2023

Informationssikkerheds-håndbog

ISO 27001/2

WIRED RELATIONS

SYDDANSK UNIVERSITET | Campusvej 55, 5230 Odense M

Indholdsfortegnelse

1 Indledning

1.1 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. f.eks. Center for Cybersikkerhed (CFCS) og DKCERT's trusselsvurderinger.
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 tekniske og organisatoriske sikkerhedsforanstaltninger. Det kan være organisatoriske tiltag bestående af politikker, retningslinjer, procedurer og vejledninger eller tekniske systemrelateret foranstaltninger.

1.2 Hvorfor er informationssikkerhed nødvendig?

Information og informationsbehandlingsprocesser, -systemer og -netværk er væsentlige 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 forskningssamarbejde.
Samtidigt er uddannelses- og forskningssektoren den sektor, der på verdensplan er udsat for flest cyberangreb per organisation. Center for Cybersikkerhed vurderer truslen mod danske universiteter som "meget høj" forhold til cyberspionase og cyberkriminalitet.

1.3 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.

1.4 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 eller organisation, for enkelte afdelinger eller for specifikke informationssystemer, systemkomponenter 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.

1.5 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

Dette er de nuværende, tidligere godkendte termer, men der arbejdes på at lave en central fortegnelse over anvendte, tværgående begreber. Derfor vil understående liste fremadrettet ikke figurere direkte i denne håndbog.

Active Directory (AD): En fortegnelse på tværs af hele SDU, der styrer håndteringen af bruger- og computerrettigheder.
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, kodeord): Kombination af tegn, som benyttes til verifikation af en brugers identitet.
Adgangskort: Et adgangskort er en identifikationsbærer, der fx er udformet som et "plastikkort". Kortets dataindhold identificerer den person, kortet er udstedt til.
Aktiver: Alt, der har værdi for universitetet - således også immaterielle værdier som fx informationsbehandlingssystemer, data og dokumentation. Aktiver understøtter processer, kan være resultatet af en proces, eller ligefrem blive påvirket af en proces. Se også "informationsaktiver".
Anråb/svar: 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"/autenticitetsbevis godkendes, gives der tilladelse. På engelsk kaldes det et "Challenge/Response"-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".
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 pc'en.

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" og "dataejer".
Dataarkiv: Se "arkiv".
Dataejeren: En person, som er ejer af de data, der findes på systemet og dermed bestemmer, hvordan data må tilgås og af hvilke brugere.
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 eller organisation en naturlig forventning til, hvem der er "ejer" af et system og dets informationer, og at "ejeren" har såvel ansvar som rettigheder vedrørende informationerne. "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 områdeniveau er institutleder og områdechef enhedschef.
Entitet: En uafhængig enhed, der har selvstændig eksistens, fx en node/en person.

Firewall: Se "logisk filter".
Forretningskritiske systemer: Systemer, som i forbindelse med risikovurdering klassificeres som A eller B.
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.
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: Se fortrolighed.
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 eller organisationens 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** og **hjælpeprogrammer**.
  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 sammenhængende opgavekomplekser i en virksomhed eller mellem flere virksomheder. De udvikles som en specialopgave af 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. Standardsystemer anskaffes fra mange forskellige lagerførende leverandører. De kan af den enkelte bruger ved at vælge mellem nogle indbyggede parametermuligheder tilpasses dennes ønsker om opsætning og de regelsæt, hvorefter standardsystemet skal fungere. Ofte sammensættes flere af ovennævnte programtyper til en integreret programpakke.

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-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 organisationens ledelse.

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.

Kildekode: Et informationsbehandlingsprogram, der er skrevet i et symbolsk og standardiseret programmeringssprog.
Klartekst: Ubeskyttet og umiddelbar læselig tekst.
Kodeord: Se adgangskode.
Kompatibilitet: Den forenelighed, der skal være til stede, for at noget (et system) kan virke sammen med noget andet (andre systemer).
Konfidentialitet: Se fortrolighed.
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, så teksten ikke er læsbar for udenforstående, uden at de er i besiddelse af krypteringsforskriften og krypteringsnøglen.

Ledelsen: Direktionen.
Logoff: 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 eller sønderrivning af læsbare medier i strimmel- eller flagestørrelser, der ikke kan gensammensættes til læsbare informationer.

MFA: Multifactor Authentication (Multifaktorgodkendelse), der benytter to eller flere faktorer til verificeringer af brugerens identitet. De forskellige faktorer kan være noget du ved (fx password), noget du har (fx nøglekort, token) og noget du er (fx fingeraftryk).
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: Et 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.
Operationelle systemejer: Den person, som har ansvaret for installation og konfiguration af systemet, og som har ansvaret for beskyttelse af de data og applikationer, som systemet behandler. Den operationelle systemejer har ofte delegeret rettigheder på vegne af systemejer.
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 nødvendige autorisation og uden at blive opdaget. Se også "hacking".
Personaleansvarlig: En medarbejders nærmeste leder.
Phishing: En form for svindel, hvor it-kriminelle via forfalskede e-mail eller websider, prøver at narre brugernavne og kodeord fra autoriserede brugere. De afslørede brugernavne og kodeord bruges derefter af svindleren til at få uautoriseret adgang til systemerne.
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.
Proces: En beskrevet arbejdsgang, der bearbejder information. Processer understøttes af aktiver.
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.

Ransomware: En form for svindel, hvor it-kriminelle lykkes med at lægge et skadeligt program på en slutbrugers computer, som krypterer alle computerens filer samt alle filer, som slutbrugeren har skriveadgang til på filservere, skytjenester (fx Dropbox), m.v. Herefter kræver de it-kriminelle en løsesum for at slutbrugeren igen kan få adgang til sine filer.
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 eller oragnisationens 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 nødvendige justeringer for at fastholde det ønskede sikkerhedsniveau.

Sikret område: Et område, hvis afgrænsninger er mekanisk eller 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".

Supplerende arbejdsplads: Et sted som medarbejderen har indrettet som en arbejdsplads udenfor SDU's kontormiljø (hjemmearbejdsplads).

Systemadministrator: Er en privilegeret rolle, der giver adgang til fx at oprette og nedlægge brugere.

Systemejeren: Den person, som enten benytter eller er leder af den afdeling, der primært benytter systemet. Systemejeren har det overordnede ansvar for evt. leverandørstyring samt at systemet er passende indrettet mht. sikkerhed og funktionalitet. Systemejeren har ansvar for, at der forelægger relevante opdaterede risikovurderinger af systemet, der både tager høje for risikoen for SDU samt risikoen for eventuelle fysiske

personer, hvis oplysninger som behandles i systemet. Systemejeren kan uddelegere ansvar for daglig drift og sikkerhed til en operationel systemejer eller systemadministrator.
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., så tyveri og utilsigtet gennembrydning eller åbning 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, som 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-mailadresse,
- 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 computer-virus (malware) eller andre former for programmer, der kan afbryde eller ødelægge driften af såvel interne som eksterne systemer,
- påvirke fortroligheden af data,
- oprette trådløse net med direkte adgang til SDU's net uden forudgående godkendelse fra SDU's IT,
- kopiere tredjepartsmateriale 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 medmindre 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 DS/ISO/IEC 27001 og 27002.
- 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 nye it-systemer, hardware og tjenesteydelser.

4 Risikovurdering og -håndtering

Der skal være forståelse for de trusler, universitetet kan blive udsat for og for universitetets sårbarheder. Vurderingen skal også belyse sandsynligheden for at it-aktiverne udsættes for trusler, omfattende tilfældige, forsætlige og uforsætlige hændelser.

4.1 Overordnet risikovurdering

Som grundlag for ajourføring af SDU's tekniske og organisatoriske it-sikkerhedsforanstaltninger foretages engang årligt risikovurderinger af SDU’s forretningskritiske it-systemer. Udvalget for informationssikkerhed og

databeskyttelse forelægges det samlede risikobillede i en risikorapport og indstiller den accepterede risikoappetit til direktionen med henblik på endelig godkendelse. Ikke kritiske it-systemer skal have passende risikovurdering som minimum ved anskaffelsen.
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.
- 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.

4.2 Risikoanalyse

Der tages udgangspunkt i en risikoidentifikation for alle forretningskritiske systemer, der danner grundlag for identifikation af relevante trusler og risici.
Risikoanalysen skal belyse sandsynligheden for at it-aktiverne udsættes for trusler, herunder tilfældige, forsætlige og uforsætlige hændelser, der fører til hændelige eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger eller forretningsoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.
Risikoanalysen for hvert enkelt system består af en konsekvensvurdering og en sandsynlighedsvurdering. I konsekvensvurderingen vurderes der både konsekvens for SDU og de personer (de registrerede), hvis personoplysninger behandles i systemet. Denne vurdering foretages af systemejeren eller den operationelle systemejer (repræsenterer de forretningsmæssige krav) men med understøttelse fra SDU Digital Compliance.
Sandsynlighedsvurdering foretages af de system- og driftsansvarlige ligeledes med understøttelse af SDU Digital Compliance.
Analyserne samles i en risikorapport, som forelægges udvalget for informationssikkerhed og databeskyttelse som tidligere beskrevet.

5 Informationssikkerhedspolitikker

5.1 Retningslinjer for styring af informationssikkerhed

5.1.1 Politikker for informationssikkerhed

Sprog for sikkerhedspolitik

Informationssikkerhedspolitikken skal udarbejdes på de sprog, der anvendes som forretningssprog hos SDU, jævnfør SDU's sprogpolitik.

Omfang af informationssikkerhedspolitik

Informationssikkerhedshåndbogen er en integreret del af den overordnede informationssikkerhedspolitik. Informationssikkerhed defineres som de samlede foranstaltninger til at sikre fortrolighed, tilgængelighed og integritet. Foranstaltninger inkluderer tekniske, proceduremæssige, regel- og lovmæssige kontroller.

Publicering af sikkerhedspolitik

Informationssikkerhedspolitikken skal offentliggøres og kommunikeres til alle relevante interessenter, herunder alle medarbejdere.

5.1.2 Gennemgang af politikker for informationssikkerhed

Vedligeholdelse af sikkerhedspolitik

Den overordnede informationssikkerhedspolitik ejes, vedligeholdes og godkendes af direktionen.
I praksis reviderer SDU Digital Compliance informationssikkerhedspolitikken en gang årligt, hvorefter den forelægges Udvalget for informationssikkerhed og databeskyttelse på SDU mhp. indstilling til godkendelse af direktionen.

Andre politikker, regler og procedurer, der udarbejdes på baggrund af den overordnede informationssikkerhedspolitik, tilknyttes en ejer, som sikrer vedligeholdelse og godkendelse af de pågældende politikker, regler og procedurer.

Informationssikkerhedshåndbogen revideres og valideres én gang årligt SDU Digital, Compliance i samarbejde med SDU IT og Udvalget for informationssikkerhed og databeskyttelse. Andre politikker, regler, retningslinjer og procedurer vedligeholdes efter behov eller i forbindelse med ændringer, der kan have indflydelse på informationssikkerheden, herunder ændringer i organisationen, forretningsforhold, teknisk forhold eller juridiske forhold og ændringer af krav mod organisationen.

Underliggende procedurer

Vedligeholdelse af politikker, regler, retningslinjer og procedurer bør omfatte en vurdering af mulighederne for at forbedre organisationens politikker og metoder til styring af informationssikkerheden. Vedligeholdelsen bør tage højde for gennemførte revisioner og tilsyn.

6 Organisering af informationssikkerhed

6.1 Intern organisering

6.1.1 Roller og ansvarsområder for informationssikkerhed

Overordnede ansvarlig for informationssikkerheden
Rektor for SDU har det overordnede ansvar for informationssikkerheden.
Direktionen som helhed deler ansvaret for sikkerhed og vil uddelegere opgaver og ansvar vedrørende de enkelte funktionsområder, herunder også for vejledning og instruktion af de personer, der anvender SDU's it-faciliteter.
I praksis er det universitetsdirektøren, der særligt bærer informationssikkerhedsperspektivet i Direktionen.
Udvalget for informationssikkerhed og databeskyttelse på SDU
Udvalget er nedsat af universitetsdirektøren og udstikker retning og træffer beslutning om overordnede it-sikkerhedstiltag. Udvalget består af 1 repræsentant fra hver af SDU's fakulteter, SDU IT, SDU Digital, fællesområdet og SDU RIO. Cheferne for SDU IT og SDU Digital er fødte medlemmer. Både SDU's informationssikkerhedschef og databeskyttelsesrådgiver deltager som observatør.

Vurdering af risici og accept af restrisiko
Det er den enkelte system- og procesejer, der er ansvarlig for, at der foreligger en passende risikovurdering, hvor system- og/eller procesejer kan acceptere restrisikoen. System- og procesejer understøttes af den digitale organisation. Systemer der driftes af SDU IT, skal som udgangspunkt have indgået en systemforvaltningsaftale, hvor ansvaret mellem SDU IT og den forretningsenhed, der har systemejerskabet er aftalt og fordelt.
På nogle systemer kan det give mening at have en dataejer, der ejer de data, der findes på systemet og dermed bestemmer, hvordan data må tilgås og af hvilke brugere.

Generelt ansvar
Enhver ansat, studerende og konsulent på SDU har et medansvar for it-sikkerheden og vil til støtte herfor blive holdt informeret om sikkerhedsmæssige problemer og tiltag for at kunne leve op til dette ansvar. Retningslinjer for ansatte og studerendes anvendelse af IT på SDU er tilgængelig på henholdsvis SDUnet og MitSDU.

6.1.2 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.

Sikring af forretningskritiske systemer
Forretningskritiske systemer skal sikres gennem etableringen af brugerprofiler for at hindre misbrug af disse. Forretningskritiske systemer skal beskyttes ved hjælp af funktionsadskillelse så risikoen for misbrug af privilegier minimeres. Dette princip er en grundlæggende forudsætning for forebyggelse og begrænsning af konsekvenser, som stammer fra fejl, uheld og bevidst negative handlinger forårsaget af enkeltpersoner eller

grupper af enkeltpersoner. I de tilfælde, hvor funktionsadskillelse ikke er muligt, kompenseres så vidt muligt med andre sikkerhedskontroller.
Der skal være passende autorisationer og passende logning.

Funktionsadskillelse: udvikling, test og driftsmiljøer
Der skal være funktionsadskillelse i forhold til udviklings-, test- og driftsmiljøet.

6.1.3 Kontakt med myndigheder

Samarbejde med tilsynsmyndigheden for personoplysninger
SDU skal svare tilsynsmyndigheden inden for en rimelig frist, som fastsættes af tilsynsmyndigheden. Svaret skal omfatte en redegørelse for de iværksatte foranstaltninger og de opnåede resultater som reaktion på bemærkningerne fra tilsynsmyndigheden.

