arbejdsstationer	Alt IT-udstyr, der er tilsluttet SDU's datanet skal, hvis det er muligt, have et aktivt og opdateret antivirusprogrammel installeret, dette gælder også udstyr der tilsluttes netværket via fjernopkobling f.eks. fra hjemmet.
Kontrol af antivirus på arbejdsstationer	Det skal løbende kontrolleres, at anti-virus er aktivt på arbejdsstationer og at signatur-filerne ikke er over én uge gamle.
Spyware	Installation af spyware søges undgået gennem:Begrænsninger i muligheder for softwareinstallation.Patch-management-processer. IT-service skal sikre at der regelmæssigt scannes for spyware på alle arbejdsstationer.
Adware	Adware beskyttelse baseres på medarbejder-"awareness", sikkerhedsindstillinger i internetbrowser, begrænsninger i brugeres muligheder for softwareinstallation samt brug af adware-scannere.

Anti-virus-produkter på servere	Der skal være installeret anti-virus beskyttelse på alle serversystemer, hvor dette er muligt.
Styring af anti-virus	IT-service skal kunne styre anti-virus på alle systemer fra en central lokation. Med styring menes tvungen opdatering, scanning og oprydning.

10.5 Sikkerhedskopiering

Der skal gennemføres rutinemæssige procedurer for sikkerhedskopiering af data samt drifts-, hændelses- og fejllogning. Hvor procedurerne foreskriver det, skal udstyr og lokale m.m. overvåges.
Der skal foretages en sikkerhedskopiering, som sikrer, at alle SDUs essentielle data og programmer samt parameteropsætninger, kan gendannes i tilfælde af fejl og uheld. Faciliteterne til sikkerhedskopiering skal være omfattet af de krav, der er anført i SDUs beredskabsplaner og de specifikke regler vedrørende sikkerhedskopiering for de enkelte systemer skal godkendes af ejerne.
Der skal instrueres om:

- Hvilke data og programmer der skal sikkerhedskopieres,
- hvor hyppigt der skal foretages sikkerhedskopiering af data og programmer, i hvor mange eksemplarer og på hvilke medier, hvor de skal placeres og hvor længe de enkelte sikkerhedskopier skal opbevares,
- hvordan de forskellige kopieringsmedier udvendigt mærkes med komplette oplysninger om det mediet indeholder eller med en entydig identifikation,
- at den backupansvarlige har ansvaret for, at sikkerhedskopierne opbevares betryggende.

Sikkerhedskopier skal gives samme fysiske beskyttelse, som er gældende for de IT-aktiver de sikrer.
Sikkerhedskopiens anvendelighed skal testes med jævne mellemrum.

Sikkerhedskopiering af data på serversystemer	IT-service er ansvarlig for sikker lagring og backup af data på serverudstyr For IT-systemer, hvor der stilles særlige myndighedskrav om opbevaring af data i længere tid, er der udarbejdet en udvidet backupprocedure.
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 proces-ændringer der kan påvirke backup rutiner.
Sikkerhedskopiering af data på andre systemer	På arbejdsstationer anbefales det af hensyn til datas sikkerhed, at brugerdata lagres på filservere i mapper for personlige eller fælles data i stedet for lokalt på arbejdsstationen. Hvis ejeren alligevel vælger at lagre data lokalt, er det dennes ansvar, at der forefindes sikkerhedskopi af disse data. På Udviklings- og testsystemer vurderes det i hvert enkelt tilfælde, om der skal gennemføres sikkerhedskopiering.
Opbevaring af sikkerhedskopier på ekstern lokation	Datamedier til reetablering af forretningskritiske systemer skal opbevares i sikker afstand fra backup-systemet. Reserveanlæg og -udstyr og datamedier med sikkerhedskopier skal opbevares i sikker afstand for at undgå skadevirkninger fra et uheld på det primære anlæg.

10.6 Netværkssikkerhed

IT-service har det overordnede ansvar for det totale netværk.
Lokalnetværkets driftsstabilitet skal sikres. Ethvert lokalnetværk skal planlægges omhyggeligt og dets funktionalitet skal kontrolleres løbende.
Netværkets tilgængelighed, ydeevne, oppetid og driftsstabilitet skal kontrolleres. Det skal vurderes om netværk - specielt de, der udbreder sig på tværs af organisatoriske grænser - skal have indbyggede kontroller, der overvåger deres driftstilstand.
De kabelinstallationer, noder og komponenter, som kontrolleres, skal registreres. Registreringen skal omfatte til- og afgang af aktiver, deres identitet, type, serienummer, beskrivelse, producent, primære bruger, installationslokation, vedligeholdelsesansvarlig og konfigurativ afhængighed med andre komponenter.
I forbindelse med den årlige budget- og aktivitetsplanlægning gøres status over belastningen af datanettet og nødvendige udbygninger budgetteres.

Sikring af netværk	SDUs datanet overvåges med et SNMP-baseret overvågningssystem. Der føres statistik over trafikken på datanettets hoveddele vha. et webbaseret program. Trafikken på SDU, dvs. data fra de centrale netværksenheder, logges i SDU's firewall.De indsamlede logs bruges bl. a. til:At afsløre detaljer i tilfælde af hacking eller andet misbrug mod SDU's IT-systemer eller netværk.At finde frem til en intern brugers identitet, når der bruges NAT adresser (Network Address Translation), f.eks. hvis en ekstern organisations netværk/systemer eller ophavsret er krænket via SDUs netværk.At løse driftsmæssige problemer med opkoblinger gennem firewall'en.
Adgang til aktive netværksstik	Adgang til aktive netværksstik skal kontrolleres. Det skal sikres at der ikke forefindes ubenyttede aktive netværksstik i offentligt tilgængelige rum som gange, kantine og lignende.
Installation af netværksudstyr	Det er ikke tilladt at installere netværksudstyr på SDU's netværk uden forudgående sikkerhedsgodkendelse af IT-service.
Tilslutning af udstyr til netværk	Generelt må kun IT-service koble udstyr på det interne netværk, men IT-service kan uddelegere retten til at opkoble udstyr.
Fjernstyring og administration	Værktøjer til fjernadministration tillades, men som hovedregel ikke til forretningskritiske systemer. Det vil sige at forretningskritiske systemer kun må administreres indefra universitetets lokaliteter, medmindre dette er godkendt af både systemejeren og enhedens IT-afdeling.
Beskyttelse af diagnose- og konfigurationsporte	Fysisk og logisk adgang til diagnose- og konfigurationsporte skal kontrolleres.

Opdeling af netværk	SDU's netværk er opdelt i et antal virtuelle netværk (VLAN), hvor al trafik mellem de enkelte VLAN's kontrolleres af den centrale firewall. Hver enhed på SDU administrerer sin egen del af netværket i form af et antal VLANs, der som hovedregel er opdelt i de følgende netværkszoner: Server, printer og bruger. Som minimum skal server-VLAN være adskilt fra bruger-VLAN.
Rutekontrol	IT-service skal begrænse rutning imellem forskellige netværkssegmenter således at kun nødvendig trafik videresendes. Opsætning af udstyr, der ruter trafik skal forhåndsgodkendes eller installeres af IT-service.
Kryptering af administrative netværksforbindelser	Forbindelser, der benyttes til it-administration, skal krypteres hvis de benytter offentlige eller usikre netværk, for eksempel internet.
Firewall-funktioner på servere	Alle servere med indbygget firewall funktionalitet skal benytte denne til at sikre, at der kun gives adgang til nødvendige services.
Personlige firewalls	Alle arbejdsstationer skal benytte firewalls.

Trådløse netværk

Trådløse lokalnet må kun etableres med forhåndsgodkendelse fra IT-service. I forbindelse med godkendelsen skal alle sikkerheds- og driftsmæssige aspekter overvejes og analyseres, herunder at nettet skal konfigureres således, at uautoriseret tilgang og aflytning ikke er muligt.

Brug af trådløse lokalnetværk	Brug af trådløse netværk tillades for alle med gyldigt brugernavn/kodeord. Der er etableret trådløst netværk på alle SDU's geografiske lokationer. Brugerne af de trådløse netværk er selv ansvarlige for beskyttelse af deres klienter, da de indbyggede sikkerhedsfaciliteter ikke er slået til på accesspunkterne. De interne systemer må kun tilgås fra det trådløse lokalnet via en krypteret tunnel (VPN). Trådløse netværk betragtes som usikre, ubeskyttede netværk.
Adgang til trådløse netværk for gæster	Gæster, hvis identitet er kendt, må få udleveret kodeord til gæstenettet og tilslutte eget udstyr til gæstenettet, forudsat at udstyret ikke generer andre systemer.
Gæsters brug af universitetets trådløse netværk	Netværket kan og må kun anvendes til internet-adgang, direkte adgang til interne systemer må kun ske med tilladelse fra IT-service via en krypteret forbindelse (VPN).

Forbindelser med andre netværk

Opkobling af et netværk til et andet netværk og forbindelsesvejene mellem netværk skal registreres og kontrolleres. Trafikken mellem Internettet og SDUs datanet kontrolleres af logiske filtre (Firewall). Adgangen udefra via porte i Firewallen skal begrænses mest muligt og i givet fald tildeles adgangsrettigheder via konkrete porte til specifikke medarbejdere/segmenter. Der må ikke uden særlig tilladelse fra IT-service tilsluttes kommunikationsudstyr (modemer osv.), som omgår SDUs Firewall. Dataforbindelser til supplerende arbejdsplads i hjemmet etableres via en Internetudbyder. Ved adgang til interne IT-ressourcer på SDUs datanet benyttes VPN. Det er enhedschefens ansvar, at der er et arbejdsmæssigt behov for medarbejderens adgang til SDUs datanet fra en supplerende arbejdsplads. Enhedschefen skal derfor godkende oprettelsen. Ved oprettelse af forbindelse til en supplerende arbejdsplads skal medarbejderen erindre de dermed forbundne sikkerhedsregler.

Indkommende netværksforbindelser	Der tillades kun etablering af forbindelser fra internet til sikkerhedsgodkendte servere - eksempelvis til e-mail- og web-servere.
Udgående netværksforbindelser	Der er ingen restriktioner på forbindelser der etableres fra det interne netværk til internet eller andre netværk.
Ansvar for internetforbindelser	Det overordnede ansvar for internetforbindelserne ligger hos IT-service. Netværksleverandørers (offentlige og private leverandører af netværk og teleforbindelser) sikringsforanstaltninger og risici i forbindelse med benyttelse af leverandørens serviceydelser skal analyseres.SDU benytter en række teleleverandører dels til interne forbindelser mellem byer og i byerne og dels til forbindelse til supplerende arbejdspladser i hjemmet (typisk: ADSL og fællesantennesystemer).
Adgang fra distancearbejdspladser	Der må kun gives adgang til sikkerhedsgodkendte systemer på internt netværk. Adgang gives kun for brugere, der er autentificerede med brugernavn og kodeord. Der skal anvendes krypteret forbindelse.

10.7 Databærende medier

Flytbare datamedier - f.eks. magnetbånd, disketter, CDer, diske - og print, skal beskyttes mod ødelæggelse, tyveri, forlæggelse og uautoriseret anvendelse.

Brug af datamedier	Al lokal håndtering af datamedier er dataejerens ansvar. I forbindelse med Klasse A flerbrugersystemer anvendes flytbare datamedier til sikkerhedskopiering og arkivering. Alle medier er mærkede og opbevares i båndarkiv ved maskinstuen og - for udvalgte medier - som kopi i aflåst brandskab i en anden brandzone. Arkivmedier håndteres af betroet personale.

Bortskaffelse og genbrug af medier	Før datamedier kan udleveres eller genanvendes i andre systemer, skal unødvendige data på genanvendelige datamedier enten slettes eller overskrives i henhold til deres klassifikation. Et datamedium, der indeholder data, der er klassificeret som "følsomme forskningsdata" og/eller "fortroligt", skal altid overskrives på en sådan måde, at data ikke kan genskabes. Datamedier, som ikke længere anvendes, skal slettes, overskrives eller makuleres for at forebygge kompromittering af data.
Beskyttelse af følsomme og fortrolige data på datamedier	Følsomme forskningsdata og fortrolige data skal beskyttes mod uautoriseret indseende og misbrug.Der skal foreligge procedurer, som sikrer beskyttelse af følsomme og fortrolige data såvel på flytbare arbejdsstationer som på dokumenter, disketter, magnetbånd, print, rapporter m.v..Der skal foreligge procedurer til sikring af, at følsomme og fortrolige data, som er lagret digitalt, beskyttes i henhold til deres klassifikation og personalet skal instrueres om korrekte procedurer ved håndtering af datamedier.De ovennævnte procedurer er beskrevet i dokumentet "Dataklassificering på SDU".
Opbevaring og registrering af datamedier	Dataejer skal sikre at medierne eller informationerne på mediet klassificeres, og at brugere er instrueret i at opbevare mediet i henhold til regler for klassifikationen.
Forretningsgang for beskyttelse af datamediers indhold	Forretningsgangen for beskyttelse af datamediers indhold skal omfatte:• Håndtering og mærkning.• Adgangsbegrænsning.• Log over tildelte autorisationer.• Fysiske krav til opbevaringssted.• Minimering af distribution.• Klar mærkning af alle kopier.
Virusscanning af mobile datamedier	Inden ibrugtagning skal brugeren scanne ethvert datamedie for virus, hvis det har været i brug på eksternt udstyr. Med datamedie menes for eksempel transportable hukommelsesenheder, transportable drev, cd'er, dvd'er, og disketter.
Beskyttelse af systemdokumentation	IT-afdelingerne skal opbevare systemdokumentation passende sikkert. Systemdokumentation kan indeholde fortrolige oplysninger, der beskriver et systems processer, procedurer, datastrukturer, autorisationsprocesser m.v. Adgangsrettigheder til systemdokumentation skal holdes på et minimum og godkendes af systemejer. Dokumentation skal beskyttes mod uautoriseret adgang og indseende.
Lagring og adgangsrettigheder til systemdokumentation	Originalversionen af system- og driftsdokumentation skal forefindes på elektronisk form på SDUs dokumentationssystem og for klasse A IT-systemer i en papirversion i brandskabet. Dokumentationen skal beskyttes ved logisk adgangskontrol, således at kun medarbejdere med et fagligt relevant behov har adgang. Sikkerhedskritisk information om firewall-, router- og netværkskonfiguration og andre sikkerhedskritiske IT-systemer og procedurer skal behandles fortroligt.

Bortskaffelse eller genbrug af udstyr	Når udstyr bortskaffes eller genbruges, skal det sikres at kritiske/følsomme informationer og licensbelagte systemer fjernes eller overskrives.

10.8 Informationsudveksling

Tab, modifikation eller misbrug af data under forsendelse eller transmittering skal forebygges. Udveksling af data og programmer må kun ske på basis af formelle aftaler.
Det er normalt dataejeren, der har ansvaret for formelle aftaler om dataudveksling, men hvis vedkommende ikke er til stede, kan dataejerens nærmeste chef påtage sig ansvaret for dataudvekslingsaftaler.
Der skal foreligge regler for beskyttelse af data under forsendelse og transmittering. De særlige sikkerhedsrisici i forbindelse med elektronisk dataudveksling skal vurderes iht. datas klassificering.
Data, der er klassificeret Fortroligt skal udveksles over en sikker forbindelse hvor autenticitet og fortrolighed sikres. Det samme gælder al kommunikation af betydning for IT-sikkerheden.
For udveksling af data til/fra SCR, SCL/SLS og bankforbindelser følges de særlige sikkerhedsinstrukser for disse systemer.

Aftaler om informationsudveksling	Inden datakommunikationsforbindelse etableres til en samarbejdspartners IT-systemer, skal der udføres en risikovurdering. Den skal mindst omfattehvilke typer data der skal gives adgang til,nødvendige sikringsforanstaltninger,hvilke personalegrupper, der skal gives adgang til og privilegier til data.Inden der åbnes for adgang til SDUs IT-aktiver, skal der i hvert enkelt tilfælde udarbejdes en skriftlig aftale, der pålægger samarbejdspartneren at overholde SDUs IT-sikkerhedsregler.I tilfælde hvor en konsulent eller lignende via fjernadgang skal udføre systemarbejde skal vedkommende underskrive en fortrolighedsaftale inden adgangen åbnes. Der skal indgås skriftlig aftale om al rutinemæssig dataudveksling, dvs. udveksling af indkøbsordrer, fakturaer, betalingsordrer o.s.v., med eksterne partnere. Sikringsforanstaltningerne skal afstemmes med karakteren af de udvekslede data, herunder brug af vpn, ftp, kryptering mv.
Fysiske datamediers sikkerhed under transport	Fysisk transport af datamedier skal beskyttes mod tab, forvanskning og misbrug af data.
Automatisk indholdsfiltrering	E-mail skal håndteres i henhold til den gældende standard for SMTP. Nuværende standard er RFC5321, opdateret oktober 2008. Alle e-mail til/fra SDU skal passere SDUs e-mail skannings system, der frasorterer virus og markerer spam. Der må ikke eksistere e-mailservere der kan sende e-mail uden om dette system. Dette sikrer, dels at virus ikke når frem til modtageren, dels at misbrug der kan miskreditere SDU og dermed forhindre legal mail i at komme frem, ikke kan finde sted. Al transport af e-mail logges så det til enhver tid er muligt at se, hvad der er sket med en given e-mail på et givet tidspunkt. E-mail systemer overvåges i henhold til de til enhver tid gældende regler for SDUs vagtordning.