Kontakt med relevante myndigheder
Ved brud på sikkerheden skal der være etableret en procedure for håndtering af bevismateriale og eventuelt kontakt med relevante myndigheder.
Hvis personoplysninger kompromitteres, skal det indrapporteres til Datatilsynet inden for 72 timer. Hvis der ikke er klarhed over hændelsen, laves der en foreløbig indrapportering, der efterfølgende opdateres.
Hvis tredjepart behandler personoplysninger på vegne af SDU, skal denne jf. databehandleraftalen underrette SDU, hvis der er opstået et brud på persondatasikkerheden.

6.1.4 Kontakt med særlige interessegrupper

Kontakt med interessegrupper og fora
SDU skal oparbejde og vedligeholde kontakt med sikkerhedsfaglige interessegrupper.
Informationssikkerhedschefen deltager i relevante it-sikkerhedsfaglige erfagrupper.
CIO og CISO deltager i henholdsvis CIO-forum og CISO-forum under Danske Universiteter, hvor der sidder repræsentanter fra alle universiteter i Danmark.

Fagligt samarbejde med grupper og organisationer
Udvalget for informationssikkerhed og databeskyttelse har ansvar for at holde sig orienteret om den generelle udvikling på it-sikkerhedsområdet og for at videregive relevant information inden for SDU.

Udvalget for informationssikkerhed og databeskyttelse 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.

Information om nye trusler, virus og sårbarheder
Den operationelle systemejer skal holde sig orienteret inden for de benyttede platforme.

Den operationelle systemejer skal informere relevante personer i ledelsen om nye trusler, som potentielt kan berøre de pågældende forretningsenheder.
SDU IT skal definere en proces for identifikation af sårbarheder. SecOps har den daglige overvågning af systemerne. SDU har moderne sikkerhedsprodukter, der dagligt bliver opdateret med nye exploits. SDU abonnerer på alarmer fra CSIS. Desuden modtages varsler fra DKCERT og Center for Cybersikkerhed.
It-chefen er ansvarlig for fastlæggelse af sikkerhedsniveauet og kan søge rådgivning ved Informationssikkerhedschefen og Team Sikkerhed.

6.1.5 Informationssikkerhed ved projektstyring

Projektmodellen skal indeholde følgende overvejelser omkring informationssikkerhed:
Kravspecifikationen skal indeholde kravene til informationssikkerhed. IT-systemer skal være indrettet med passende organisatoriske og tekniske sikkerhedsforanstaltninger. Sikkerheden skal tilpasses alt efter hvilken klassifikation af oplysninger, der behandles i systemet. IT-systemer der indeholder fortrolige forretningsoplysninger eller følsomme eller fortrolige personoplysninger skal sikres passende mod tab af fortrolighed, integritet og tilgængelighed af data.

Identifikation af nødvendige sikringstiltag skal blandt andet gøres ved hjælp af risikovurderinger. Derudover skal principperne om databeskyttelse gennem design og standardindstillinger efterleves.

Informationssikkerhed skal være en integreret del af alle it relaterede projekter.

Der henvises desuden til SDU's projektmodel og porteføljestyring samt retningslinjen om sikkerhedsvurderinger ved it-anskaffelser.

6.2 Mobilt udstyr og fjernarbejdspladser

6.2.1 Politik for mobilt udstyr

Sikkerhed i forbindelse med mobile enheder
Brugere af organisationens bærbare pc'er og andre mobile dataenheder (fx telefoner, tablets m.fl.) er ansvarlige for at beskytte de data, der behandles på disse, samt enhederne selv.

Adgang til bærbare computere
Bærbare computere skal beskyttes med adgangskode, pinkode, fingeraftryk eller flerfaktorautentifikation som fx YubiKeys.
BIOS-konfiguration på bærbare pc'er skal beskyttes med adgangskode.

Adgang til mobile enheder

Adgang til data på mobile enheder skal være beskyttet af adgangskontrol (password, fingeraftryk, biometri, flerfaktorautentifikation).
Mobile enheder må ikke efterlades uden opsyn i uaflåste rum.

Fortrolige data på mobile enheder
Der må opbevares fortrolige data på mobile enheder, hvis disse data beskyttes med et produkt, der er godkendt af SDU IT.

Backup af mobile enheder
Slutbrugere er ansvarlige for backup af deres mobile enheder.

Installation af software på mobile enheder
Slutbrugere må kun installere apps fra Firmaportal, MacSDU, Microsoft Store, Google Play, Apple Appstore eller Windows Store på deres mobiltelefoner og tablets.
Installation af software på PC er som udgangspunkt begrænset til SDU godkendt software med mindre, der er tale om lokalt begrænset brug jf. retningslinjen for sikkerhedsgodkendelse af it-anskaffelser.

Sikkerhedskontroller for mobilt udstyr
Mobile enheder skal som udgangspunkt sikres med antivirus, firewall (fx Microsoft Defender for Endpoint, hvor det er muligt) og adgangskontrolsystemer. Disse foranstaltninger skal opdateres løbende.

Ansvar og ejerskab for privat udstyr
Medarbejderen forpligter sig til at overholde de samme regler, som gælder for øvrig brug af organisationens udstyr.

Brug af privat udstyr
Det er tilladt at koble privat udstyr op mod arbejdspladsens informationssystemer, så længe SDU's sikkerhedsforanstaltninger ikke bliver omgået. Det kan fx være relevant for studerende og eksterne lektorer.
SDU's administrative systemer må kun tilgås fra SDU's administrerede maskiner.

Mobile enheders tilslutning til andre netværk
Det er tilladt at forbinde mobilt udstyr til andre netværk. På PC kræver opkobling til SDU's interne systemer VPN.

Sikkerhedskopiering (backup) af privat udstyr
Anvendelse af privat udstyr til udførelse af arbejde for SDU bør begrænses i videst muligt omfang.
Der foretages ikke sikkerhedskopiering af informationer på privat udstyr.
Medarbejderen er ansvarlig for at sikkerhedskopiere relevante informationer, så datatab undgås.
Medarbejderen skal acceptere en særskilt erklæring om, at SDU må slette (Wipe) data på privat udstyr, der anvendes til opbevaring af SDU's informationer.

SDU er ikke erstatningspligtig for tyveri, bortkomst, skade eller tab af personlige informationer for privat udstyr.

Logning og overvågning af privat udstyr
Brugen af privat udstyr på netværket logges og overvåges, som arbejdspladsens øvrige udstyr. SDU-identitet, som tilgår SDU data vil bl.a. blive logget i sign-in logs.

6.2.2 Fjernarbejdspladser

Forsikringsdækning for mobile enheder
SDU er selvforsikret.

Adgang fra distancearbejdspladser
Der skal anvendes krypteret forbindelse.
Adgang gives kun til brugere via flerfaktorautentifikation (MFA).

Sikring af fjernarbejdspladser
Fjernarbejdspladser og deres kommunikationsforbindelser skal beskyttes i forhold til de informationer og forretningssystemer, de benyttes til.
Det er ikke tilladt at overlade SDU enheder til børn, familie eller venner.
Enheder skal opbevares så der ikke er uautoriseret adgang for tredjemand. Fx skal der benyttes låsekode.

7 Medarbejdersikkerhed

7.1 Før ansættelsen

7.1.1 Screening

Verifikation af referencer
Udvalgte referencer eller eksamensbeviser for betroede medarbejdere skal verificeres. Den ansættende enhed vurderer individuelt nødvendigt omfang af verifikation. Denne vurdering kan understøttes af SDU HR.

Ren straffeattest
Ved besættelse af stillinger, hvor dette er relevant, skal ansøgeren forud for ansættelse erklære at være ustraffet, samt ikke at være sigtet eller tiltalt i verserende sager.

Baggrundscheck af medarbejdere skal omfatte:

- Identitetskontrol.

- Ansøgerens curriculum vitæ.
- En personlig reference.
- Uddannelser og professionelle kvalifikationer.

Baggrundscheck af ansatte

- Den ansættende enhed, eller efter aftale SDU HR, udfører hvor det skønnes relevant et baggrundstjek. Omfanget af baggrundstjekket er afstemt med den ansættende enhed i forbindelse med at stillingen slås op.
- Der skal laves et forsvarligt baggrundscheck af medarbejdere med ansvar for forretningskritiske arbejdsområder og it-medarbejdere.
- I enkelte tilfælde kan det vurderes, at der skal laves egentlig sikkerhedsgodkendelse med ret til at læse klassificeret materiale jf. sikkerhedscirkulæret.
- PET-sikkerhedsgodkendelse af øvrigt af personale finder ikke sted.
- Til sikkerhedsstillinger skal det vurderes om kandidaten kan betros rollen og om kompetencer er på plads.

7.1.2 Ansættelsesvilkår og betingelser

Indhold af ansættelseskontrakter

- Der skal orienteres om krav til fortrolighed - fx at Straffelovens § 152 er gældende.
- Der skal stilles krav om compliance med lovgivningen – fx ved behandling af personoplysninger.
- Klassifikation af data skal efterleves.
- Der skal orienteres om ansættelsesretlige konsekvenser ved manglende efterlevelse.

Samarbejdsaftaler

For at sikre, at organisationens sikkerhedsmålsætning ikke kompromitteres, skal ethvert formaliseret eksternt samarbejde være baseret på en samarbejdsaftale.

Aftale om ansættelse

Faste og midlertidige medarbejdere skal underskrive en aftale om ansættelse, der beskriver SDU's og medarbejderens ansvar og forpligtelser vedrørende informationssikkerhed.

Specifikke fortrolighedserklæringer

HR-afdelingen og det ansættende fakultet kan desuden supplere med specifikke fortroligheds erklæringer såfremt den ansatte vil få adgang til data, der vurderes som værende specielt forretnings kritiske.

7.2 Under ansættelsen

7.2.1 Ledelsesansvar

Det er ledelsens ansvar at alle medarbejdere:

- er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med sikkerhed, før de tildeles adgang til organisationens systemer og data.
- er gjort bekendt med nødvendige retningslinjer, således at de kan leve op til organisationens informationssikkerhedspolitik og evt. forskningsinstruks.
- er motiverede til at leve op til organisationens informationssikkerhedspolitik og retningslinjer.
- holder sig inden for de retningslinjer og bestemmelser, der er for ansættelsen, inkl. organisationens informationssikkerhedspolitik og konkrete arbejdsmetoder.
- at vurdere behovet for revurdering af sikkerhedsgodkendelsen under ansættelsesforholdet. PET-sikkerhedsgodkendelser gælder som standard i 10 år.

7.2.2 Bevidsthed om uddannelse og træning i informationssikkerhed

Uddannelse i sikkerhedspolitikken

- Alle medarbejdere skal have træning i organisationens informationssikkerhedspolitik og baggrundsviden omkring denne.
- Alle medarbejdere modtager løbende instruktioner i overholdelse af organisationens informationssikkerhedspolitik samt retningslinjer for brug af it for ansatte.
- Indholdet skal omfatte politikker og procedurer samt regulering og andre krav rettet mod organisationen.
- Der skal være selvstændigt fokus på behandling af personoplysninger – herunder på politikker og procedurer, på hvad en sikkerhedshændelse kan have af konsekvenser, og hvordan og til hvem der rapporteres.
- Informationssikkerhedspolitikken og retningslinjer for brug af it for ansatte er tilgængelig på SDUnet, hvor medarbejdere er forpligtiget til at holde sig opdateret.
- Træning af medarbejderne i organisationens informationssikkerhedspolitik skal foregå ved inddragelse af forskellige formidlingsmetoder, eksempelvis ved hjælp af e-mail, plakater, rundskrivelser, møder eller kampagner.
- Alle medarbejdere modtager løbende uddannelse for at sikre viden om og opmærksomhed på informationssikkerhed.
- Alle nye medarbejdere modtager, senest på første arbejdsdag, organisationens informationssikkerhedspolitik.

Sikkerhedsuddannelse for it-medarbejdere

- It-medarbejdere skal løbende gennemgå produktspecifik sikkerhedsuddannelse for de it-produkter, der er mest udbredte i organisationen.
- Alle it-medarbejdere skal specifikt uddannes i sikkerhedsaspekter, for at minimere risikoen for sikkerhedshændelser.

Uddannelse i klassificering af informationer

De ansatte skal modtage instruktioner om, hvorledes data og dokumenter klassificeres.

7.2.3 Sanktioner

Overtrædelse af sikkerhedsretningslinjerne

- Det er ledelsens ansvar, at sanktioner for brud på organisationens politikker, regler eller retningslinjer håndhæves konsekvent og i overensstemmelse med gældende lovgivning.
- Det er ikke tilladt at foretage uautoriseret afprøvning af sikkerheden.
- Det er ikke tilladt at forsøge at omgå sikkerhedsmekanismer.
- Hændelser, hvor medarbejdere er involverede, bliver håndteret konsekvent i overensstemmelse med gældende personalepolitik.
- Bevidste eller gentagne overtrædelser kan medføre disciplinære sanktioner.
- Der skal være grundig bekræftelse af, at der har været et brud på informationssikkerheden.
- Det skal være klart for medarbejdere, at brud kan medføre sanktioner, men generelt arbejdes der efter en lærende tilgang til sikkerhedshændelser, hvor der er fokus på at lære af fejl mhp. forebyggelse.

7.3 Ansættelsesforholdets ophør eller ændring

7.3.1 Ansættelsesforholdets ophør eller ændring

Fortrolighedserklæring og fratrædelse

Ved fratrædelse gælder den samme fortrolighed, der er nedskrevet i kontrakten.
Hvis den tidligere ansatte er underlagt et krav omkring fortrolighed ud over straffelovens §152 vil den tidligere ansatte modtage meddelelse herom i sin Digital Post-udbyder ved sin fratrædelse.

Bortvisning

Adgangskort skal inddrages og spærres, adgang til ressourcer skal spærres, nøgle inddrages nøgler, og udstyr indhentes.

8 Styring af aktiver

8.1 Ansvar for aktiver

8.1.1 Fortegnelse over aktiver

Registrering af it-udstyr

Det er SDU IT's ansvar, at alle computere og smartphones er registreret med ejer, bruger, serienummer og eventuelt placering.
Der skal vedligeholdes en fortegnelse over samtlige relevante enheder, som er forbundet til organisationens it-infrastruktur.

8.1.2 Ejerskab af aktiver

Sikkerhedsansvar for informationsaktiver
Inventarlister over informationsaktiver og it-udstyr med tilhørende ansvarlige ejere skal udarbejdes og vedligeholdes.

Ejere betyder de personer der er ansvarlige for sikker drift af udstyret.

Ejeren skal sikre, at aktivet er klassificeret og beskyttet på behørig vis.

Ejeren skal definere og regelmæssigt gennemgå adgangsbegrænsninger og klassifikation for vigtige aktiver.

Den digitale organisation har ansvar for vedligeholdelse af en liste over samtlige informationssystemer. Listen skal angive henholdsvis den sikkerhedsansvarlige data- og systemejer for hvert enkelt system.

Alle it-aktiver skal som udgangspunkt registreres og afmeldes jf. SDU's regnskabsinstruks afsnit 2.2.2.6 samt bilag 17. Hvis et it-aktiv udleveres til personligt brug, skal brugeren registreres både ved modtagelse og aflevering. Når it-aktivet kasseres, skal det afmeldes.

8.1.3 Accepteret brug af aktiver

Information omkring SDU's politikker og procedurer for anvendelse af SDU's aktiver
Væsentlige retningslinjer som medarbejdere forventes at kende, skal være tilgængelige på SDUnet.

Brug af cloud services
Cloud-løsninger må anvendes, hvis der er et forretningsmæssigt behov og der ikke er væsentlige sikkerhedsmæssige risici forbundet med løsningen.
Der skal gennemføres en risikovurdering, hvor de it-sikkerhedsmæssige trusler databeskyttelsesretlige problemstillinger som er forbundet med cloud-løsningen, vurderes, inden aftale indgås.

Opbevaring af personoplysninger ved brug af cloudløsninger kræver en godkendt databehandleraftale. Ligeledes kræver opbevaring af SDU’s fortrolige forretningsoplysninger at systemet er centralt godkendt jf. retningslinjen for sikkerhedsvurderinger ved it-anskaffelser. Det er derfor som udgangspunkt ikke tilladt at dele, eller lagre organisationens fortrolige informationer eller personoplysninger i 'skyen', ved brug af cloud serviceudbydere som fx Dropbox, Googledrive.

Brugere af sociale medier skal være specielt opmærksomme på at:
De sociale medier, som du bruger, kan registrere og gemme oplysninger om dig og hvilke informationer du søger og bruger.
Informationer som du har lagt ud på et socialt medie, kan kun meget vanskeligt, måske aldrig, trækkes tilbage.
Du vil med stor sandsynlighed opleve at nogen forsøger at franarre dig dine bruger-id'er og/eller dine adgangskoder (phishing).
Hvis du benytter sociale medier som led i dit arbejde for SDU, skal du være opmærksom på ikke at dele fortrolige forretningsoplysninger eller personoplysninger, du ikke har ret til at dele. Deling af personoplysninger fx billeder på sociale medier vil i de fleste sammenhænge kræve samtykke.

Sociale netværk med forretningsforbindelser
Informationssikkerhedshåndbogen regulerer som udgangspunkt kun din anvendelse af sociale medier, når du benytter sociale medier som led i dine arbejdsopgaver for SDU. Det er dog alment kendt, at aktører kan målrette deres interesse på ansattes private sociale medier mhp. at få adgang til dig og din adgang til SDU. Det er tilladt at "connecte" eller "være ven" med samarbejdspartnere og kunder på sociale medier eller netværk. Vær opmærksom på falske profiler, der kan være aktører, der er interesseret i dig og dit netværk.

Overvågning af sociale medier
Browsere på SDU's pc'er gemmer blandt andet information om din brug af sociale medier, og du må forvente, at SDU kan få adgang til denne information.
Som led i den almindelige netværksovervågning bliver netværkstrafik til sociale medier også overvåget.

Omfang af brug af sociale medier
Anvendelse af sociale medier må ikke genere almindelig drift og brug af SDU's it-systemer.

Accepteret brug af informationsaktiver
Udvalget for informationssikkerhed og databeskyttelse skal placere ansvaret for hvem i organisationen, der skal lave retningslinjer for accepteret brug af alle organisationens informationsaktiver. Som udgangspunkt laves de overordnede retningslinjer i SDU Digital Compliance med inddragelse af SDU IT og andre relevante afdelinger. SDU Digital Compliance skal tilse at der findes retningslinjer for accepteret brug af alle virksomhedens informationsaktiver.
Som udgangspunkt bør man kun benytte SDU's aktiver (it-udstyr og software) til løsning af arbejdsopgaver for SDU. Indenfor lovgivningens- og rettighedsmæssige rammer kan det i begrænset og rimeligt omfang benyttes til privat brug. Se retningslinjer for brug af it for ansatte.

Medarbejderes private brug af e-mail
Det anbefales ikke, at SDU-e-mail benyttes til private formål.
Det er acceptabelt at benytte e-mail til private beskeder i rimeligt og begrænset omfang.

Al mailtrafik betragtes som SDU's ejendom.

Medarbejdere bør som udgangspunkt nøje overveje hvilke private dokumenter, der opbevares på udstyr stillet til rådighed af SDU. Private dokumenter, mails og lignende skal markeres med "privat" for at blive undtaget fra eventuel manuel gennemgang ved sikkerhedshændelser. SDU forbeholder sig ret til at skaffe sig adgang til data og e-mail for medarbejdere, hvis dette sker af drifts- eller sikkerhedshensyn. SDU må som udgangspunkt ikke tilgå emner, der er mærket privat, medmindre der forelægger særlige omstændigheder (fx mistanke om misbrug) eller der er grund til at tro at fx filer kan udgøre en sikkerhedsmæssig risiko for SDU.
Se retningslinjer for brug af it for ansatte samt personalepolitikken.

8.1.4 Tilbagelevering af aktiver

Returnering af aktiver ved aftrædelse
Medarbejderen skal returnere samtlige informationsaktiver, der tilhører organisationen, på sin sidste arbejdsdag.

Informationer på privat udstyr, ansættelsens ophør
Såfremt en medarbejder undtagelsesvis har opbevaret SDU informationer på privat udstyr skal disse slettes ved ansættelsens ophør.
SDU IT skal, i samarbejde med den relevante lokale ledelse, sikre, at organisationens informationer på privat udstyr ikke er tilgængelige ved ansættelsens ophør.
Medarbejderen skal være indforstået med, at enheden nulstilles (wipes) ved ansættelsens ophør.

8.2 Klassifikation af information

8.2.1 Klassifikation af information

Informationer og data skal klassificeres
Der skal foreligge en beskrivelse af, hvordan data og informationer klassificeres.

Klassifikation af it-systemer
Digitaliseringsstyrelsen har i regi af den fællesoffentlig digital arkitektur (FODS) arbejdet med at etablere en fælles standard for beskrivelse af it-systemer.
It-systemer skal kunne opmærkes ift. deres grad af kritikalitet ved hjælp af klassifikation for kritikalitetstyper:

- Samfundskritisk it-system
- Forretningskritisk it-system
- Ikke kritisk it-system

Et *samfundskritisk it-system*, som enten er vigtigt for den nationale sikkerhed eller for vigtig infrastruktur, hvor misbrug af data vil få store konsekvenser, eller hvor driftsforstyrrelser kan have stor betydning for økonomien i staten eller for mange borgere eller virksomheder.

Et *forretningskritisk it-system* er et it-system, hvor driftsforstyrrelser kan medføre, at størstedelen af myndighedens medarbejdere ikke kan udføre deres arbejde, eller at myndigheden vanskeligt kan overholde sine

forvaltningsmæssige forpligtigelser. I forhold til SDU vil det være it-systemer, der ved længere tids driftspåvirkning vil medføre, at SDU ikke kan udføre sine kerneopgaver; forskning, undervisning og videnssamarbejde.

Ikke kritiske it-systemer er de resterende systemer.

Klassifikation af data

Data, herunder dokumenter, i it-systemer bør klassificeres med forskellige klassifikationer ift. fortrolighedsgrad jf. SDU's Retningslinjer for dataklassifikation.

Aktuelt er der tale om understående kategorier:

Klassificeringstrin	Kritikalitet for registrerede personer	Kritikalitet for SDU
0. Offentligt	Ikke personoplysninger	Offentlige forretningsoplysninger
1. Internt	Almindelige personoplysninger	Interne forretningsoplysninger
2. Fortroligt	Fortrolige personoplysninger	Fortrolige forretningsoplysninger
3. Følsomt	Følsomme personoplysninger	Følsomme forretningsoplysninger

SDU kan undtagelsesvis have klassificerede dokumenter jf. sikkerhedscirkulæret (EU/NATO)

- Yderst hemmeligt
- Hemmeligt
- Fortroligt
- Til tjenestebrug

Kun medarbejdere med relevant sikkerhedsgodkendelse, kan få adgang til at håndtere klassificerede dokumenter jf. sikkerhedscirkulæret.

Uddannelse i klassificering af informationer

Alle ansatte skal modtage instruktioner om, hvordan data og dokumenter klassificeres. Retningslinjerne er tilgængelige på SDUnet.

Ansvar for klassifikation

Aktivets ejer har ansvaret for, at aktivet er klassificeret.

8.2.2 Mærkning af information

Klassifikationsmærkning

SDU's informationer og data klassificeres i henhold til Retningslinjer for Dataklassifikation. I nogle tilfælde gives en samlet klassifikation for alle data i et system eller en proces. I andre tilfælde mærker SDU mapper og dokumenter, hvor det er relevant, og hvor der fx kan ske en teknisk understøttelse af sikkerhedsniveauet ved

opbevaring. Et eksempel kan være blokering af data kan deles med eksterne i et fortroligt SharePoint- eller teamwebsted.

Forretningsgangen for beskyttelse af datamediers indhold skal omfatte:
Klar mærkning af alle kopier.
Adgangsbegrænsning.
Fysiske krav til opbevaringssted, f.eks. temperatur og luftfugtighed ifølge leverandørens specifikationer.
Minimering af distribution.

8.2.3 Håndtering af aktiver

Beskyttelse af klassificerede data ved lagring
Data behøver ikke være krypterede ved lagring on-premise, men skal beskyttes via adgangskontrol svarende til datas klassifikation.
Fortrolige og følsomme oplysninger, der hostes eksternt af tredjepart, skal som udgangspunkt opbevares krypteret.

Procedurer for informationsudveksling
De retningslinjer og procedurer, der definerer hvorledes SDU's data skal håndteres, er beskrevet i dokumentet "Sikkerhedsklassificering af data på SDU". Denne retningslinje er under revision så klassifikationen tilpasses de klassificeringstrin, der er beskrevet i "Retningslinjer for dataklassifikation".

Tyveri eller bortkomst af mobilt udstyr
Medarbejderen er ansvarlig for, at SDU-enheder samt privat udstyr, der undtagelsesvis anvendes til behandling af SDU's informationer, opbevares på forsvarlig vis.
Servicedesk skal kontaktes straks, i tilfælde af tyveri/bortkomst af enheden.
SDU IT skal sikre, at informationer på bortkommet mobilt udstyr kan slettes (wipes).

8.3 Mediehåndtering

8.3.1 Styring af flytbare medier

Der skal implementeres procedurer til styring af flytbare medier i overensstemmelse med dataklassifikationen.

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.

Brug af datamedier

Al lokal håndtering af datamedier er dataejerens ansvar.

Alle SDU administrerede computere er monitoreret og følger CIS benchmarks. Det er ikke tilfældet med eksterne harddisk eller USB-sticks. Disse må derfor ikke bruges til at opbevare persondata, men alene til at flytte data. Eksterne harddisk skal krypteres før flytning af persondata, og persondata skal slettes straks efter flytningen.

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.

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".

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

Virusscanning af mobile datamedier

Inden ibrugtagning skal brugeren sikre, at ethvert datamedie er scannet for virus, hvis det har været i brug på eksternt udstyr. Med datamedie menes f.eks. transportable hukommelsesenheder, transportable drev, cd'er, dvd'er, og USB-stiks.

Brug af bærbare medier til fortrolige data

Fortrolige informationer skal krypteres når de opbevares eller transporteres på bærbare medier, f.eks. USB-hukommelse, håndholdt computer, 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.

Opbevaring af fortrolige informationer på privat udstyr

Der må som udgangspunkt ikke behandles eller opbevares fortrolige informationer på udstyr, der ikke tilhører universitetet. SDU stiller sikker opbevaring til rådighed.
Personligt ejet it-udstyr som fx pc'er, håndholdte computere, bærbare harddiske, memorysticks og lignende må ikke anvendes til kopiering eller opbevaring af fortrolige eller følsomme data.

8.3.2 Bortskaffelse af medier

Bortskaffelse og genbrug af medier
Beholdere med papirmateriale til destruktion skal holdes aflåste.
Alle datamedier skal slettes inden genbrug.
Hvis en ekstern leverandør benyttes til destruktion af SDU's datamedier, skal det sikres at leverandøren efterlever de aftalte sikkerhedskrav.
Harddiske skal sikkerhedsslettes eller destrueres inden bortskaffelse. Dette kan ske i samarbejde med ekstern operatør.
Andre datamedier, f.eks. disketter, cd'er, dvd'er, bånd og USB-sticks, som indeholder fortrolige eller følsomme informationer, skal sikkerhedsslettes eller destrueres inden bortskaffelse.

8.3.3 Transport af fysiske medier

Brug af datamedier
Udstyr eller medier, der indeholder fortrolig information må kun forsendes med sikker kurer, eller via en præcis sporbar leveringsmetode.
Der skal føres en log over medier med fortrolige informationer, som er blevet flyttet fra sikre områder. Loggen skal opbevares og være tilgængelig for revision.

9 Adgangsstyring

9.1 Forretningsmæssige krav til adgangsstyring

9.1.1 Politik for adgangsstyring

Begrænset adgang til informationer

Adgang til systemfunktioner og informationer for brugere og personer med supportfunktioner skal administreres efter princippet: blokering af adgang til alt andet end det, som specifikt er tilladt.

Brugere og medarbejdere med supportfunktioner må kun få adgang til systemfunktioner og informationer, hvis dette er forretningsmæssigt begrundet.

Inddragelse af privilegier ved fratrædelse

Adgangsrettigheder skal inddrages i forbindelse med en medarbejders fratrædelse eller afskedigelse.

Der skal forefindes en liste over fratrådte medarbejdere for de seneste seks måneder.

Proceduren for inddragelse af privilegier skal indeholde en liste over funktioner og personer, der skal informeres i forbindelse med fratrædelsen.

Brugeradministration, outsourcing leverandør

Leverandøren skal følge SDU's regler for brugerstyring.

9.1.2 Adgang til netværk og netværkstjenester

Politik for adgang til netværk og netværkstjenester
Der skal foreligge en beskrevet og opdateret politik for adgang til netværk og netværkstjenester.