Brug af kryptering i forbindelse med dataudveksling	Kompromittering af data, der transmitteres over både offentlige og private netværk, skal forebygges.Data skal beskyttes i henhold til deres klassifikation, herunder hemmeligholdelse ved hjælp af kryptering. Kriterierne for klassificering er beskrevet i dokumentet "Dataklassificering på SDU". SDU's produktions webservere, som behøver et certifikat til kryptering af trafikken, må ikke benytte selvudstedte certifikater, men skal være udrustet med et officielt *-certifikat udstedt af IT-service.
Brug af kryptering i forbindelse med opbevaring af data	IT-systemer, der ejes af SDU, skal være tilgængelige for institutionen. Det betyder at, systembrugernavne og tilhørende kodeord, krypteringsnøgler og nøgler til andre sikringsmekanismer, skal deponeres i pengeskabe eller på anden betryggende vis, således at administrator eller andre bemyndigede medarbejdere i givet fald kan få adgang til systemerne, ved den normale ejers fravær. De deponerede oplysninger skal ajourføres, når der sker ændringer. Materiale, der er omfattet af offentlighedsloven eller forvaltningsloven, må ikke opbevares/arkiveres på krypteret form. Dette gælder dog ikke for data, der er omfattet af Persondataloven, forudsat at SDUs godkendte krypteringssoftware anvendes. Kryptering og efterfølgende dekryptering, der sker (automatisk) mellem afsender og modtager for at sikre datatransporten er ikke omfattet af forbudet mod kryptering.
Kryptering af filer	Kryptering af filer skal ske iht. kriterierne i "Dataklassificering på SDU".

10.9 Elektroniske forretningsydelser

Offentlig tilgængelig information	Det er driftsleverandørens ansvar at offentlig tilgængelig information, for eksempel på virksomhedens web-server(e), er passende beskyttet mod uautoriserede ændringer.

10.10 Logning og overvågning

Hvor det er muligt skal driftslogning etableres til kontrol og eftersporing af, hvad der sker i driftsafviklingsforløbet og netværksstyringen. Det fysiske driftsmiljø i maskinstuen overvåges. Datanet og flerbrugersystemer overvåges via et centralt overvågningssystem, som i tilfælde af kritiske fejl alarmerer den systemansvarlige/vagthavende IT-medarbejder via SMS/e-mail.

Kapacitetsovervågning	Alle serversystemer med kritiske informationer skal løbende overvåges for tilstrækkelig kapacitet til at sikre pålidelig drift og tilgængelighed.

Overvågning af systemanvendelse

Det skal kontrolleres, at IT-systemer anvendes korrekt. Overvågningsniveauet skal bestemmes ud fra en risikovurdering for det individuelle system og alle overvågningsaktiviteter skal beskrives. Af driftstekniske, sikkerhedsmæssige og/eller afregningsmæssige årsager sker der en løbende automatisk registrering af alle aktiviteter på de fleste IT-systemer. Denne overvågning sker automatisk og kræver ikke brugernes godkendelse. Ved mistanke om misbrug har systemadministratorer og de netværksansvarlige ret til at overvåge aktiviteterne, herunder ind- og udgående e-mail, uden på forhånd at informere brugerne herom i det konkrete tilfælde. En sådan overvågning kan kun ske med rektors forudgående tilladelse.

Hvor lovgivningskrav kræver det, skal IT-systemerne registrere anvendelsen med henblik på afklaring af uregelmæssigheder.

Systemlogs fra alle IT-systemer, der er klassificerede i kategori A, opsamles på den centrale logserver. Hvad der skal logges, samt logniveauet afgøres af systemernes dataklassificering. Som minimum skal al ”logon” information logges, dvs. adgang til applikationer/services på systemet.

På kritiske systemer med applikationer, som har en applikationsspecifik logfil (f.eks. ftploggen på servere med ftp adgang, skal denne logfil også sendes til en central logserver. Maskiner, der anvender "syslog" til logning af hændelser (Unix og Linux), bruger denne facilitet, hvorimod flerbruger-Windows-servere skal have installeret en syslog client (f.eks. EventReporter), som sender eventlogs til den centrale logserver i syslog format. Logs opbevares online på den centrale logserver i minimum 2 måneder, men kan fra backup spores yderligere et år tilbage.

Overvågning af netværk

IT-service skal have den nødvendige viden og redskaber til overvågning af universitetets netværk, for eksempel til fejlretning samt detektering og sporing af sikkerhedshændelser.

IT-service skal løbende overvåge netværket med henblik på detektering af brud på sikkerheden.

Der føres trafikstatistik over trafikmængden på netværket. Målingerne foretages på de enkelte router-interfaces på de primære netværks forbindelser og server forbindelser. Trafik målinger til/fra arbejdsstationer foretages kun ved særlige behov.

Overvågning af internetforbindelser

IT-service skal løbende overvåge internetforbindelser med henblik på at detektere elektroniske angreb. Logfiler skal gennemgås regelmæssigt og opbevares minimum 1 måned.

Registrering af driftsstatus

Fejl, som opstår i forbindelse med driftsafvikling af kritiske systemer, skal logges og rapporteres og der skal foretages udbedring, som dokumenteres. Brugerne skal holdes orienteret om fejlen og status på fejlretningen via SDUs "driftstatus" hjemmeside.Der skal være klare instruktioner og procedurer for logning og behandling af rapporterede fejl. Ejeren af et brugersystem skal godkende afhjælpninger. Fejlrettelser skal gennemgås for at sikre, at fejlene er blevet tilfredsstillende rettet, herunder at sikkerhedskontrollerne ikke er blevet kompromitteret og at de indgreb, der er sket, er autoriserede.

Tilgængelighedshændelser	Hændelser der har indflydelse på tilgængelighed skal afklares i henhold til gældende driftsaftaler (OLA). Driftshændelser der ikke kan afklares indenfor aftalt tid, skal udløse procedurer for hændelseshåndtering. De ramte brugere og systemejere skal informeres.
Skanning af netværk og systemer	For at opretholde et tilfredsstillende sikkerhedsniveau på såvel netværk som tilsluttede systemer udføres der skanning efter uønsket åbne porte, virus, uønskede tjenester m.v. Skanning må kun udføres af IT-medarbejdere eller efter aftale med eksterne samarbejdspartnere. Skanning på IT-systemer skal normalt annonceres til de berørte områders dataejere passende tid i forvejen. Skanning af netværkssegmenter skal, hvis de ikke foretages af den netværksansvarlige for det pågældende segment, annonceres til den netværksansvarlige passende tid i forvejen. Skanning skal udføres på en sådan måde, at belastning på netværk og systemer ikke forhindrer systemernes drift. Det er ikke tilladt at skanne eksterne netværk fra SDU's netværk.
Opfølgningslogning	Sikkerhedshændelser, fejlhændelser og væsentlige brugeraktiviteter på universitetets A og B klassificerede systemer skal logges. Uønskede hændelser skal så vidt muligt kunne spores.
Administratorlog	Aktiviteter udført af systemadministratorer og -operatører samt andre med særlige rettigheder skal logges.
Fejllog	Fejllogs fra alle IT-systemer, der er klassificerede i kategori A, opsamles på den centrale logserver, hvor disse skannes automatisk for uregelmæssigheder og en rapport sendes til den vagthavende IT-medarbejder.
Beskyttelse af log-oplysninger	Log-faciliteter og log-oplysninger skal beskyttes mod manipulation og tekniske fejl.
Tidssynkronisering	Driftsanlægs 'ure' skal være synkroniserede op mod ntp.sdu.dk af hensyn til akkurate registrerings- og logningsinformationer.

11 Adgangsstyring

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

11.1 De forretningsmæssige krav til adgangsstyring

Systemer til styring af adgangskoder	Så vidt muligt skal der benyttes it-systemer der automatisk kan styre de krav der findes til adgangskoder i afsnittet "Adgangskoder og metoder"
Sikker log-on	Log-on-grænsefladen skal give mindst mulig information om det system, der forsøges opnået adgang til. Der bør ikke anvendes samme administratorkodeord på maskiner indenfor og udenfor SDU's firewall.

Retningslinier for adgangsstyring

Retningslinierne skal omfatte:Betingelser for adgang til IT-anlæg.Alle kontraktlige og lovgivningsmæssige forhold vedrørende beskyttelse af adgang til IT-systemer, uanset om disse befinder sig på SDU, hos en samarbejdspartner eller hos en serviceleverandør.Brugerne skal være informeret om kravene til autoriseret adgang. Brugerne tildeles adgang til SDU's datanet og øvrige IT-aktiver alene ud fra et arbejds- og/eller studiebetinget behov. Alle ansatte får tildelt en brugerkonto med tilhørende kodeord og en e-mailadresse ved ansættelsen. Det er enhedschefens ansvar at fastsætte den enkelte medarbejders behov for adgang til øvrige systemer.