Forbindelse til fremmede trådløse netværk
Brugere må forbinde sig til fremmede trådløse netværk.

Styring af netværksadgang
Adgangskontrolsystemet skal som standard være konfigureret til at blokere al anden adgang end den, som er specifikt tilladt.
Der skal implementeres et automatiseret adgangskontrolsystem, som dækker samtlige systemkomponenter.
SDU IT skal ved styring af brugernes netværksadgang sikre imod uautoriseret anvendelse af fælles netværk og hertil knyttede tjenester.

Adgang til applikationer på virksomhedens netværk
Der gives kun adgang til applikationer på internt netværk, som er sikkerhedsgodkendt af SDU IT.

Adgang til trådløse netværk
Brugere skal autentificeres, ved hjælp af et certifikat, før der gives adgang til organisationens trådløse netværk, f.eks. ved hjælp af IEEE 802.1x.

Overvågning af netværk
SDU IT skal have den nødvendige viden og redskaber til overvågning af organisationens netværk, f.eks. til fejlretning samt detektering og sporing af sikkerhedshændelser.

SDU IT er ansvarlig for kontinuerligt at overvåge brugen og sikkerheden af organisationens netværksinfrastruktur. Driftsafdelingen er ansvarlig for identificering, diagnosticering, løsning og rapportering af hændelser, samt for samarbejde med andre interessenter.
SDU IT skal løbende overvåge netværk med henblik på detektering af brud på sikkerheden.
SDU IT skal årligt udføre evalueringer af regler for netværkstrafik i firewalls og routere.

Autentificering ved adgang til netværket
Fjernadgang til det interne netværk skal beskyttes ved hjælp af VPN med individuelle certifikater.
To-faktor autentifikation skal benyttes ved fjernadgang til det interne netværk.

Retningslinjer for brug af netværkstjenester
SDU IT Operations har ansvaret for, at der findes en fortegnelse over de netværk og tjenester, der må tilgås.
Brugere skal kun have adgang til de tjenester, de er autoriseret til at benytte.

9.2 Administration af brugeradgang

9.2.1 Brugerregistrering og -afmelding

Identifikation og autentifikation af brugere
Der skal benyttes en passende autentifikationsteknik til verifikation af brugernes identitet.
Alle brugere skal have en unik identitet til personlig brug.
Brugeridentiteten skal kunne spores til den person, som er ansvarlig for en given aktivitet.
Der må ikke anvendes fælles adgangskoder eller brugerprofiler, medmindre dette er forretnings- eller driftsmæssigt nødvendigt, og skal i så fald godkendes af systemejeren og dokumenteres.
Der må ikke forekomme genanvendelse af bruger-id.

Kompromittering af bruger-id til behandling af personhenførbare oplysninger
Der skal forefindes en beskrivelse af, hvordan der tages hånd om den situation, hvor en konto, som benyttes til behandling af personhenførbare oplysninger, kompromitteres. [27701:6.6.2.1]

Identifikation af brugerprofiler for eksterne brugere
Bruger-id skal udarbejdes efter en standard-navnekonvention. Dette gælder også for gæster, konsulenter og lignende således, at disse let kan identificeres.
Eksterne brugerprofiler skal, gennem konsistent navngivning, være tydeligt adskilt fra fastansatte medarbejderes brugerprofiler.

Fratrædelse
Når ansættelse eller midlertidige kontrakter ophæves, skal alle tilknyttede rettigheder trækkes tilbage. Id-kort og lignende skal afleveres, og it-udstyr skal inddrages inden sidste lønning udbetales.
Ved fratrædelse skal alle brugerprofiler og systemrettigheder for brugeren øjeblikkeligt nedlægges.

Brugeradministration, cloudløsning

Organisationen skal sikre at der er etableret procedurer, der sikrer at der er tilstrækkelig brugerstyring, herunder at der sker nedlukning ved afsked og at der nødprocedurer for lukning af 'bad leavers'.
Organisationen skal sikre at der er sporbarhed, så det er muligt at kunne logge brugeres adgang til klassificerede informationer.

Gennemgang af brugerprofiler

Alle brugerprofiler skal gennemgås mindst én gang årligt for at identificere inaktive profiler eller tilsvarende, der skal fjernes eller ændres.
Eksterne krav kan nødvendiggøre hyppigere gennemgang. [27701:6.6.2.1]

Dataansvarliges brugeradministration i systemer, hvor SDU er databehandler

Der skal forefindes dokumentation eller procedure for brugeradministration i løsninger, hvor en dataansvarlig, der benytter SDU som databehandler, selv håndterer brugeridentiteter. [27701:6.6.2.1]

9.2.2 Tildeling af brugeradgang

Registrering af brugere

Systemejer skal autorisere brugeradgang.
It-afdelingen skal vedligeholde fortegnelser over, hvordan bruger-id eller rettigheder fjernes eller ændres ved ophør eller ændring af brugeres jobfunktion.
Der skal ske en verifikation af, at rettighedsniveauet er i overensstemmelse organisationens generelle sikkerhedsretningslinjer.
Serviceleverandører skal anvende tilsvarende eller samme autorisationsprocedure som SDU.
Procedurer for autorisation af brugeradgang skal omfatte en formel autorisationsformular i hvilken de nødvendige privilegier specificeres.

Brugerprofiler for konsulenter og deltidsansatte

Midlertidigt personale tildeles ikke normalt adgang til it-systemerne. Begrænset adgang kan tildeles efter godkendelse fra systemejer.

Processerne for tildeling af adgangsrettigheder skal indeholde:

Kontrol af, om de ønskede adgangsrettigheder er i overensstemmelse med SDU's behov.
Hvordan brugere eller brugerrettigheder fjernes eller ændres ved ophør af eller ændringer i brugeres jobfunktioner.
Kontrol af, om de ønskede adgangsrettigheder på nogen måde er i strid med kravet om funktionsadskillelse.
Kontrol af, om adgangsrettigheder er i overensstemmelse med klassificeringen af oplysningerne.
Kontrol af, at der kun autoriseres adgang til personoplysninger fra personlige bruger-id.
Kontroller der sikrer, at der ikke sker brud på relevant lovgivning og kontrakter ved disse adgangsrettigheder.

Medarbejderes omplacering

Ved ændringer af roller for medarbejderne skal rettigheder og privilegier revurderes. Dette gælder især for forretningskritiske systemer

9.2.3 Styring af privilegerede adgangsrettigheder

Formel godkendelsesproces

Der skal foreligge en formel godkendelsesproces for tildeling af privilegerede adgangsrettigheder.
Det må ikke tildeles privilegerede adgangsrettigheder før godkendelsesprocessen er tilendebragt.

Fortegnelse over privilegerede adgangsrettigheder

Der skal forefindes en fortegnelse over alle identificerede, privilegerede adgangsrettigheder i alle systemer og applikationer.

Skift af administratoradgangskode ved fratrædelse

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

Tildeling af brugerrettigheder

Systemejer for et it-system bestemmer nødvendige brugerrettigheder for systemet.
SDU IT tildeler brugerrettigheder via AD. På nogle systemer forestås brugeradministrationen af den operationelle systemejer efter relevant godkendelse.

Administration af privilegier

Administratorkonti må ikke benyttes til ikke-administrative opgaver.
Konti med administrative rettigheder skal tildeles til særskilte og personlige bruger-id.
Anvendelse af administratorkonti skal logges.

Udvidede adgangsrettigheder

Der skal benyttes særlige brugeridentiteter til de udvidede rettigheder af hensyn til overvågning og opfølgning.
De udvidede adgangsrettigheder skal registreres.
De udvidede adgangsrettigheder må kun tildeles i begrænset omfang og alene ud fra et arbejdsbetinget behov.

Kompetencer

Kompetencerne hos brugere med privilegerede adgangsrettigheder skal gennemgås regelmæssigt for at verificere, at de er i overensstemmelse med deres opgaver.

Opbevaring af adgangskode til administrativ adgang

Særlige kritiske adgangskoder til administrativ adgang skal opbevares i forseglet kuvert i aflåst og brandsikkert pengeskab.

Ændring af administrative adgangskoder
Administrative adgangskoder skal ændres hvis udenforstående får kendskab til disse, herunder hvis administratorer forlader organisationen.
Se i øvrigt afsnit 9.3.1 Brug af hemmelig autentifikationsinformation.

9.2.4 Styring af hemmelig autentifikationsinformation om brugere

Overdragelse af adgangskode
Midlertidig hemmelig autentifikationsinformation skal gives så den ikke kan opsnappes af uvedkommende. Fx må adgangskoder ikke overdrages på ukrypterede forbindelser, f.eks. e-mail. Adgangskoder kan overdrages verbalt, også f.eks. over telefonen.

Retningslinjer for adgangskoder
SDU IT skal etablere og vedligeholde en procedure for tildeling af midlertidige adgangskoder.
SDU IT skal etablere og vedligeholde en procedure for, hvordan en brugers identitet fastslås, før en ny midlertidig adgangskode må udleveres.
Midlertidige adgangskoder skal være unikke, må ikke genbruges og skal opfylde de almindelige krav til adgangskoder.
Ved brugeroprettelse eller nulstilling af adgangskode skal brugere tildeles en sikker, midlertidig adgangskode, som skal ændres umiddelbart efter første anvendelse.
Standard-autentifikationsinformation fra leverandører skal ændres.

9.2.5 Gennemgang af brugernes adgangsrettigheder

Gennemgang af administrativ adgang
Autorisationer og privilegerede adgangsrettigheder til brugere med administrativ adgang skal gennemgås hver 3. måned (oftere end normale brugere).
Dette skal ligeledes skal øjeblikkeligt ved ændringer i ansættelsen; i særdeleshed ved ændring af jobfunktion.
Ændringer i autorisationer til privilegerede adgangsrettigheder skal logges og gennemgås regelmæssigt.

9.2.6 Inddragelse eller justering af adgangsrettigheder

Medarbejderes omplacering
Ved omplacering af medarbejdere skal alle rettigheder for pågældende bruger revurderes.

Inddragelse af privilegier ved fratrædelse

Der skal forefindes en opdateret procedure for inddragelse af privilegier i forbindelse med fratrædelse eller afskedigelse af personale.
Proceduren for inddragelse af privilegier skal indeholde en liste over funktioner og personer, der skal informeres i forbindelse med fratrædelsen.

Område eller sekretariatschefen kan træffe særskilt beslutning om, hvornår en fratrådt medarbejder skal udelukkes helt fra - fysisk og logisk - at anvende SDU's it-aktiver. Udelukkelsen skal dog ske indenfor maksimalt 3 måneder, medmindre medarbejderen stadig har særlige arbejdsopgaver for SDU. Hvis der er behov for at en tidligere medarbejder fortsat har adgang til et system efter ansættelsens ophør skal denne underskrive en fortrolighedserklæring.

Når en systemadministrator eller lignende fratræder, skal der omgående skiftes kodeord på alle systemer, som den pågældende havde adgang til.

9.3 Brugernes ansvar

9.3.1 Brug af hemmelig autentifikationsinformation

Valg af sikre adgangskoder
Aktuelt er det vurderingen, at længden af kodeordet er den væsentligste faktor i forhold til, hvor sikker en adgangskode kan betragtes. SDU følger med i udviklingen på området og justerer løbende vores regler i henhold til understående. Derfor kan der ske løbende tilpasninger som udmøntes i retningslinjer på SDUnet.

Lagring af adgangskoder
Adgangskoder må aldrig lagres elektronisk i klartekst og må heller ikke noteres på papir. Det er tilladt at benytte programmer som beskytter kodeord og forenkler anvendelse af forskellige kodeord til forskellige formål. SDU IT vedligeholder en liste af accepterede password managers. Det er ikke tilladt at anvende private passwords managers til opbevaring af passwords relateret til ansættelsen på SDU. Som udgangspunkt skal der benyttes multifaktorautentifikation (MFA) og single sign-on, hvor det er muligt.

Krav til længde af adgangskode
Adgangskoder skal indeholde mindst 15 tegn på almindelige brugerkonti (krav ved dannelse af nye kodeord). Management konti, der giver adgang til servere fx sa-konti skal indeholde mindst 18 tegn. Service-konti, der bruges til applikationsdrift, skal om muligt være en gMSA-konti (indbygget teknologi i Windows og Windows Servere), hvor der ikke direkte bliver benyttet et kodeord. Såfremt det ikke kan lade sig gøre er kravet minimum 25 tegn.

Krav til indhold af adgangskode
Adgangskoder skal indeholde kombinationer fra mindst tre af følgende kategorier: store bogstaver, små bogstaver, tal og specialtegn. Adgangskoder må ikke indeholde delstrenge (længere end 3 tegn) fra brugerens

fornavn, efternavn og brugernavn. Fx må "risti" ikke forekomme, hvis man hedder Christian. Det er heller ikke tilladt at bruge ofte anvendte tastaturvandringer af tal eller bogstaver på et tastatur (fx 12345678, 123qweasd eller qwerty). Der kan løbende tilføres flere regler om kodeords kompleksitet, såfremt det vurderes at være passende og nødvendige sikkerhedstiltag.

Genbrug af adgangskode
En bruger kan ikke vælge en adgangskode, der er identisk med brugerens 25 seneste anvendte adgangskoder. Medarbejderne må ikke anvende samme adgangskode til organisationens infrastruktur som til adgang til tredjeparts udstyr, f.eks. internet-websteder og netbanker. Omfattende brug af samme adgangskode på tredjepart-systemer øger sandsynligheden for, at adgangskodens fortrolighed kompromitteres.

Krav til skift af adgangskode
Adgangskoder skal skiftes, når SDU's tjek af kodeord har identificeret kodeordet som kompromitteret eller svagt.
SDU tjekker kodeord ved brug af specialsoftware og databaser. Såfremt et kodeord kan knækkes inden for 48 timer, bliver brugeren anmodet om at skifte sit kodeord.
Kodeord bliver altid tjekket ved skift af kodeord, og efter behov når SDU modtager information om lækkede kodeord fra eksterne kilder og portaler. Derudover tjekkes styrken af alle kodeord halvårligt.
SDU kræver på grund af ovenstående foranstaltninger ikke periodisk skift af kodeord. Det er derved kun brugere, der vurderes at have et usikkert kodeord, der bliver bedt om at skifte det.

Brug af autologin funktioner
Automatiseret log-in til systemer og applikationer må som udgangspunkt ikke anvendes og aldrig på enheder, der er til personligt brug. Pc'er med specifikke formål og/eller begrænset adgang er undtaget herfra. Det gælder fx såkaldte "kiosk maskiner" eller pc'er, der er til fri afbenyttelse fx på biblioteket.

Adgangskoder er strengt personlige
Adgangskoder er strengt personlige og må ikke deles med andre. Ved mistanke om at andre kender kodeordet, skal dette straks ændres alle de steder, hvor det benyttes.

9.4 Styring af system- og applikationsadgang

9.4.1 Begrænset adgang til informationer

Adgang til data på SDU's netværk
Ved fjernadgang til data på SDU's netværk, må der ikke gemmes data på lokale harddiske eller andre eksterne medier.

Adgang til funktionalitet og data i forretningssystemer
Informationssystemer skal overholde SDU's adgangskontrolpolitik.

Politikken for adgangskontrol på de enkelte systemer skal baseres på en risikovurdering og på de forretningsmæssige behov.
Det skal altid vurderes, hvilke data og applikationer, hvilke bruger bør have adgang til, herunder hvilke rettigheder (læse, skrive, redigere, slette) hvilke brugere skal have.

Andre applikationers adgangsrettigheder
Hvor en applikation skal have adgang til data, skal det altid vurderes, hvilket adgangsrettigheder denne applikation har brug for og begrænse dem til de allermest nødvendige.

Adgang til medarbejderes data og mail ved langtidsfravær
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.

Begrænsning i uddata
Det skal altid vurderes, hvordan uddata skal begrænses.

9.4.2 Procedurer for sikkert log-on

Automatiske afbrydelser
Funktioner i et informationsbehandlingssystem, der ikke har været aktivt i et fastlagt tidsrum, skal automatisk afbrydes.

Sikre login-procedurer skal som udgangspunkt indbefatte:

- At data fra systemet eller applikationen ikke vises ved login.
- Vise en advarsel om, at kun autoriserede brugere kan få adgang til systemet.
- Begrænsning af oplysninger, der kan benyttes af en uautoriseret bruger i forbindelse med login.
- Beskyttelse mod brute-force loginforsøg.
- Logning af succesfulde loginforsøg.
- Logning af mislykkede loginforsøg.
- At indtastede adgangskoder ikke vises.
- At der ikke sendes adgangskoder i klartekst over netværk.

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

SDU som serviceudbyder
Hvis SDU udbyder en tjeneste, hvor kunderne administrerer egne brugere, skal det sikres, at de kan logge ind på en sikker måde.

9.4.3 System for administration af adgangskoder

Implementering af et system til håndtering af adgangskoder

For at håndhæve SDU's regler for adgangskoder, skal der implementeres et system til håndtering af adgangskoder for samtlige systemer.

- Adgangskodesystemerne bør sikre, at der anvendes personlige bruger-id og adgangskoder.
- Adgangskodesystemerne bør sikre, at adgangskoderne opfylder kvalitative krav til udformning.
- Adgangskodesystemerne bør kræve skift af adgangskode ved første log-in.
- Adgangskodesystemerne bør lagre og transmittere adgangskoder i krypteret form.
- SDU IT sikrer med jævne mellemrum, at kodeordet er tilstrækkeligt stærkt og ikke kendes af andre (fx eksterne fortegnelser over ID og kodeord).

9.4.4 Brug af privilegerede systemprogrammer

Brug af systemværktøjer

It-afdelingen skal begrænse og styre adgangen til systemværktøjer, f.eks. utilities, der kan påvirke eller omgå systemers eller enheders sikkerhed.

Al brug af systemværktøjer skal logges.

Der skal være en procedure for autorisation ved ad hoc anvendelse af systemværktøjer.

Ubenyttede systemprogrammer skal fjernes.

Hvor funktionsadskillelse er påkrævet, må brugere ikke have adgang til både systemværktøjer og brugersystemer.

9.4.5 Styring af adgang til kildekode til programmer

Adgangskontrol for kildetekst

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

Kontrolleret adgang til kildekode

Kildekode må som udgangspunkt ikke opbevares i driftsmiljøet.

Kildekoden til udviklingsprojekter skal sikres mod uautoriseret adgang. Ændringer skal kontrolleres for at sikre integritet. Dette gælder især kritiske applikationer.

Alle adgange til kildebibliotekerne skal logges.

10 Kryptografi

10.1 Kryptografiske kontroller

10.1.1 Politik for anvendelse af kryptografi

Kryptering og andre kryptografiske metoder bliver som udgangspunkt anvendt og konfigureret i forhold til Best-practices for hærdning af software komponenter. Dette sker eksempelvis via CIS benchmarks.

Standard teknologier og software bliver anvendt til at implementere kryptografi.

Softwarepakker bliver opdateret i henhold til vores standardprocedurer.

Kryptografiske metoder bliver anvendt til at beskytte data fortrolighed og integritet i alle relevante områder. Det gælder blandt andet kryptering af trafik og kryptering af lagret data. Det gælder også andre kryptografiske metoder, eksempelvis hash funktioner, som blandt andet bliver brugt til at sikre autentificering.

10.1.2 Administration af nøgler

Nøglehåndtering
Procedurer for nøglehåndtering skal beskrive hvordan uautoriseret udskiftning af nøgler forhindres samt hvordan opdeling af samlet kendskab til nøgler på to eller tre personer (split knowledge) foregår.
Adgang til krypteringsnøgler skal begrænses til færrest mulige nøgleforvaltere/kustoder.
SDU IT eller den operationelle systemejer skal etablere et nøglehåndteringssystem, som understøtter organisationens s anvendelse af kryptografi.
Proceduren for nøglehåndtering skal beskrive hvordan generering, distribution, opbevaring og destruktion af nøgler håndteres.
Proceduren for nøglehåndtering skal beskrive hvordan tilbagekaldelse af gamle eller ugyldige nøgler håndteres.
Proceduren for nøglehåndtering skal beskrive, hvordan periodisk skift af krypteringsnøgler skal foregå.
Udskiftning skal ske mindst en gang om året eller som anbefalet i forbindelse med konkret anvendte applikationer.

11 Fysisk sikring og miljøsikring

11.1 Sikre områder

11.1.1 Fysisk perimetersikring

Overvågning i sikre områder
Videokameraer, som benyttes til overvågning af sikre områder, skal placeres inden for det sikre område eller på anden vis beskyttes mod modifikationer og deaktivering.
SDU IT skal sørge for at arbejde i sikre områder overvåges.
Videooptagelser fra sikre områder skal opbevares i en måned.

Oplysninger om sikre områder

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

Indbrudsalarmer

SDU skal anvende passende alarmsystemer baseret på risikovurderinger.

11.1.2 Fysisk adgangskontrol

Adgang til datacenter, herunder serverrum, hovedkrydsfelter og it-klargøringsrum

Adgangen beskyttes på en måde, så det sikres, at kun medarbejdere med et fagligt ærinde, kan slå alarmsystemet fra og få adgang til rummet fx ved hjælp af medarbejderkort, PIN-kode og brik. En lidt bredere kreds af medarbejdere (Teknisk Service og rengøring) kan have adgang men vil udløse alarmsystemet, der tilkalder vagten.

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, men kan vælge at uddelegere opgaven til f.eks. chefen for IT Operations.

Private og særlige sikkerhedsområder 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.

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.

Brug af personlige adgangskort

Personers adgang til og ophold i sikkerhedsområder (halvprivate, private og særlige) skal registreres og kontrolleres i henhold til reglerne i SDU's ISMS.

Medarbejdere skal bære deres id-kort eller adgangskort synligt på universitetets særlige sikkerhedsområder.

Brik skal udleveres mod kvittering. Modtageren af brik og adgangskort 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 brik, nøgle og/eller adgangskort.

Personale, der fratræder, skal have deres adgangsmuligheder inddraget.

Det skal sikres, at adgangsrettigheder og logs over adgange kontrolleres jævnligt.

11.1.3 Sikring af kontorer, lokaler og faciliteter

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.

SDU's elektroniske overvågning baseres generelt på skalovervågning og rumovervågning. Den elektroniske overvågning skal give alarm til (vagt)personale, der kan reagere på alarmen døgnet rundt.

Ansvar for den fysiske adgangskontrol

Områdechefen for Teknisk Service har det overordnede ansvar for administration af den fysiske adgangskontrol, f.eks. nøgleadministration til kontorer og it-områder, men opgaven er typisk uddelegeret til SDU's organisatoriske enheder. SDU IT skal sikre en årlig kontrol af fysisk adgang til it-områder.
Der skal være kontrol af fysisk adgang til universitetets faciliteter. Dette ansvar delegeres til betroede medarbejdere i organisationen, f.eks. sikkerhedsvagter.

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 ISO 27002:2014, betragtes som offentligt sikkerhedsområde dvs. "at det kun i begrænset omfang er muligt at kontrollere personers adgang". Bygningsskallen er i princippet aflåst i tidsrummet hverdage kl. 20-07 samt i weekend, helligdage, men som følge af forskellige retningslinjer på SDU's lokationer, arrangementer om aftenen og i weekends må bygningsskallen generelt betragtes som ikke aflåst i relation til nærværende sikkerhedsforskrift. Når bygningerne er aflåst, foregår adgang for autoriserede brugere via adgangskontrol-systemet.

Gæsters adgang

Gæster må ikke lukkes ind i sikrede områder, medmindre tilladelse til dette er indhentet af den relevante ansvarlige.
Eksterne leverandører tillades at færdes i sikre zoner, når det er registreret, at disse har modtaget nødvendig instruktion.
Gæster må færdes frit på universitetets offentlige områder.

Oplysninger om sikre områder

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

11.1.4 Beskyttelse mod eksterne og miljømæssige trusler

Miljømæssig sikring af serverrum

Serverrum, krydsfelter og tilsvarende områder skal på forsvarlig vis sikres mod miljømæssige hændelser som brand, vand, eksplosion og tilsvarende påvirkninger.

Forsyningssikkerhed

Områdechefen for Teknisk Service har ansvaret for, at alle forsyninger til serverrum som elektricitet, vand, kloak, varme, og ventilation har den nødvendige kapacitet, og løbende inspiceres for at forebygge uheld, der kan have indflydelse på informationsaktiverne.
Data- og telekommunikationsforbindelser skal etableres via minimum to adgangsveje for forretningskritiske systemer.

Brandsikring

Serverrum må ikke benyttes som lager for brændbare materialer.
Serverrum skal sikres med veldimensioneret brandslukningsudstyr.

11.1.5 Arbejde i sikre områder

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. Sabotage af sikringsanlæg giver ikke adgang til sikrede områder.
Nøgle- og låsesystemer skal være konstruerede så de yder beskyttelse mod uautoriseret adgang til lokaliteter med adgangsbegrænsning.

Kameraer

Der må ikke fotograferes i universitetets særlige sikkerhedsområder uden tilladelse frachefen for SDU IT eller SDU IT Operations.

Overvågning i sikre områder

Teknisk Service skal sikre at arbejde i sikre områder så vidt muligt bliver overvåget.
Se SDU's Sikringspolitik

Optageudstyr i sikre områder

Uautoriseret optageudstyr er ikke tilladt i sikre områder.

Aflåsning af lokaler og bygninger
Alle døre og vinduer skal kunne låses forsvarligt.

11.1.6 Områder til af- og pålæsning

Af- og pålæsningsområder
Af- og pålæsningsområder skal indrettes, så risiko for uautoriseret adgang til organisationens øvrige områder mindskes.
Adgang til af- og pålæsningsområder må kun gives til identificerede og autoriserede personer

Leverandører bør identificeres og autoriseres og kun have adgang til de områder, de er autoriseret til.
Leveret materiale bør inspiceres for farlige materialer og bør registreres.

Der er offentlig adgang til Teknisk Services varemodtagelse ved Killerupvej/Campusvej.
Adgang til SDU IT's forberedelsesrum med adgang fra Campusvej er sikret.

11.2 Udstyr

11.2.1 Placering og 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 datacentre, så 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.

Adgang til serverrum og hovedkrydsfelter
Adgang til serverrum og hovedkrydsfelter tillades kun udvalgt personale fra SDU IT eller efter nødvendig instruks i adfærd.
SDU IT afgør specifikt, hvem der skal have adgang.

Spisning og rygning i nærheden af udstyr
Der må ikke ryges i serverrum.
Der må ikke spises og drikkes i nærheden af forretningskritisk udstyr.
Der må ikke spises og drikkes i serverrum.

Distribueret it-udstyr
Alle krydsfelter, afdelings-serverrum og lignende faciliteter med delt it-udstyr skal aflåses for at hindre uautoriseret adgang til disse.

Aflåsning af hovedkrydsfelter og lignende teknikrum
Alle krydsfelter og andre teknikrum skal være aflåste.

11.2.2 Understøttende forsyninger (forsyningssikkerhed)

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
Alle server-systemer skal beskyttes med nødstrømsanlæg til at sikre hurtig og korrekt system-nedlukning i tilfælde af strømudfald.

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 linjer, 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 elforsyning 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.

Sikring af udstyr uden for universitetets overvågning
Eksternt placeret it-udstyr som hjemmeudstyr og mobile enheder, 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.

11.2.3 Sikring af kabler

Sikring af kabler

Kabler og tilhørende udstyr til elforsyning 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.

11.2.4 Vedligeholdelse af udstyr

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 (masterdata).

11.2.5 Fjernelse af aktiver

Udstyr må kun fjernes fra SDU, hvis der foreligger en underskrevet kvittering på det udleverede.

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

Udlån af udstyr skal så vidt muligt være tidsbegrænset.

11.2.6 Sikring af udstyr og aktiver uden for organisationens lokaler

Opsyn med mobile enheder

Mobile enheder må ikke efterlades uden opsyn i uaflåste rum.

Adgang til data på bærbare computere skal være under adgangsbeskyttelse.

Udstyr med fortrolige forretningsoplysninger eller personoplysninger skal anvende harddisk-kryptering.

Mobile enheder må ikke efterlades uden opsyn under transport.

Bærbare enheder bør medbringes i håndbagagen på rejser.

Tyverimærkning af it-udstyr

It-udstyr tyverimærkes, hvor det findes relevant. Der tages bæredygtighedshensyn, hvor udstyr kan genanvendes.

Fjernarbejdspladser
Enheder skal opbevares på en måde så uvedkommende ikke kan få adgang til udstyr og aktiver.

11.2.7 Sikker bortskaffelse eller genbrug af udstyr

Alt it-udstyr, der indeholder lagermedier skal kontrolleres før fjernelse for at sikre, at alle følsomme og fortrolige data tillige med licenserede og egne brugerprogrammer er slettet.

Denne kontrol kan dokumenteres med rapport fra scrubbing-partner, hvor it-udstyret sendes til genanvendelse.

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.