Adgangen til netværk administreres af IT-afdelingerne. Adgang til fælles systemer, infrastruktur og ydelser administreres af IT-afdelingerne. Brugerrettigheder til fælles administrative systemer (ØSS, STADS mf.) tildeles af den brugeransvarlige for det pågældende system.Der skal foreligge en præcis beskrivelse af hvordan en bruger oprettes og nedlægges. (Ansattes konti bør principielt ikke slettes, men blot spærres for at undgå genbrug af kontonavnet).Beskrivelsen skal også indeholde kontaktpersoner til de afdelinger, der huser systemer eller netværk hvortil denne afdeling ikke har privilegeret adgang.

Registrering af brugere

Hver ansat udstyres med et ”over tid unikt” brugernavn, således at forveksling aldrig kan forekomme. Brugernavnet konstrueres med mindst 3-8 tegns arbitrær bogstavkombination. Der anvendes altid opslag i PH, AD og LDAP for at sikre imod dubletter.

Der tildeles kodeord på en måde der sikrer, at brugeren tvinges til at skifte kodeord ved første log on. Et kodeord skal følge retningslinierne for gode kodeord.

Der oprettes en postkasse i det postsystem den pågældendes organisatoriske enhed anvender. Her anvendes typisk brugernavnet som postkasse, men dette er ikke et krav. Det er dog vigtigt, at postkassenavnet identificerer den ansatte bedst muligt. Postkassenavnet kan ændres over tid. Det er enhedschefens ansvar at få den nyansatte tilmeldt de relevante distributionslister og tilmeldt PH-systemet.

Afhængigt af hvilket arbejde den ansatte udfører, skal vedkommende have adgang til programmer og dele af netværk med egne autorisationssystemer f.eks. STADS, ØSS og Scanjour. Den ansatte kan i disse systemer kun oprettes med sit AD brugernavn som adgangsnavn. Kodeord i disse systemer skal også følge retningslinierne for kodeord.

Hvor det er teknisk muligt skal systemerne indeholde procedurer for tidsbegrænset udelukkelse af brugeren, hvis der gentagne gange indtastes fejlagtigt kodeord.Såfremt en bruger glemmer sit kodeord, skal Helpdesk på betryggende måde sikre sig brugerens identitet inden udlevering af nyt.

Al IT-anvendelse skal i videst muligt omfang kunne spores tilbage til en person. Der er dog en situation hvor det er lovligt at oprette konti hvorom det gælder, at man ikke direkte kan henføre en bestemt person til kontoen. Hvis de studerende skal til eksamen på PC og der i eksamensreglerne står, at der ikke må være adgang til private ting accepteres det, at der udleveres et brugerid og kodeord til den studerende, uden en registrering af, hvilket brugerid den studerende får udleveret. Kontoen skal lukkes umiddelbart efter eksamen for at forhindre misbrug.Dette sker for at opretholde den studerendes anonymitet i forhold til eksamen.

Der skal findes procedurer for registrering og afmelding af alle brugere og alt udstyr. Enhver bruger og ethvert IT-udstyr skal tildeles en entydig identifikation, som skal være den samme i al den tid, brugeren eller udstyret har adgangsrettigheder. Identifikationen må normalt ikke tildeles nogen anden person eller noget andet udstyr.

Et privilegium er en specifikation af en brugers tilladelse til at anvende specifikke funktioner i et IT-system, som benyttes af flere brugere. Systemprivilegier, dvs. privilegier, der tilknyttes f.eks. basisprogrammel inklusive operativsystemer, brugerprogrammer, databasesystemer, hjælpeprogrammer og netværksstyresystemer skal identificeres. En medarbejder, der tildeles systemprivilegier for at kunne udføre sine arbejdsopgaver, må kun udnytte disse privilegier til de formål, de er tildelt for. Medarbejderen skal være klar over, at enhver form for information, medarbejderen får adgang til under udførelsen af disse arbejdsopgaver, er fortrolig og ikke må misbruges under nogen form. Personkategorier og udstyr, der kan få behov for privilegier skal ligeledes identificeres. Tildeling og ændring af privilegier skal registreres og deres anvendelse

	skal kontrolleres og revurderes regelmæssigt. Det er enhedschefens ansvar, hvad den enkelte bruger får adgang til. Brugerne skal informeres om hvilke adgangsrettigheder og privilegier de får tildelt. Brugerens misbrug af rettigheder og privilegier vil blive betragtet som sikkerhedsbrud, der medfører sanktioner.
Identifikation af brugerprofiler for eksterne brugere	Brugernavn skal udarbejdes efter en standard navnekonvention. Dette gælder også for gæster, konsulenter og lignende, således at disse kan identificeres enkelt og ligetil. Standardkodeord må ikke anvendes på universitetets systemer. Disse skal ændres eller slettes.
Medarbejderes omplacering	Ved omplacering af medarbejdere skal alle rettigheder for pågældende bruger revurderes.
Gennemgang af brugerprofiler	Der skal etableres en opfølgningsprocedure således, at ejeren af IT-systemer kan foretage en regelmæssig gennemgang (mindst én gang pr. år) af tildelinger af adgangsrettigheder med tilhørende privilegier for at afdække om uønskede adgangsrettigheder eller privilegier er opnået uden om de gældende vilkår. Det er enhedschefens ansvar, at de tildelte privilegier ajourføres ved ændring af medarbejdernes arbejdsopgaver, herunder sletning ved medarbejderens fratrædelse.

11.2 Administration af brugeradgang

Systemejerne har ansvaret for, at der opstilles procedurer til kontrol af tildeling af adgangsrettigheder til IT-systemer. Procedurerne skal omfatte alle brugerkategorier og hele den periode, hvori adgangsrettighederne er gældende, d.v.s. fra registrering til formel afmelding af en bruger, der ikke længere har et arbejds- eller studiebetinget behov for adgang. Særlig opmærksomhed skal rettes mod de personer, der tildeles privilegier, som giver dem mulighed for at omgå et IT-systems kontroller.

Retningslinier for kodeord	Ved brugeroprettelse eller nulstilling af kodeord skal brugere tildeles en midlertidig adgangskode, som skal ændres umiddelbart ved første anvendelse. Brugerne skal følge god sikkerhedspraksis ved udvælgelsen og brug af kodeord. Hvis en bruger beskytter sin personlige arbejdsstation med BIOS kodeord, skal kodeordet deponeres i pengeskabe eller på anden betryggende vis, således at systemadministrator eller andre bemyndigede medarbejdere i givet fald kan få adgang til systemerne, ved den normale ejers fravær. Brugerinstruktionen om kodeord skal fastslå at:Kun brugeren må kende sit kodeord.Kodeord må ikke noteres ned, med mindre notatet kan opbevares sikkert.Kodeord må aldrig videregives til tredjemand.Ved mistanke om at kodeord er kendt af andre, skal det straks skiftes. Anvendes det samme kodeord i flere systemer, skiftes der også kodeord i disse.Kodeord må ikke inkluderes i nogen automatisk log-on-procedure. F.eks. må kodeord ikke lagres i forbindelse med en funktionstast eller en webbrowser.

Krav til skift af kodeord	IT-systemerne skal sættes op sådan at kodeord skal skiftes efter højst 180 dage.

11.3 Brugerens ansvar

Uautoriseret brugeradgang må ikke kunne forekomme. Opnåelse af betryggende sikkerhed forudsætter, at de autoriserede brugere følger de vedtagne retningslinier for håndtering af kodeord m.v. Alt hvad der foretages via brugerens brugernavn er entydigt brugerens ansvar. De nedenstående punkter skal derfor iagttages af brugeren:

Valg af sikre kodeord	Kodeord bør, udover at de skal følge SDUs normale regelsæt for kodeord, konstrueres efter følgende retningslinier:Undgå ”hackervenlige” kodeord såsom egne børns navne, ægtefælles navn, hundens navn og lignende d.v.s. ord der kan forekomme i en ordbog.Bland bogstaver, tal og/eller specialtegn. Vær dog opmærksom på, at ikke alle specialtegn er tilladte, herunder nationale bogstaver (f.eks. æ, ø å).Genbrug aldrig kodeord.
Brug af kodeordsbeskyttet pauseskærm	Alle arbejdsstationer aktiverer automatisk kodeordsbeskyttet skærmlås efter det interval, som IT-sikkerhedsudvalget har defineret. Medarbejderne bør dog selv aktivere skærmlåsen når de forlader deres arbejdsstation.
Opbevaring af kodeord til administrativ adgang	Kodeord for administrativ adgang til systemer, som er medtaget i SDUs beredskabsplan, skal opbevares i forseglet kuvert i aflåst og brandsikkert pengeskab.
Uovervåget udstyr	Data der er lagret på uovervågede pc'er (stationære og bærbare) betragtes i sikkerhedsmæssig henseende som offentligt tilgængelige med mindre maskinen er fysisk beskyttet (låst inde, hvilket betragtes som adgangskontrol). Brugere, der arbejder med følsomme data og/eller administrative konti, skal sikre sig at arbejdsstationen lukkes når arbejdspladsen forlades. Når en arbejdsstation undtagelsesvis anvendes af flere brugere til log-in på egen brugerkonto, skal den enkelte bruger foretage log-off fra datanettet inden arbejdsstationen efterlades. Anonyme brugerkonti anvendes kun, hvor almindelige brugerkonti ikke findes, f.eks. på arbejdsstationer på SDU’s offentlige bibliotek, der skal kunne bruges af gæster, samt hvor en særlig opsætning er nødvendig på udstyr til kontrol af og dataopsamling fra måleudstyr. Uautoriseret brug af disse anonyme konti forhindres ved kun at gøre dem anvendelige på bestemte arbejdsstationer. Til alle anonyme konti er knyttet en ansvarlig SDU medarbejder.