Kasserede (flytbare) datamedier skal destrueres af renovationspartner under en aftale om destruktion af materiale med følsomme og fortrolige informationer.

11.2.8 Brugerudstyr uden opsyn

Uovervåget udstyr
Data der er lagret på uovervågede arbejdsstationer (stationære og bærbare) betragtes i sikkerhedsmæssig henseende som offentligt tilgængelige medmindre 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 logoff 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.

11.2.9 Politik for ryddeligt skrivebord og blank skærm

Brug af adgangskodebeskyttet pauseskærm
Adgangskodebeskyttet skærmlås skal aktiveres på pc-arbejdspladser efter 30 minutters inaktivitet.

Opbevaring af fysiske dokumenter

Dokumenter med personhenførbare oplysninger må ikke ligge tilgængelig for uvedkommende.
Dokumenter med personhenførbare oplysninger skal opbevares i aflåst skab eller skuffe efter arbejdstid.
Fortrolige dokumenter skal opbevares i aflåst skab eller skuffe.

Print af følsom og fortrolig information

Behandling af personoplysninger på fysiske medier skal begrænses mest muligt.
Print af følsom og kritisk information skal ske via kopimaskiner med adgangskontrol.

12 Driftssikkerhed

12.1 Driftsprocedurer og ansvarsområder

12.1.1 Dokumenterede driftsprocedurer

Driftsansvar

SDU IT er ansvarlig for drift og administration af fælles it-systemer samt disses sikkerhed. Dette inkluderer efterlevelse af sikkerhedspolitikker, regler og procedurer. SDU IT er ligeledes ansvar for administration af operativsystemet af udleverede arbejdsstationer.
Systemejerskab og driftsansvar er nærmere beskrevet i systemforvaltningsaftaler.

Sikring af arbejdsstationer inden ibrugtagning

Alle arbejdsstationer skal installeres ved brug af den af SDU IT fastlagte procedure.
Alle arbejdsstationer skal sikres inden brug. Minimum sikring inkluderer installation af seneste sikkerhedsrettelser for operativsystemet, screening ved hjælp af sikkerhedsanbefalingerne CIS og antivirusprogram.
SDU's 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.

Deaktivering af beskyttelsesmekanismer

Det er ikke tilladt at deaktivere eller omgå universitetets beskyttelsesmekanismer, medmindre andet er aftalt med it-chefen og samtidigt dokumenteret.

Sikkerhed i systemplanlægning

Ved planlægning af systemer skal sikkerhedsbetragtninger altid medtages i overvejelserne.
Konfigurationsstandarder for samtlige systemkomponenter skal kunne håndtere alle kendte sårbarheder og være overensstemmende med branche-accepterede standarder for hærdning af systemer.

It-sikkerhedskrav skal tages i betragtning ved design, aftestning, implementering og opgradering af it-systemer samt ved systemændringer.
Alle systemer skal gennemgås ved brug af CIS benchmarks. Systemer, som håndterer følsomme persondata skal som minimum overholde CIS18 controls 1-4 og 18.
Inden ibrugtagning skal driftsafviklingssystemer, netværk og brugersystemer afprøves. Testen skal godkendes af systemejeren.
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 systemejer og dataejer. Produktionssystemerne ændres/opgraderes og afprøves med så få ulemper for brugerne som muligt.

Driftsafviklingsprocedurer
Driftsafviklingsprocedurer for forretningskritiske systemer skal være dokumenterede, ajourførte og tilgængelige for driftsafviklingspersonalet og andre med et arbejdsbetinget behov.
Operationelle procedurer skal indeholde installationen, konfiguration af systemer samt en beskrivelse af, hvordan databehandling håndteres manuelt og automatiseret (services og batch jobs).
Operationelle procedurer skal omfatte krav til og konfiguration af log, backup, job-schedulering, sæsonafhængige oppetidskrav, sikkerhedskonfigurationer og instruktioner til håndtering af fejl.
Driftsprocedurer skal omfatte beskrivelser af genopretnings- og retableringsprocedurer samt konfiguration af overvågnings- og revisionsspor (audit).

Sikring af serversystemer
Alle serversystemer skal sikres til et baseline niveau fastsat af SDU IT.
Denne sikring omfatter at pålægge serverne et sikret sæt politikker baseret på *best practice*.
Alle servere skal hærdes gennem deaktivering af unødvendige og usikre services og protokoller.
Alle systemkomponenter skal hærdes ved at styre den lokale firewall til kun at tillade den nødvendige trafik, fra hvor det er nødvendigt.

Registrering af driftsstatus
SDU IT er ansvarlig for at identificere, logge og håndtere hændelser og afvigelser i driften af de it-systemer de er ansvarlige for.
Der skal registreres væsentlige forstyrrelser og uregelmæssigheder i driften af systemerne samt årsager hertil.

12.1.2 Ændringsstyring

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.

- Små ændringer kan besluttes alene af en IT-medarbejder.
- Lidt større ændringer kan besluttes af en teamleder.

- Større ændringer kan besluttes af afdelingsleder eller områdeleder.

Systemer skal sikkerhedsgodkendes før de tages i brug jf. "Retningslinjen for sikkerhedsvurdering af it-systemer ved indkøb og udvikling". Kravet til dokumentation og risikovurderinger afhænger af systemets kritikalitet og hvilke typer oplysninger systemet skal behandle.
Systemejeren kan opstille særskilte krav til 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.

Ændringsstyring
Ændringsønsker (request for change, RFC) og deres videre skæbne skal noteres i en ændringslog.
Der skal vedligeholdes en versionsstyring for alle systemændringer.
Eventuelle konsekvenser for de registrerede skal vurderes.
Der skal indhentes en formel godkendelse af større ændringen, før arbejdet med den går i gang.
Der skal vedligeholdes et kontrolspor for alle ændringer.
Driftsdokumentation og forretningsgange for brugerne skal holdes opdateret, således at de stadig er gældende efter ændringen.
Ved ændringer skal der foregå en gennemgang af sikringsforanstaltninger og integritetskontroller for at sikre, at disse ikke forringes ved implementeringen.
Der skal foretages test af driftsfunktionaliteten før ændringer gennemføres i produktionsmiljøet.
SDU IT skal oprette og vedligeholde procedurer for ændringsstyring for alle software- og systemkonfigurationsændringer (inklusive netværksudstyr).
Der skal foretages test af ændringer i netværk, firewall og routere. Det tilstræbes at teste ændringer, hvor det påvirker mindst.
Der skal tilstræbes, at der eksisterer et beredskab/en metode til at rulle ændringerne tilbage i tilfælde af udfordringer.

12.1.3 Kapacitetsstyring

Kapacitetsplanlægning
It-systemernes dimensionering skal afpasses efter kapacitetskrav. Belastning skal overvåges således, at opgradering og tilpasning kan finde sted løbende. Dette gælder især for forretningskritiske systemer.
SDU IT skal have procedurer, der minimerer risikoen for driftsstop som følge af manglende kapacitet.
Der skal være løbende afklaring af forretningsbehov og brugen af ovenstående ressourcer bør følges tæt, så der ikke opstår flaskehalse.
Det skal løbende vurderes, om kapaciteten bruges fornuftigt.

12.1.4 Adskillelse af udviklings-, test- og driftsmiljøer

Sikring af applikationsudviklingsmiljøerne

Udviklingsmiljøer skal sikres mod trusler som uautoriseret adgang, ændringer og tab. Data skal sikres efter klassifikation (kritikalitet/følsomhed).

Adskillelse af udvikling, test og drift

- Der må som udgangspunkt ikke forefindes ægte personoplysninger i udviklings- og testmiljøer.
- Hvis det ikke kan undgås, skal der sikres samme sikkerhedsforanstaltninger i testmiljøet (fx adgangsstyring og log) som i produktionssystemet.
- Når det er muligt, bør der benyttes syntetiske data.
- Fortrolige/følsomme forretningsdata/personoplysninger må ikke kopieres ind i testmiljøet, medmindre der findes tilsvarende kontroller for testsystemet.
- Der stilles ikke krav til adskillelse af drifts- og udviklingsmiljøer for forskningsdata, som ikke indeholder persondata.
- Personer med adgang til flere eller alle miljøer kan udgøre en sikkerhedstrussel, hvis de manipulerer med ændringer til egne formål. Derfor skal der ske adskillelse af personers roller, og deres aktiviteter på systemerne skal logges.
- Brugere skal anvende forskellige brugerprofiler til drifts- og testsystemer, og menuer skal vise passende identifikationsbeskeder for at reducere risikoen for fejl.
- Kompilatorer, editorer og andre udviklingsværktøjer eller systemværktøjer må ikke være tilgængelige fra driftssystemer, når det ikke er påkrævet.
- Til forretningskritiske it-systemer er der oprettet separate udviklings-/testmiljøer, hvor nyudviklede/nyanskaffede faciliteter samt fejlrettelser kan afprøves forinden overførsel eller installation på produktionsmiljøer.
- Der skal ske tests af ændringer inden de sættes i produktion.
- Bortset fra under ekstraordinære omstændigheder må der ikke foretages test på driftssystemer.
- Systemer, hvor der ikke kan opsættes realistiske testmiljøer, skal afprøves indenfor de aftalte service-vinduer.
- Miljøer skal adskilles, og det skal dokumenteres, hvordan ændringer overføres mellem miljøer, og hvem der godkender overførslerne.

12.2 Beskyttelse mod malware

12.2.1 Kontroller mod malware

Malware-beskyttelse på systemer

- IT Operations skal sikre, at der er installeret aktive anti-malware-produkter på samtlige computere i SDU, og at disse opdateres løbende via en central automatisk platform eller højst et døgn efter leverandørens opdateringer.

- Eneste undtagelse er systemer, hvor der er krav om, at der ikke bliver ændret på fx laboratorieudstyr. Infrastrukturen skal så til gengæld skærmes mod dette udstyr, og det skal overvejes, om det overhovedet skal sluttes til netværket.
- Der skal fastlægges en politik, som håndterer enheder, der ikke er på netværket (fx hjemmearbejdspladser eller mobile enheder, som sjældent sluttes direkte til organisationens netværk).
- Der skal fastlægges en politik, som forhindrer brugen af uautoriseret software (se 12.6.2 og 14.2).
- Der skal implementeres kontroller, som forhindrer eller sporer brugen af uautoriseret software (fx hvidlisting af applikationer).
- Der skal ske blokering af kendte ondsindede sider på internettet.
- Der skal fastlæggelse en formel politik for at beskytte mod risici forbundet med at få filer eller software fra eller via eksterne netværk eller på andre medier med angivelse af, hvilke beskyttelsesforanstaltninger der bør tages.
- Begrænsning af sårbarheder, som ville kunne udnyttes af malware, fx gennem styring af tekniske sårbarheder (se 12.6).
- Regelmæssig gennemgang af software og dataindhold i systemer, der understøtter kritiske forretningsprocesser; tilstedeværelsen af ikke-godkendte filer eller uautoriserede ændringer bør undersøges formelt.
- Installation og regelmæssig opdatering af malwaresporings- og reparationssoftware til at scanne computere og medier som en forebyggende kontrol eller rutinemæssigt; den udførte scanning bør omfatte,
    - at scanne filer, som modtages over netværk eller via anden form for lagringsmedie, for malware inden brug,
    - at scanne elektronisk vedhæftede og downloadede filer for malware inden brug; denne scanning bør udføres forskellige steder, fx på elektroniske mailservere, desktop computere, og når der skaffes adgang til organisationens netværk,
    - at scanne websider for malware.
- Der skal være en proces for at rapportere hændelser med malware og i tilknytning hertil en proces for opsamling af erfaringer med malware i organisationen.
- Som led i den almindelige drift, skal malwareangreb være integreret i beredskabsplaner, backup skal kunne genindlæses, software skal opdateres, så malware ikke kan udnytte kendte sårbarheder, og der skal gennemføres awarenesskampagner om malware – fx *phishing*-angreb.
- Isolering af miljøer, hvor nedbrud kan have katastrofale følger.

12.3 Backup

12.3.1 Backup

Politik for backup

Der skal affattes en politik for backup, som omfatter:

- hvem der er ansvarlig for at tage backup af hvad, hvornår og hvordan og som er ansvarlig for at backuppen virker,
- hvilke data, systemer og software, der tages backup af,
- med hvilken frekvens backuppen skal tages,
- en beskrivelse af at backup placeret et andet sted end hvor originalerne befinder sig,
- beskyttelse af backuppen med passende foranstaltninger,
- test af gendannelse fra backup – dels ved at kontrollere at backup ikke har meldt en fejl og dels ved at kontrollere at data faktisk kan genindlæses,
- hvorvidt der er taget stilling til, hvor systemer og data genindlæses, hvis hardwaren ikke er tilgængelig,
- hvorvidt der er personoplysninger på backup,
- hvorvidt der er taget stilling til, hvordan slettede personoplysningerne i produktionsmiljøet skal slettes, hvis der bliver behov for at genindlæse backup,
- hvorvidt det logges, hvis personoplysninger genindlæses, og af hvem.

Opbevaring af sikkerhedskopier på ekstern lokation

Den fysiske sikkerhed på den eksterne opbevaringslokalitet skal sikres gennem besigtigelse mindst en gang årligt.

Reserveanlæg og -udstyr samt datamedier med sikkerhedskopier skal opbevares i sikker afstand for at undgå skadevirkninger fra et uheld på det primære anlæg.

Datamedier til retablering af forretningskritiske systemer skal opbevares på et, for it-driftsorganisationen, eksternt opbevaringssted.

Backup af systemer og data

SDU IT er ansvarlig for sikker lagring og backup af data på serverudstyr.

Backup skal være nøjagtig, fuldstændig og omfatte dokumenterede restore-procedurer.

Backup-data skal beskyttes med passende logisk og fysisk adgangskontrol.

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

I situationer, hvor fortroligheden er vigtig, bør backupkopier beskyttes ved hjælp af kryptering.

Sikkerhedskopiering af data på andre systemer

Der foretages ikke sikkerhedskopiering af arbejdsstationer.

Brugeren af arbejdsstationen skal sikre, at alle informationer som minimum forefindes på filsystemer, hvor der foretages sikkerhedskopiering.

For udviklings- og testsystemer vurderes til i hvert enkelt tilfælde, om der skal gennemføres sikkerhedskopiering.

Overvågning af procedurer for sikkerhedskopiering

Muligheden for at retablere data fra backup-systemer skal regelmæssigt testes i et testmiljø. Endvidere skal retablering testes efter system- eller proces-ændringer, der kan påvirke backup-rutiner.

12.4 Logning og overvågning

12.4.1 Hændelseslogning

Politik for hændelseslogning

Der skal forefindes en politik for, hvad der logges, hvor log skal gemmes, hvor længe logs gemmes og hvem, der har adgang.

Politikken skal overordnet beskrive, hvilke hændelser, der skal udløse alarmer, som driftspersonalet reagerer på.

Politikken skal også forholde sig til, hvem der anvender logs til at afdække hændelser relateret til fysiske personer.

Opfølgningslogning

SDU IT skal logge sikkerhedshændelser på SDU's væsentlige systemer.

SDU IT skal sikre, at der foretages logning af al adgang til systemkomponenter (inklusive netværksudstyr).

SDU IT skal logge fejlhændelser på SDU's væsentlige systemer.

SDU IT skal logge væsentlige brugeraktiviteter på SDU's systemer.

SDU IT skal logge fejlhændelser på SDU's systemer.

SDU IT skal logge sikkerhedshændelser på SDU's systemer.

Opbevaring af opfølgningslog

Varigheden af opbevaring afhænger af risikovurdering, behov og lovgivning.

SDU IT skal, hvis teknisk muligt, opbevare log for fejlhændelser på alle relevanter systemer i mindst 6 måneder.

SDU IT skal opbevare log for sikkerhedshændelser på ethvert system i mindst 6 måneder. Dette kan eventuelt ske i et SIEM-system.

SDU IT skal opbevare log for brugerhændelser på ethvert system, som behandler persondata, i mindst 6 måneder.

Hændelseslogning

Logning i forbindelse med alle systemkomponenter skal indeholde registrering af adgang til alle logs.

Loggen for systemkomponenter skal indeholde oprettelse og sletning af objekter på systemniveau.

Alle produktionssystemer skal logge information om adgang og forsøg på adgang, for at kunne spore uautoriseret aktivitet fx i et SIEM-system.

Alle sikkerhedshændelser skal logges og opbevares i en fastlagt periode af hensyn til opfølgning på adgangskontroller og eventuel efterforskning af fejl og misbrug.

Loggen for systemkomponenter skal indeholde al brug af identifikations- og autentifikationsmekanismer.

12.4.2 Beskyttelse af log-oplysninger

Beskyttelse af log-oplysninger

Log-faciliteter og log-oplysninger skal beskyttes mod manipulation og tekniske fejl.
Systemlogs skal i realtid kopieres udenfor systemadministrator og/eller driftsafdelingens kontrol.
Hvor dette ikke er muligt, skal der forefindes andre foranstaltninger for at sikre, at uautoriserede ændringer i loggene kan opdages.
Særligt i forhold til personoplysninger er det centralt, at logs ikke gemmes længere, end der er et behov for, og adgangen er begrænset mest muligt.

12.4.3 Administrator- og operatørlogge

Log-gennemgang

Det skal sikres, at det opdages, hvis systemadministrator og systemoperatører manipulerer med loggene på informationsbehandlingsfaciliteter, som er i deres varetægt.
SDU IT skal vedligeholde procedurer vedrørende daglig gennemgang af sikkerhedslogs og krav i forbindelse med opfølgning på uregelmæssigheder.
Log-registreringer fra servere, som udfører sikkerhedsfunktioner, eksempelvis Intrusion Detection Systems (IDS), autentifikation, autorisation og RADIUS, skal gennemgås dagligt eller automatiseret.

12.4.4 Tidssynkronisering

Tidssynkronisering

- Interne og eksterne krav til tidsangivelse, synkronisering og nøjagtighed skal dokumenteres.
- Metoden til at opnå en referencetidsangivelse fra ekstern(e) kilde(r), og måden, hvorpå interne ure synkroniseres sikkert, skal dokumenteres og implementeres.

12.5 Styring af driftssoftware

12.5.1 Softwareinstallation i driftssystemer

Installation af programmer på arbejdsstationer

SDU IT leverer servere og klienter (PC-er) med operativsystemer og relevante applikationer.

Softwareopdateringer generelt

SDU IT skal videst mulig udstrækning holde sig informeret om alle programrettelser til alle programmer, der anvendes på SDU og snarest installere disse på alle computere, f.eks. servere og arbejdsstationer, når det vurderes, at rettelserne har positiv indflydelse på den samlede sikkerhed.
Systemejere er ansvarlige for, at der løbende sker regelmæssig opdatering af anvendt software.

Softwaren bør være testet inden implementering i driftsmiljøet og den bør kunne rulles tilbage. Der skal foretages logning af sådanne systemændringer.
Ved tvungne opdateringer fra større leverandører, laves der en passende vurdering af, om det ændrer på servicens samlede risikovurdering herunder om det udsætter registrerede for en større risiko.
SDU IT skal forestå installation af alle større programrettelser, når det vurderes, at disse har positiv indflydelse på den samlede sikkerhed.

12.6 Sårbarhedsstyring

12.6.1 Styring af tekniske sårbarheder

Rettelser til operativsystemer
SDU IT skal løbende vurdere tilgængelige sikkerhedsrettelser, for eksempel "patches" eller "hot-fixes", til anvendte operativsystemer. Udrulning/installation skal foretages efter behov.

Rettelser til applikations-programpakker
SDU IT skal mindst hver uge vurdere tilgængelige sikkerhedsrettelser f.eks. patches eller hot-fixes. Udrulning/installation skal foretages efter behov.
Der bør samles op på opdateringer fra leverandøren.
Risikobilledet bør løbende vurderes - herunder med henblik på at fastlægge om der opdages sårbarheder i de anvendte systemer.
Ved fund af en ny sårbarhed bør risiko vurderes, og der bør tages stilling til, hvornår opdateringen skal foretages (inkl. test og godkendelse). Ændringer bør altid logges.

Større operativsystem-opdateringer f.eks. "service packs"
Når større opdateringer f.eks. "service packs" er gjort tilgængelige fra leverandører, skal SDU IT vurdere, om disse skal installeres.
Større opdateringer skal testes grundigt for kompatibilitet med anvendte applikationer, inden opdateringerne installeres i produktionsmiljøet.

Styring af anti-virus
SDU IT skal kunne styre anti-virus på alle systemer fra en central lokation. Med styring menes tvungen opdatering, scanning og oprydning. Eventuelle undtagelser skal godkendes af informationssikkerhedschefen.

12.6.2 Begrænsninger på softwareinstallation

Sikkerhedsindstillinger i web-browser
Der må kun anvendes godkendte webbrowsere. Brugerne må ikke forsøge at omgå eller bryde sikringsforanstaltningerne.

Administration af softwarelicenser
Registrering af software licenser sker gennem SDU IT. Det er it-chefens overordnede ansvar, at der er et tilstrækkeligt antal licenser.

Administration af arbejdsstationer
Software installeres primært fra SDU IT's Software Center. Som udgangspunkt tillader SDU ikke, at man er permanent lokal administrator. På Windows kan man søge om at elevere sine rettigheder i 15 min via et program, som SDU IT administrerer på arbejdsstationen. Derefter vil det kræve login (autentificering) at køre det ønskede program som administrator. Mac brugere kan ligeledes elevere rettigheder vha. MacOS's indbyggede rettighedsstyring fx ved systemændringer, installation af programmer m.v. For begge platforme har SDU's SecOps -team mulighed for at gennemgå logs, der registrerer elevering af rettigheder eller brug af root-rettigheder på Mac's.

12.7 Overvejelser i forbindelse med audit af informationssystemer

12.7.1 Kontroller i forbindelse med audit af informationssystemer

Sikkerhed i forbindelse med revision
De personer, der udfører revisionen, skal være uafhængige af det reviderede område.
Hvis revisionen nødvendiggør mere end læseadgang, må dette kun tillades på kopier af de berørte filer, der skal slettes efter brug.
Al adgang i forbindelse med revision skal logges.
Revisionskrav og revisionshandlinger i forbindelse med systemer i drift skal planlægges omhyggeligt og aftales med de involverede for at minimere risikoen for forstyrrelser af SDU's forretningsaktiviteter.

13 Kommunikationssikkerhed

13.1 Styring af netværkssikkerhed

13.1.1 Netværksstyring

SDU IT har det overordnede ansvar for det totale netværk.
Netværkets driftsstabilitet skal sikres. Ethvert netværk 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.

Sikring af netværk

SDU's datanet overvåges med et til formålet egnet 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 SDU's netværk.
- At løse driftsmæssige problemer med opkoblinger gennem firewallen.

Adgang til aktive netværksstik

Aktive netværksstik skal være beskyttet af 802.1x-autentifikation og -autorisation, som teknisk sikrer, at kun godkendte aktiver kan komme i forbindelse med forretningsressourcer.

Aktuelt er etablering på 802.1x en proces, så ikke alle netværksstik er beskyttet af 802.1x.

Installation af netværksudstyr

Det er ikke tilladt at installere netværksudstyr på SDU's netværk uden forudgående godkendelse af SDU IT.

Tilslutning af udstyr til netværk

Generelt må kun SDU IT koble udstyr på det interne netværk, men SDU IT kan uddelegere retten til at opkoble udstyr.

Fjernstyring og administration

Værktøjer til fjernadministration tillades, men som hovedregel ikke til forretningskritiske systemer, medmindre VPN eller lignende benyttes. Undtagelser fra dette skal godkendes af både systemejeren og SDU IT.

Beskyttelse af diagnose- og konfigurationsporte

Fysisk og logisk adgang til diagnose- og konfigurationsporte skal kontrolleres.

Rutekontrol

SDU IT skal begrænse trafikken imellem forskellige sikkerhedszoner således at kun nødvendig trafik videresendes.

Opsætning af udstyr, der ruter trafik skal forhåndsgodkendes eller installeres af SDU IT.

Kryptering af administrative netværksforbindelser

Forbindelser, der benyttes til it-administration, skal krypteres, hvis de benytter offentlige eller usikre netværk, f.eks. internettet.

Firewall-funktioner på servere

Alle servere skal benytte firewall-funktionalitet til at sikre, at der kun gives adgang til nødvendige services for relevante brugere.

Trådløse netværk

Adgang til trådløse netværk for gæster
Der eksisterer et gæstenet, som universitetets gæster kan anvende. Netværket kan og må kun benyttes til internetadgang.
Gæster kan ligeledes benytte eduroam, hvis de allerede har adgang til det.

Trådløse lokalnet må fortrinsvist kun etableres af SDU IT. Hvor der etableres lokale netværk, som har forbindelse SDU's interne netværk skal disse være registreret hos SDU IT.

Forbindelser med andre netværk

Opkobling af et netværk til et andet netværk og forbindelsesvejene mellem netværk skal registreres og kontrolleres. Trafikken mellem Internettet og SDU's 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 SDU IT tilsluttes kommunikationsudstyr, som omgår SDU's firewall. Dataforbindelser til supplerende arbejdsplads i hjemmet etableres via en Internetudbyder. Ved adgang til interne it-ressourcer på SDU's datanet benyttes VPN eller lignende.

Indkommende netværksforbindelser
Der tillades kun etablering af forbindelser fra internet til godkendte servere, eksempelvis e-mail- og web-servere.

Udgående netværksforbindelser
SDU IT foretager løbende begrænsninger i muligheder for udadgående netværksforbindelser på basis af anbefalinger fra samarbejdspartnere for at sikre universitetets aktiver. Dette gælder både IP-adresser og websteder. Restriktioner revideres løbende.

Ansvar for internetforbindelser
Det overordnede ansvar for internetforbindelserne ligger hos SDU IT.

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: Bredbånd, fiberforbindelser og fællesantennesystemer).

Snitflader mod andre netværk

SDU IT forestår sikring, teknisk sammenkobling og løbende kontrol af snitflader imod andre netværk. Snitflader sikres med firewall-løsninger eller lignende.

13.1.2 Sikring af netværkstjenester

Sikring af netværk

ISDU IT har det overordnede ansvar for at beskytte SDU's netværk.

Fjernstyring og administration

Forbindelser til fjernadgang til brug for leverandører og support, skal overvåges, mens de benyttes.
Det er tilladt at benytte værktøjer til fjernadministration, hvis der foreligger sikkerhedsgodkendelse af produktet.
Adgang til administrations- og konfigurationsporte til trådløse netværk skal begrænses til administratorer.

Trådløse netværk for gæster

SDU tilbyder trådløs netværkstjeneste til gæster.

Afvikling af programmer i forbindelse med internetsurfing

Det er tilladt at afvikle browserbaserede programmer, f.eks. netbank-programmer, forudsat at sikkerhedspolitikken (retningslinjer for brug af it for ansatte) i øvrigt overholdes.

Internetbaserede tjenester

Det er tilladt at bruge internettjenester, der ikke er beskrevet i sikkerhedspolitikken, såfremt dette ikke indebærer forøgede sikkerhedsrisici.

Brug af kryptering i forbindelse med dataudveksling

Adgangskoder skal sendes krypteret.

13.1.3 Opdeling i netværk

Opdeling af netværk

SDU IT skal segmentere netværk for at etablere en passende adskillelse imellem forskellige tjenester, brugergrupper eller systemer.
Mindstekrav til netværkssegmentering er, at SDU IT etablerer en "demilitariseret zone" (DMZ), hvor offentligt tilgængelige servere placeres adskilt fra internt tilgængelige servere.

13.2 Informationsoverførsel

13.2.1 Politikker og procedurer for informationsoverførsel

Ansvar

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.
Følsomme og fortrolige personoplysninger samt fortrolige forretningsoplysninger skal sendes krypteret.

Dataklassifikation

Alle politikker og procedurer er beskrevet i "Retningslinjer for dataklassifikation".

Fortrolige informationer i offentlige rum

Der skal udvises forsigtighed ved omtale af fortrolige informationer i offentlige rum.
Fortrolige informationer må ikke efterlades uden opsyn i offentligt tilgængelige rum.

Opbevaring og bortskaffelse af data

Der skal foreligge en procedure for håndtering af opbevaringstiden for data.
Data må kun opbevares i det tidsrum, som er nødvendigt.

Elektroniske dokumenter

Elektroniske kopier af dokumenter, f.eks. indscannede dokumenter og faxer, med fortrolige eller følsomme informationer, må kun behandles og lagres på passende it-udstyr.

13.2.2 Aftaler om informationsoverførsel

Inden datakommunikationsforbindelse etableres til en samarbejdspartners it-systemer, skal der udføres en risikovurdering. Den skal mindst omfatte:

- hvilke 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 SDU's it-aktiver, skal der i hvert enkelt tilfælde udarbejdes en skriftlig aftale, der pålægger samarbejdspartneren at overholde SDU's it-sikkerhedsregler. Der er ikke i alle tilfælde lavet aftaler med ansatte forskere, som har opstillet og/eller driver servere fra SDU’s netværk, men det forventes at alle rulles over på en systemforvaltningsaftale.