11.4 Styring af netværksadgang

Identifikation af netværksudstyr	De enkelte netværksenheder er grupperet indenfor en af de følgende 3 kategorier:Perimeter enheder: Betegner netværksudstyr, som er koblet direkte op mod Internettet på mindst et interface, f.eks. firewalls, VPN og dial-in udstyr.Kerne enheder: Betegner netværksudstyr, som er en del af SDU's backbone netværk, f.eks. centrale routere.Distributions/access enheder: Betegner netværksudstyr, som enten distribuerer trafikken mellem backbone netværket og de enkelte organisatoriske enheder på SDU, eller netværksudstyr, som distribuerer trafikken i en enkelt organisatorisk/geografisk enhed, f.eks. fordelingsswitche i lokale krydsfelter.Det er kun medarbejdere i IT-service NS, der har administrativ adgang til perimeter og kerne enheder, hvorimod det kan tillades at give andre IT-medarbejdere, herunder også de enkelte enheders IT-medarbejdere, adgang til distributions/access enheder.
Beskyttelse af diagnose- og konfigurationsporte	Forbindelser til diagnoseporte skal sikres mod uautoriseret anvendelse og adgangen skal kontrolleres.Der skal udarbejdes en procedure således, at diagnoseporte kun er tilgængelige i en tidsbegrænset periode, som er aftalt mellem ejeren og den eksterne leverandørs tekniske personale.
Autentificering ved adgang til netværket	Adgangen til det interne netværk fra andre lokationer end universitetets skal ske ved brug af brugernavn/kodeord via en krypteret tunnel (VPN) eller en SSH jumphost. Enhver undtagelse herfra er midlertidig og skal på forhånd godkendes af SDUs IT-sikkerhedskoordinator.
Retningslinier for brug af netværkstjenester.	Brugere skal kun have adgang til de tjenester, de er autoriseret til at benytte.
Anvendelse af sociale netværk	Det er tilladt SDUs brugere at anvende sociale netværkstjenester som f.eks. Facebook, Twitter og LinkedIn fra SDUs netværk, forudsat at brugen ikke generer eller forhindrer almindelig drift og brug af universitetets IT-systemer. Der må som udgangspunkt kun offentliggøres SDU informationer, som er klassificerede "Offentligt " på sociale netværk. Al anden SDU information, f.eks. præsentationer, billeder, film og andre data må ikke offentliggøres på sociale netværk hvis det kan indebære tvivl om hvorvidt universitetet bevarer sine intellektuelle rettigheder til informationerne. Som et led i den almindelige netværksovervågning bliver netværkstrafik til sociale netværk også overvåget.

11.5 Styring af systemadgang

Adgangen til flerbrugersystemer skal begrænses til autoriserede brugere og IT-systemer. Det skal være muligt at

- fastslå og verificere identiteten af hver enkelt autoriseret bruger og udstyr hvorfra brugeren søger adgang,
- sørge for, at adgangskontrolsystemet så vidt mulig sikrer brug af gode kodeord.

Begrænset netværkstid	SDU's systemer er i princippet tilgængelige døgnet rundt, med undtagelse af planlagte systemservice og systemopgraderinger, som lægges i de aftalte servicevinduer og annonceres på IT-services hjemmeside.
Automatiske afbrydelser	I det omfang det er muligt, skal der ske en automatisk terminering af sessioner når de har været inaktive i en given periode.
Brug af systemværktøjer	Adgangsrettigheder og tilhørende privilegier til at anvende systemhjælpeværktøjer skal begrænses og kontrolleres. Enhver form for fjernkontrol med en brugers IT-system skal i hvert enkelt tilfælde godkendes af den pågældende bruger.
Udvidede adgangsrettigheder	De udvidede adgangsrettigheder til SDUs infrastruktur, som f.eks. giver adgang til at rette i SDUs Active Directory, må kun tildeles i meget begrænset omfang og alene ud fra et arbejdsbetinget behov. Disse adgangsrettigheder tildeles udelukkende af enhedens IT-chef. Der skal benyttes særlige brugeridentiteter (såkaldte A-konti) til de udvidede rettigheder af hensyn til overvågning og opfølgning. De udvidede adgangsrettigheder, som giver administrator-adgang til IT-systemer, må kun tildeles i begrænset omfang og alene ud fra et arbejdsbetinget behov. Disse rettigheder tildeles af enhedens IT-chef. Tildeling af udvidede adgangsrettigheder til administrering af hostede systemer og applikationer, som vedligeholdes af IT-afdelingen, sker alene ud fra et arbejdsbetinget behov. Disse adgangsrettigheder tildeles udelukkende af systemejeren.
Skift af administrator kodeord ved fratrædelse	Hvis en person med kendskab til administrative kodeord fratræder skal disse kodeord ændres med det samme.
Kodeordsadministration	Systemerne skal så vidt muligt indeholde kodeordsadministration, der sikrer,at kodeord så vidt muligt overholder reglerne for gode kodeord,at brugerne ved valg af nyt kodeord skal indtaste dette to gange, ogat kodeord ikke vises på skærm ved indtastning.
Ændring af administrative kodeord	Administrative kodeord skal følge samme minimumsregler som øvrige kodeord. Administrative kodeord skal ændres hvis udenforstående får kendskab til disse, herunder administratorer der forlader universitetet.
Administration af arbejdsstationer	Generelt må lokale administrative adgangskoder ikke gives til brugerne af de arbejdsstationer der anvendes i organisationen. Dispensation gives kun af de enkelte enheders IT-sikkerhedsansvarlige.

11.6 Styring af adgang til brugersystemer og informationer

Adgangskontrol til programmer skal forebygge uautoriseret adgang til informationer, der er lagret på dem. Adgang til programmer og data kan kontrolleres ved hjælp af logisk adgangskontrol. Kontroller for programmer kan

- overvåge brugeradgang til data og programmers funktioner, f.eks. i overensstemmelse med en adgangspolitik,
- beskytte mod uautoriseret adgang fra ethvert hjælpeprogram, der er i stand til at omgå driftsafviklingssystemers og programmers kontroller,
- beskytte mod uautoriserede rettelser og ændringer af programmer,
- undgå, at andre IT-systemers sikkerhed, hvor man deles om de IT-tekniske ressourcer, kompromitteres.

Adgangsbegrænsning til informationer	Brugere af IT-systemer, inklusive IT-teknisk støttepersonale, skal kun gives adgang til data og IT-systemers funktioner i overensstemmelse med en defineret adgangspolitik. Hvis en ansat er rejst eller er langtidssyg og man har behov for adgang til denne medarbejders data eller postkasse, kan dette ikke ske uden tilladelse fra en personaleansvarlig eller medarbejderen selv. Henvendelse til servicedesk bør derfor først ske når en sådan tilladelse er indhentet. Proceduren skal sikre mod utilsigtet adgang til fortrolige data.
Isolering af særligt kritiske brugersystemer	Der skal træffes foranstaltninger til at mindske risici ved sensitive IT-systemers afvikling. Sensitiviteten kan indikere, at IT-systemerne skal isoleres og afvikles på et dedikeret driftssystem, der kun deler ressourcer med andre tilsvarende sensitive IT-systemer.

11.7 Mobilt udstyr og fjernarbejdspladser

Fortrolige data på mobile enheder	Der må kun opbevares fortrolige data på mobile enheder som laptops og mobiltelefoner, såfremt disse data beskyttes med et sikkerhedsgodkendt krypteringsprodukt.
Fjernarbejdspladser	Fjernarbejdspladser tillades når sikkerhedspolitikken i øvrigt overholdes.
Antivirusprogrammer	Anti-virusprogrammer skal være installeret på mobile og fjernarbejdspladser. Det er brugerens ansvar at softwaren holdes opdateret.
Adgang til netværket	Adgangen til universitetets netværk må kun ske gennem sikkerhedsgodkendte løsninger. Privat udstyr må kun tilkobles SDUs trådløse net og er derudover ikke tilladt på netværket.
Adgang til data på universitetets netværk	Der er ingen begrænsning i de dataklasser, der tillades fjernadgang til på virksomhedens netværk

Adgang til applikationer på universitetets netværk	Fjernadgang til universitetets applikationer er normalt begrænset til standard kontor-applikationer som mail, tekstbehandling, regneark og lignende. Yderligere adgang til applikationer begrænses /gives af de respektive systemejere
Opbevaring af fortrolige informationer på privat udstyr	Der må ikke behandles eller opbevares personhenførbare eller andre fortrolige informationer på andet udstyr end universitetets. Personligt ejet it-udstyr som f.eks. pc, PDA, bærbare harddiske, USB-hukommelse, MP3-afspillere, minidisks, cd- eller dvd-brændere må ikke anvendes til kopiering eller opbevaring af fortrolige data.
Brug af bærbare medier til fortrolige data	Fortrolige informationer skal krypteres når de opbevares eller transporteres på bærbare medier, f.eks. USB-hukommelse, PDA'er, cd'er, dvd'er eller disketter Manglende kryptering tillades hvis medierne, der benyttes til transport af fortrolige data, under transporten er overvåget af betroede personer.
Sikkerhedskontroller overfor fjernopkoblet udstyr.	Mobile enheder skal sikres med antivirus, firewall og adgangskontrolsystemer. Disse foranstaltninger skal opdateres løbende.

12 Anskaffelse, udvikling og vedligeholdelse af informationsbehandlingsystemer

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 bør sikkerhedsovervejelser altid indgå som en integreret del af processen. Sikkerhedskrav til IT-systemer, inklusive krav til reetableringsprocedurer, skal identificeres allerede i de indledende analysestadier for at skabe et optimalt løsningsgrundlag. Sikkerheden i basisprogrammellet og brugersystemer skal supplere hinanden.

12.1 Sikkerhedskrav til informationsbehandlingssystemer

Anskaffelsesprocedurer	Det skal sikres, 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 risikovurderes inden ibrugtagning.

Specifikation af sikkerhedskrav

Krav til sikringsforanstaltninger i nye IT-systemer eller ændrede, eksisterende IT-systemer skal specificeres som en del af den dokumenterede kravspecifikation til IT-systemet. Sikringsforanstaltningerne skal også overvejes ved evaluering af et standardsystem. Kravene til IT-sikkerhed og kontrol skal reflektere den værdi, som informationsaktiverne tillægges og de ødelæggelser, der kan opstå som følge af manglende sikkerhed. Indbyggede sikringsforanstaltninger i IT-systemer skal dokumenteres i alle relevante brugermanualer og driftsafviklingsinstruktioner. Sikkerhedsforanstaltningerne vurderes årligt under hensyntagen til registrerede hændelser og det generelle trusselsbillede.

Ekstra sikringsforanstaltninger kan være påkrævet for brugersystemer, der afvikler eller har indvirkning på følsomme eller fortrolige informationer.

Områder for kravspecifikation

Kravspecifikation skal omhandle følgende områder:Adgangskontrol.Alle væsentlige hændelser logges og overvåges.Beskyttelse imod fortrolighedskrænkelser i det omfang systemet skal behandle fortrolige eller personhenførbare informationer.Overholdelse af relevante love eller kontrakter.Mulighed for backup af data og system.Mulighed for genetablering efter kritiske, uforudsete fejlsituationer.Krav til viden og uddannelse af driftspersonale.

12.2 Korrekt informationsbehandling

Validering af inddata

Inddatavalidering skal beskytte brugersystemet mod inddatafejl og skal anvendes, hvor det vurderes hensigtsmæssigt for at sikre, at data overholder formelle formatkrav.

Kontrol af intern databehandling

Data, der dannes under driftsafviklingen skal løbende valideres og afstemmes. Validerings- og afstemningskontroller skal indbygges i IT-systemets driftafvikling for at afsløre forvanskninger. Kontrolniveauet afhænger af brugersystemets art og af, hvilken betydning en forvanskning kan få.

Ved overførsel af forretningsdokumenter eller andre dokumenter af juridisk betydning skal det ved manuelle eller automatiske procedurer sikres:At det enkelte dokument overføres netop én gang.At datameddelelser i en løbende transmissionsrækkefølge ikke bliver udeladt eller fremkommer i forkert rækkefølge.

Integritet af meddelelser

Integritetssikring skal forhindre uautoriseret modifikation af data. Ved anskaffelse af IT-systemer til behandling af juridisk bindende dokumenter skal der i hvert tilfælde tages stilling til og - hvor det er nødvendigt - opstilles krav til IT-systemerne til sikring af integritet, autenticitet og uafviselighed.

Validering af uddata

Dataejeren skal stille krav om at uddata fra universitetets systemer eller applikationer løbende valideres med det formål at sikre, data så vidt muligt er korrekte.

12.3 Kryptografi

Kryptering af harddiske	Indholdet af harddiske på arbejdstationer og mobile enheder skal krypteres i henhold til regelsættet i dokumentet "Dataklassificering på SDU".
Godkendelse af krypteringsprodukter	IT-sikkerhedsudvalget skal godkende alle krypteringsprodukter, før disse må benyttes på SDU.

12.4 Styring af driftsmiljøet

Sikring af testdata	Testdata skal beskyttes og kontrolleres. Brug af virkelige persondata til test skal begrænses. Hvis sådanne data anvendes til test, skal de så vidt muligt anonymiseres. Testdata, der indeholder virkelige data, skal beskyttes i overensstemmelse med deres klassifikation.
Kontrolleret adgang til kildekode	For at minimere risikoen for utilsigtede ændringer af kildekoder og objektkoder til edb-programmer skal der foretages kontrol med adgangsrettigheder og privilegier til brug af kildekoder og objektkoder, der findes i programbibliotekerne.
Migreringsstyring	Der skal udføres en overførselskontrol, hver gang programmer overføres til driftsmiljøet, uanset om programmerne er udviklet internt eller eksternt, for at beskytte IT-systemernes eksekverbare programmer og registre/data mod fejl og uautoriserede modifikationer. Denne kontrol foretages ved at alle ændringer gennemføres vha. en formaliseret change management proces. Det skal sikres, at systemudviklere ikke har mulighed for at foretage ændringer i programmer i driftsmiljøet.
Systemudvikling udført af ekstern leverandør	I forbindelse med systemudvikling udført af ekstern leverandør bør universitetet som udgangspunkt kræve:Adgang til at overvåge udviklingsprocessen,afleveringstest,dokumenteret løbende kvalitetssikring,deponering af kildekode,ophavsrettighed på kildekode.

12.5 Sikkerhed i udviklings- og hjælpeprocesser

De ansvarlige for udviklings-, vedligeholdelses- og driftsstøttefunktioner har ansvar for at ændringer bliver gennemgået for at sikre at de ikke kompromitterer sikkerheden i et brugersystem eller dets operationelle miljø.

Ændringer i standardsystemer	Ændringer skal begrænses for at fastholde et standardprograms driftsstabilitet. Med undtagelse af ændringer i parametre og specialopsætninger skal modifikation af standardprogrammer undgås.Under særlige omstændigheder, hvor det skønnes absolut nødvendigt at modificere et færdigt standardprogram og der ikke kan skaffes et andet standardprogram, som kan opfylde de stillede specifikationskrav, skal følgende punkter overvejes:Risikoen for, at indbyggede kontroller og pålidelighedsprocesser kan blive kompromitteret,sandsynligheden for, at modifikation vil kræve leverandørens indforståelse,muligheden for at den ønskede ændring kan leveres af leverandøren som en opdatering,risikoen for, at ændringen kan medføre at SDU bliver ansvarlig for fremtidig programvedligeholdelse.Herudover skal det originale standardprogram gemmes og alle ændringer skal foretages på en entydigt identificeret kopi og dokumenteres, så de eventuelt kan foretages på fremtidige versioner.
Ændringsstyring	Der skal føres kontrol med implementering af udvidelser og ændringer af brugersystemer for at minimere fejl og misbrug. Sikkerheds- og kontrolprocedurer må ikke kompromitteres. Der skal findes procedurer til udvidelses- og ændringskontrol af brugersystemer. Tilpasninger, opsætninger eller ændringer skal ske i henhold til retningslinierne for brugersystemets anvendelse. Det pålægges den systemansvarlige at foretage tilpasning, opsætning eller ændring af programparametre eller at sikre, at dette kun må udføres som serviceopgave af programleverandøren. IT-systemets brugere må ikke have adgang til tilpasninger eller opsætninger. Implementeringen af ændringen skal foretages på et aftalt tidspunkt.
Systemudvikling udført af ekstern leverandør	Krav i nærværende regelsæt samt reglerne for offentlige indkøb følges.
Sikring af applikationsudviklingsmiljøerne	Udviklingsmiljøer skal sikres mod trusler som uautoriseret adgang, ændringer og tab. Data skal sikres efter følsomhedsniveau.
Adgangskontrol for kildetekst	Kildetekst til applikationer under udvikling skal beskyttes med adgangskontrolsystemer for at sikre integriteten.
Sikkerhed i applikationsudvikling	Sikkerhed skal inkluderes som en integreret del af alle udviklingsprojekter.
Sikring af udviklingsmiljøer	Udviklingsmiljøer skal specielt sikre integritet i udviklingsprocessen, herunder sikring mod tab af data.
Gennemgang af systemer efter ændringer	Når driftsmiljøerne ændres skal kritiske forretningssystemer gennemgås og testes som beskrevet i universitetets change mangement proces for at sikre, at det ikke har utilsigtede afledte virkninger på universitetets daglige drift.

12.6 Sårbarhedsstyring

Godkendelse af nye eller ændrede systemer	IT-afdelingerne skal etablere en godkendelsesprocedure for nye systemer, for nye versioner og for opdateringer af eksisterende systemer samt de afprøvninger, der skal foretages, inden de kan godkendes og sættes i drift.
Rettelser til operativsystemer	IT-afdelingerne skal løbende vurdere tilgængelige sikkerhedsrettelser, for eksempel "patches" eller "hot-fixes", til anvendte operativsystemer. Udrulning/installation skal foretages efter behov.
Rettelser til applikations-programpakker	IT-afdelingerne skal mindst hver uge vurdere tilgængelige sikkerhedsrettelser ("patches" eller "hot-fixes"). Udrulning/installation skal foretages efter behov.
Større operativsystemopdatinger, for eksempel "service packs".	Når større opdateringer, for eksempel "service packs", er gjort tilgængelige fra leverandører skal IT-afdelingerne vurdere om disse skal installeres. Større opdateringer skal testes grundigt for kompatibilitet med anvendte applikationer, inden opdateringerne installeres i produktionsmiljøet.
Større programpakkeopdateringer, for eksempel "service packs".	Når større opdateringer, for eksempel service packs, er gjort tilgængelige fra leverandører skal IT-service vurdere om disse skal installeres. Større opdateringer skal testes i et testmiljø, inden opdateringerne installeres i produktionsmiljøet.

13 Styring af sikkerhedshændelser

13.1 Rapportering af sikkerhedshændelser og svagheder

Alle brugere af IT-systemer skal instrueres om, at de har pligt til og ansvar for at rapportere mistænkelige hændelser så hurtigt som mulig til deres lokale IT-sikkerhedsansvarlige. Ansatte, samarbejdspartnere og eksternt service- og rådgivningspersonale skal informeres om rapporteringsprocedurer og de typer af hændelser, der kan forekomme. Hændelserne kan være sikkerheds- og lovbrud, sikkerhedssvagheder, program- og funktionsfejl.

Ansvar og forretningsgange for sikkerhedshændelser	Der skal findes procedurer, som kan sikre en effektiv og kort reaktion på hændelser, der kan true IT-sikkerheden. Driftspersonalet og brugerne skal instrueres om, at alle har ansvar for at reagere ved tegn på sikkerhedstruende eller tabsgivende hændelser under driftsafviklingen. Forholdsregler og alarmering ved kriser, hændelser af fysisk karakter og logiske angreb er beskrevet i dokumentsættet ”Beredskabsstyring”.
Rapportering af formodede sikkerhedshændelser	Ved konstatering af brud eller formodede brud på it-sikringsforanstaltninger skal rapportering straks ske til HelpDesk. Hvis der er tale om brud af kritisk karakter skal rapporteringen ske til IT-sikkerhedskoordinatoren.

Rapportering af sikkerhedshændelser	Driftsafdelingen skal mindst en gang hver måned rapportere om hændelser af betydning for sikkerheden til IT-sikkerhedskoordinatoren. Mere konkret skal ethvert brud på fortrolighed, dataintegritet og tilgængelighed af systemer rapporteres.
Rapportering af programfejl	Brugere der observerer programfejl skal rapportere dette til Helpdesk.

13.2 Håndtering af sikkerhedsbrud og forbedringer

Proces for reaktion på hændelser	IT-sikkerhedskoordinatoren har ansvar for at definere og koordinere en struktureret ledelsesproces der sikrer en passende reaktion på sikkerhedshændelser.
Kontrol og opfølgning på sikkerhedsbrud	Brud på sikkerheden, uautoriseret adgang og forsøg på uautoriseret adgang til systemer, informationer og data skal registreres.
Indsamling af beviser	Hvis et sikkerhedsbrud afstedkommer et retsligt efterspil uanset om sikkerhedsbruddet er foretaget af en person eller en virksomhed så skal der indsamles, opbevares og præsenteres et fyldestgørende bevismateriale. Dette er beskrevet nærmere i "Beredskabsstyring - hændelseshåndtering".
At lære af sikkerhedsnedbrud	IT-sikkerhedsudvalget skal etablere et system, der kan kvantificere og overvåge typer, omfanget og omkostningerne ved håndteringen af sikkerhedsbrud. Dette er beskrevet nærmere i dokumentsættet "Beredskabsstyring".
Vurdering af tidligere hændelser	IT-sikkerhedsudvalget gennemgår på sit månedlige møde den forgangne periodes hændelser og anbefaler på denne baggrund hvorvidt IT-sikkerhedssystemet kan forbedres eller præciseres. F.eks. forslag om opdaterede regler eller procedurer eller opdateret risikovurdering.

14 Beredskabsstyring

Risikostyring og kriseplanlægning er nødvendige for at sikre universitetet mod uforudsete hændelser. Nødplanerne skal være med til at opretholde driften således at skaderne for universitetet minimeres.

14.1.Beredskabstyring og informationssikkerhed

For at formindske konsekvenserne af ulykker og fejl i SDUs IT-systemer skal der gennemføres beredskabsplanlægning til retablering af forretningskritiske systemer. Følgende overvejelser danner grundlag for beredskabsplanlægningen og fastlæggelsen af omfanget af beredskabsplanen:

- Det skal vurderes, hvordan hændelige og forsætlige ulykker og fejl i IT-systemerne kan indvirke på SDUs aktiviteter, samt med hvilke midler aktiviteterne kan fortsætte, indtil retablering af IT-systemerne er foretaget.
- De kritiske systemer skal udpeges og prioriteres indbyrdes.
- Tidsrammer for, hvor hurtigt systemerne igen skal være operationelle efter et uheld, fastlægges.

- Enhedschefen beslutter hvilke systemer, der skal udarbejdes beredskabsplaner for og har kompetence til at iværksætte dem.

Ramme for beredskabsplaner	It-sikkerhedsudvalget skal fastlægge en ensartet ramme for universitetets beredskabsplaner for at sikre, at alle planerne er sammenhængende og tilgodeser alle sikkerhedskrav, samt at de fastlægger prioriteringen af afprøvning og vedligeholdelse. Beredskabsplanen skal angive betingelserne for, i hvilke situationer den helt eller delvis skal aktiveres.Den skal præcisere,hvilke persongrupper der har det overordnede ansvar under en IT-beredskabssituation,hvordan de alarmeres,hvordan den koordinerede indsats organiseres. Nye planer skal være forenelige med eksisterende nødprocedurer, f. eks. evakueringsplaner og arrangementer med hensyn til separate IT-nødinstallationer, telekommunikation, lokaliteter og personales midlertidige placering.
Beredskabsplaner for virksomhedskritiske funktioner	Systemejerne er ansvarlige for at passende beredskabsplaner udarbejdes og vedligeholdes for de enkelte systemer med det formål at minimere nedbrud og udgifter som følge af sikkerhedshændelser.
Nødprocedurer for kritiske processer	Der skal for alle forretningskritiske processer eksistere en opdateret nødprocedure, der kan sættes i drift.
Identifikation af kritiske processer	Alle forretningskritiske funktioner og deres relaterede, processer, systemer og ejere skal være identificerede og dokumenterede.
Retablering af forretningskritiske systemer på ny lokation	For alle forretningskritiske systemer skal der forefindes en plan for retablering på ny lokation.
Beredskabsstyringsproces	IT-sikkerhedsudvalget skal udarbejde og vedligeholde en tværorganisatorisk beredskabsstyringsproces, som skal behandle de krav til informationssikkerhed, der er nødvendige for universitetets fortsatte drift.
Beredskabsplan	Beredskabsplaner skal udarbejdes, afprøves og vedligeholdes for virksomhedskritiske systemer og processer. IT-sikkerhedsudvalget er ansvarlig for at koordinere disse aktiviteter og for at lave en statusrapport til topledelsen hvert år.
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.
Forsikring mod hændelser	SDU er en statslig selvejende institution som er selvforsikret.

Uddannelse i beredskabsplaner	IT-sikkerhedskoordinatoren har ansvaret for at der foregår tilstrækkelig uddannelse af medarbejdere i de aftalte beredskabsprocedurer, inklusive krisehåndtering.
Afprøvning og vedligeholdelse af beredskabsplaner	Beredskabsplanens duelighed skal verificeres, og medarbejderne skal holdes orienteret om planen. Beredskabsplanens væsentlige dele skal afprøves regelmæssigt og mindst én gang om året. Beredskabsplanens aktualitet skal sikres ved regelmæssig opdatering. Der skal tages højde for ændringer i SDU's aktiviteter eller organisation, som kan være medvirkende til, at beredskabsplanen ikke længere er aktuel. Afprøvning af beredskabsplaner skal indeholde: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).

15 Overensstemmelse med lovbestemte og kontraktlige krav

Mange aspekter af SDUs virke kan være omfattet af lovgivning eller påvirket af kontrakter eller eksterne parters rettigheder. Universitetets systemer skal være i overensstemmelse med lovbestemte og kontraktlige krav. Forretningsgange, procedurer og politik for IT-sikkerhed skal årligt tages op til vurdering af, om der er behov for justeringer.

15.1 Overensstemmelse med lovbestemte krav

15.1.1 Lov-identifikation

Identifikation af relevant lovgivning	Ledelsen er ansvarlig for at identificere lovgivning der er relevant for universitetets drift, eller udpege en person der er ansvarlig for denne opgave. Ledelsen er ansvarlig for at alle eksterne sikkerhedskrav og universitetets håndtering heraf, klarlægges, dokumenteres og løbende vedligeholdes.

15.1.2 Ophavsret

Materiale, der er beskyttet af ophavsret, må ikke kopieres uden samtykke fra den, der er indehaver af ophavsretten. Ophavsretten er styret ved udstedelse af licenser. Ved salg eller videregivelse af IT-udstyr skal det sikres, at programlicenserne overføres til de nye brugere. I modsat fald skal de berørte programmer slettes, inden IT-udstyret videregives.
SDU har ikke et centralt register over alle programmer på SDUs IT-systemer. Aktiver, som er registreret i SDUs CMDB bliver løbende ajourført automatisk. Der henvises endvidere til reglerne for Apparaturregistret.
Brugerne skal orienteres om, at overtrædelse af in- eller eksterne bestemmelser i forbindelse med ophavsretsbeskyttelse kan medføre sanktioner og anklage mod SDU og den bruger, der begår overtrædelsen.
Den person, der installerer programmel, er personlig ansvarlig for, at licenskravene er opfyldt.

Retningslinier for ophavsrettigheder

Ledelsen har det overordnede ansvar for at universitetet fastholder en passende opmærksomhed på ikke at krænke tredje parts ophavsrettigheder.

IT-afdelingerne skal vedligeholde dokumentation for ejendomsretten af licenser.

Det skal løbende kontrolleres at software-licensaftaler overholdes, f.eks. at eventuelle begrænsninger i antal brugere, servere eller kopier overholdes.

Det skal løbende kontrolleres at der kun er installeret autoriserede systemer med autoriserede licenser på universitetet.

Brugere må ikke kopiere, konvertere eller udtrække information fra billed- og lydfiler eller tilsvarende ressourcer med mindre dette specifikt tillades fra rettighedshaveren.

Administration af softwarelicenser

Registrering af software licenser sker gennem enhedens IT-afdeling. Det er IT-chefens overordnede ansvar at der er et tilstrækkeligt antal licenser.

Medarbejdere må ikke forpligte universitetet ved at acceptere licensvilkår i software, som er ikke er godkendt af enhedens IT-afdeling.

Medarbejdere, som har autorisation til at anvende kopier af SDUs programmer på deres private udstyr, skal følge de procedurer og kontroller, som generelt er gældende for SDU.

Det skal undersøges, om udlevering af licensbeskyttede programmer, som skal anvendes hos den eksterne driftsserviceleverandør, kræver licensgivers godkendelse.

Publiceringsregler

Ophavsret til dette dokument har Dansk Standard (DS) og SDU.Dele af Dansk Standard DS 484:2005 "Standard for informationssikkerhed" er gengivet i dokumentet i henhold til aftale mellem DS og IT- og Telestyrelsen af juni 2004. Aftalen med DS fastlægger følgende regler for "IT-sikkerhedshåndbogens" anvendelse og distribution:Dokumentet må ligge på SDU's intranet, hvortil kun studerende og ansatte har adgang.Alle studerende og ansatte har ret til at printe en kopi af dokumentet til eget brug.Dokumentet må ikke videregives på elektronisk form til nogen trediepart uden for SDU.SDU har ret til at videregive papirkopier af dokumentet til relevante myndigheder og eksterne samarbejdspartnere i forbindelse med IT-sikkerhedsarbejdet.Tvivlsspørgsmål om dokumentets anvendelse, videregivelse, kopiering m.v. rettes til IT-sikkerhedsudvalget.

15.1.3 Sikring af universitetets kritiske data

Lovbestemte data

SDU's lovbestemte data skal beskyttes mod tab, uautoriseret modifikation og forfalskning.

15.1.4 Overholdelse af lov om personoplysninger

Personhenførbare data, der kan identificeres, og som behandles på et IT-system, henhører under bestemmelserne i Lov om behandling af personoplysninger. Nærværende regelsæt overholder Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 og ændring ved bekendtgørelse nr. 201 af 22. marts 2001: "Bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning".

Opbevaring og behandling af personoplysninger	Der må ikke behandles personoplysninger af fortrolig karakter på privat pc. Lov om behandling af personoplysninger gælder ved enhver opbevaring og behandling af persondata. Personoplysninger af fortrolig karakter må ikke opbevares eller behandles på bærbar pc, med mindre kryptering anvendes og at bekendtgørelse 528 omkring persondataloven overholdes.

15.1.5 Beskyttelse mod misbrug

Misbrugsbeskyttelse af it-udstyr	IT-faciliteters anvendelse til uvedkommende formål uden særlig tilladelse skal betragtes som uretmæssig og skal imødegås. Hvis det ved overvågning eller på anden måde identificeres, at sådanne aktiviteter finder sted, skal det påtales umiddelbart, og aktiviteterne bringes til ophør.

15.1.6 Lovgivning vedrørende kryptografi

Regulering på kryptografiområdet	Universitetet skal efterleve de nationale regler for kryptografering. Dette gælder også for medarbejdere der besøger andre lande, medbringende bærbart og mobilt udstyr. Juridisk afdeling og IT-sikkerhedskoordinatoren er ansvarlige for at informere medarbejdere om de regler og retningslinier der er gældende.

15.2 Overensstemmelse med sikkerhedspolitik og -retningslinier

SDUs ledelse skal sikre sig, at dens IT-sikkerhedspolitik bliver overholdt, og at vedtagne sikringsforanstaltninger bliver implementeret og fungerer med den tilsigtede effekt. Til dette formål må ledelsen indføre og vedligeholde et betryggende internt kontrolsystem for det daglige arbejde, således at medlemmerne af ledelsen på alle niveauer til stadighed fastholdes på deres ansvar for sikkerheden i eget funktionsområde.

Opfølgning på implementering af sikkerhedspolitikken	Mindst en gang årligt skal der udføres systematisk opfølgning på overholdelse af sikkerhedspolitikken i hele organisationen, og resultatet rapporteres til øverste ledelse. Hver enkelt leder skal løbende sikre sikkerhedspolitikken bliver overholdt inden for eget ansvarsområde.

Gennemgang af sikkerhedspolitik	IT-sikkerhedsudvalget skal kontrollere at sikkerhedspolitikken er indarbejdet i organisationen og overholdes. Kontrollen skal foretages mindst en gang årligt.
Overtrædelse af sikkerhedsretningslinierne	Det er ikke tilladt at forsøge at omgå sikkerhedsmekanismer. Det er ikke tilladt at foretage uautoriseret afprøvning af sikkerheden. Bevidste eller gentagne overtrædelser vil medføre disciplinære sanktioner. Det er ledelsens ansvar at sanktioner for brud på universitetets politikker, regler eller retningslinier håndhæves konsekvent og i overensstemmelse med gældende lovgivning.

15.3 Beskyttelsesforanstaltninger ved revision af informationsbehandlingssystemer

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 universitetets forretningsaktiviteter. De personer, der udfører revisionen, skal være uafhængige af det reviderede område.
Beskyttelse af revisionsværktøjer	Adgangen til revisionsværktøjer skal begrænses for at forhindre misbrug.