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 osv., med eksterne partnere. Sikringsforanstaltningerne skal afstemmes med karakteren af de udvekslede data, herunder brug af vpn, ftp, kryptering mv.

Data, der er klassificeret "Fortroligt" eller "Følsomt", 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.

13.2.3 Elektroniske meddelelser

Alle e-mail til/fra SDU skal passere SDU's del af Exchange i skyen, der frasorterer virus og phishing mails samt markerer spam. Der må ikke eksistere e-mailservere der kan sende e-mail uden om dette system bortset fra lokale servere, som kan benytte en lokal gateway. Dette modvirker dels at virus når frem til modtageren, dels at misbrug der kan miskreditere SDU og dermed forhindre legal mail i at komme frem, 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-mailsystemer overvåges i henhold til de til enhver tid gældende regler for SDU IT's vagtordning.

Anvendelse af sociale netværk
Det er tilladt SDU's brugere at anvende sociale netværkstjenester som f.eks. Facebook, Twitter og LinkedIn fra SDU's netværk, forudsat at brugen ikke generer eller forhindrer almindelig drift og brug af universitetets it-systemer.

Der må kun offentliggøres SDU informationer, som er klassificerede som "Offentlige forretningsdata" på sociale netværk.

Al anden SDU-information, f.eks. præsentationer, billeder, film og andre data må ikke offentliggøres på sociale netværk, hvis det kan medføre risiko for tab af universitetets intellektuelle rettigheder til informationerne eller være i strid med Databeskyttelsesloven eller Datatilsynets vejledninger og kendelser.

13.2.4 Fortroligheds- og hemmeligholdelsesaftaler

Fortrolighedserklæring for tredjepart
Det skal sikres, at tredjepart, der kan få adgang til SDU's data, er omfattet af en fortrolighedserklæring.
SDU har en Tavshed- og fortrolighedserklæring (Code of Conduct), der kan benyttes, når eksterne samarbejdspartnere, praktikanter eller andre har brug for adgang til SDU's data.

Indhold af fortrolighedserklæringerne
Betingelser for returnering eller destruktion af informationsaktiver ved aftalens ophør.

Underskriverens ansvar for at undgå brud på den aftalte fortrolighed.
Definition af de informationer, der er omfattet.
SDU's ret til overvågning af og opfølgning på overholdelse af fortrolighedspligten.
Sanktioner ved brud på fortrolighedspligten.

Håndtering af tavsheds- og fortrolighedserklæring
Det er den enhed (fællesområde eller fakultet), der indgår aftalen, der har ansvar for, at tavsheds- og fortrolighedserklæringen underskrives og journaliseres i SDU's journaliseringssystem.

14 Anskaffelse, udvikling og vedligeholdelse af systemer

14.1 Sikkerhedskrav til informationssystemer

14.1.1 Analyse og specifikation af informationssikkerhedskrav

Anskaffelsesprocedurer
Det skal sikres, at nyanskaffelser ikke giver anledning til konflikt med eksisterende krav i sikkerhedspolitikken eller anden lovgivning fx Udbudsloven.
Anskaffelser må ikke give anledning til forøget risiko for sikkerhedshændelser, medmindre ledelsen accepterer den øgede risiko.
Anskaffelse af it-systemer og services skal være i overensstemmelse med it-sikkerhedspolitikken.
Risikovurdering af it-systemer ved anskaffelse skal ske jf. "Retningslinje for sikkerhedsvurdering ved it-anskaffelser".

Områder for kravspecifikation
Kravspecifikation skal omhandle følgende områder:

- Adgangskontrol, som understøtter identifikation, autentifikation og autorisation af brugere.
- Oplysning til brugere, operatører og administratorer om opgaver og ansvar.
- Alle væsentlige hændelser logges og overvåges.
- Beskyttelse imod fortrolighedskrænkelser i det omfang systemet skal behandle fortrolige, personhenførbare eller følsomme 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.

Sikkerhed i applikationsudvikling

Sikkerhed skal inkluderes som en integreret del af alle udviklings-, test- og anskaffelsesprojekter.
Sikkerhed i applikationsudvikling skal altid tage udgangspunkt i privacy by design og privacy by default. Der skal så vidt det er muligt arbejdes ud fra en tredeling med dev, qa og prod miljø som er funktionsopdelt.

14.1.2 Sikring af applikationstjenester på offentlige netværk

Sikring af applikationer på offentlige netværk
Der skal benyttes sikre autentifikations- og autorisationsprocesser for at sikre service-transaktioner over offentlige netværk.
Datas integritet og fortrolighed skal sikres, når der benyttes applikations-services over offentlige netværk, ved eksempelvis:

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

SDU må ikke drive egne systemer, der håndterer betaling. SDU kan drive løsninger, der understøtter betaling via godkendt tredjeparts software.
SDU skal definere håndtering og ansvarsplacering ved bedrageri og eventuelle forsikringskrav.
SDU skal fastlægge krav til leverandørers sikkerhed.
Eventuelle lovgivningsmæssige krav skal opfyldes – fx på det persondataretlige område.

14.1.3 Beskyttelse af handelsapplikationer og -tjenester

For handelsplatforme, som SDU stiller til rådighed, skal gælde at:

- kommunikationsveje skal være krypteret og protokoller sikres,
- transaktioner bliver behandlet fortroligt og kun betroet personel har adgang til data,
- lagring sker, så der ikke er tilgængelighed fra internettet,
- og der kun blive gemt det data der er relevant for selve handlen.

Online transaktioner
Der skal anvendes industristandarder for signaturer (kryptografiske løsninger) af alle involverede parter i transaktionerne.

14.2 Sikkerhed i udviklings- og hjælpeprocesser

14.2.1 Sikker udviklingspolitik

Sikkerhed i applikationsudvikling
Udviklingsmiljøet skal beskyttes.
Der skal forefindes en procedure som stiller krav til metodikken i udviklingen af software – herunder koderetningslinjer for programmeringssprog, sikkerhedskrav i designfasen, udviklingernes kompetencer,

udviklernes evne til at undgå, finde og korrigere sårbarheder, metodik for test og kodegennemgang, krav til leverandører og brug af ekstern kode og genbrug af intern såvel som ekstern kode.
Softwareudvikling skal baseres på Best practice og indbefatte informationssikkerhed gennem hele softwareudviklingens livscyklus.
Sikkerhed skal inkluderes som en integreret del af alle udviklingsprojekter.
Principper for databeskyttelses gennem design og standardindstillinger skal være en integreret del af udviklingen.

Validering af inddata (datamigrering)
Data, der sendes ind i systemerne, skal valideres for korrekthed.
Der skal genereres log over de aktiviteter, der sender data ind i systemet.

14.2.2 Procedurer for styring af systemændringer

Procedurer for styring af ændringer

- Procedurer skal omfatte nye systemer og større ændringer på eksisterende systemer.
- Der skal tages højde for de risici, som ændringerne kan medføre.
- Der skal tages stilling til autorisation af brugere.
- Al software, alle informationer, alle databaser og al hardware skal omfattes.
- Der skal tages højde for kendte sikkerhedssvagheder fx ved anvendelse af OWASP.
- Der skal være en godkendelsesproces.
- System-, drift- og brugerdokumentation skal dokumenteres version for version og der skal genereres et auditspor.
- Der skal foretages test af ændringer i et testmiljø adskilt fra produktions- og udviklingsmiljøer.
- Sikkerheds- og kontrolprocedurer må ikke kompromitteres.
- Det pålægges den operationelle systemejer at foretage tilpasning, opsætning eller ændring af programparametre eller at sikre, at programleverandøren udelukkende foretager de aftalte ændringer. It-systemets brugere må så vidt muligt ikke have adgang til tilpasninger eller opsætninger.
- Implementeringen af ændringen skal foretages på et aftalt tidspunkt og være ledsaget af en tilbagerulningsplan.

14.2.3 Teknisk gennemgang af applikationer efter ændringer af driftsplatforme

Gennemgang af systemer efter ændringer
Beredskabsplanerne og relevante risikovurderinger skal tilrettes i overensstemmelse med nye ændringer.
Ændringer i driftsmiljøerne skal annonceres i god tid således, at der er god tid til gennemgang og test inden implementeringen.

Når driftsmiljøerne ændres, skal kritiske forretningssystemer gennemgås og testes for at sikre, at det ikke har utilsigtede afledte virkninger på SDU's daglige drift.
Når der foretages ændringer af operativsystemer, skal organisationen vurdere behovet for opdatering af beredskabsplanerne.

14.2.4 Begrænsning af ændring af softwarepakker

Ændringer i standardsystemer
Ændringer skal begrænses for at fastholde en softwarepakkes driftsstabilitet. Med undtagelse af ændringer i parametre og specialopsætninger skal modifikation af standardprogrammer undgås.

Hvis det er nødvendigt at ændre en softwarepakke fra en leverandør, skal risikoen vurderes.
Kompatibilitet med eksisterende software skal vurderes.
Den oprindelige software såvel som ændringen skal opbevares som kopi.
Der skal være en proces som sikrer og dokumenterer, at de nyeste godkendte opdateringer er installeret.

Ændringer i form af opdateringer skal testes. Under særlige omstændigheder, hvor det skønnes absolut nødvendigt at modificere en færdig softwarepakke og der ikke kan skaffes en anden softwarepakke, 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.

Systemudvikling udført af ekstern leverandør
Krav i nærværende regelsæt samt reglerne for offentlige indkøb følges.

14.2.5 Principper for udvikling af sikre systemer

Sikkerhedskrav til informationsbehandlingssystemer
Sikkerhed skal indarbejdes i alle arkitekturlag (forretning, data, applikationer og teknologi).
Ny teknologi skal risikovurderes og designet bør gennemgås for kendte angrebsmønstre.
SDU's ønsker til nye såvel som bestående systemer skal indeholde krav til sikkerheden med udgangspunkt i en risikovurdering.
Principperne skal også gælde eksterne leverandører og partnere og bør integreres i kontrakter.
Hvis der behandles personoplysninger i systemerne, skal efterlevelse af de persondataretlige regler designes ind i systemerne og slås til som standard – herunder fx dataminimering, gennemsigtighed for den registrerede ift. behandlingen, klart defineret formål, dokumentering af retligt grundlag, (automatiseret) sletning, og sikkerhedsforanstaltninger, der afspejler risikoen for den registrerede.

Specifikation af sikkerhedskrav

Sikkerhedskrav skal være dokumenteret i forbindelse med enhver it-system-nyanskaffelse eller it-systemopgradering. Dette gælder både for kundetilpassede- og standardsystemer.
Såfremt en overordnet risikovurdering retfærdiggør aktiviteten, skal sikkerhedskrav dokumenteres i forbindelse med enhver forretningskritisk it-system nyanskaffelse eller it-systemopgradering. Dette gælder både for kundetilpassede- og standardsystemer.

14.2.6 Sikkert udviklingsmiljø

Udviklingsprocedure

Der skal udfærdiges en udviklingsprocedure der dækker mennesker, processer og teknologi, der er relateret til systemudviklingsmiljøerne.

Sikring af udviklingsmiljøer

Udviklingsmiljøer skal specielt sikre integritet i udviklingsprocessen, herunder sikring mod tab af data.
Ved risikovurdering af systemudvikling bør følgende overvejes:

- Omfanget af følsomme data
- Mulighed for anonymisering af data
- Lovkrav
- Adskillelse af udviklings-, test og produktionsmiljøer
- Politikker for adgangskontrol og revisionsspor
- Sikker udveksling af data mellem udvikling, test og produktion
- Sikker lagring af backup
- Revisionsspor af ændringer i miljøer

Der skal anvendes en formel livscyklus for systemudvikling, som tager højde for sikkerhed i processen.
Sikkerhedskravene bør identificere alle relevante sikkerhedsaspekter såsom beskyttelse af data der lagres, transporteres eller benyttes

Analysen af sikkerhedskrav skal desuden tage hensyn til følgende:

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

14.2.7 Outsourcet udvikling

Systemudvikling udført af ekstern leverandør

SDU kræver dokumenteret løbende kvalitetssikring.

SDU kræver som udgangspunkt ophavsrettighed på kildekode.

Aftaler om accepttest for kvalitet, nøjagtighed og sikkerhed skal identificeres og være en del af leverancer.

Organisationen skal desuden være i stand til at validere effektiviteten af udviklingsprocesserne.

Hvis der behandles personoplysninger i de outsourcede systemer, skal efterlevelse af de persondataretlige regler designes ind i systemerne og slås til som standard – databeskyttelse gennem design og standardindstillinger, herunder fx dataminimering, gennemsigtighed for den registrerede med behandlingen, klart defineret formål, dokumentering af retligt grundlag, (automatiseret) sletning, og sikkerhedsforanstaltninger, der afspejler risikoen for den registrerede.

Ejerskab af data, cloudløsninger

SDU skal sikre, at ejerskab, herunder regler for ophavsret, kildekode mm. er klart defineret mellem SDU og cloududbyder.

Ekstern revision af outsourcing-partnere

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

Der skal føres passende tilsyn med databehandlere jf. retningslinje for tilsyn med databehandlere.

14.2.8 Systemsikkerhedstests

Test af sikkerhedsfunktioner

Der skal laves en testplan, som omfatter testinddata og forventede uddata under relevante betingelser.

Der skal foretages godkendelsestests uafhængigt af udviklingsteamet, med det formål at sikre at systemet arbejder som forventet. Denne test skal som minimum udføres af SDU's it-sikkerhedsspecialister.

14.2.9 Systemgodkendelsestests

Godkendelse af nye eller ændrede systemer

SDU skal etablere en godkendelsesprocedure for nye systemer, der udvikles eller tilpasses, for nye versioner og for opdateringer af eksisterende systemer samt de afprøvninger, der skal foretages, inden de kan godkendes og sættes i drift.

Godkendelsesproceduren skal sikre, at standardværdier, eksempelvis standard administrator-logins og andre "fabriksindstillinger", bliver ændret, før et system installeres på netværket.

Systemaccepttest bør altid tage højde for relevante sikkerhedskrav for blandt andet automatiseret kodetest og sårbarhedstest.

Det skal testes at sikkerhedskravene fra ISO27002:2013 kontrol 14.1.1 og ISO27002:2013 kontrol 14.1.2 tillige med systemudviklingsmetoderne fra ISO27002:2013 kontrol 14.2.1 er efterlevet.

Ligeledes skal komponenter, der modtages fra andre systemer, og integration til andre systemer testes.

Tests kan ske med automatiserede værktøjer som f.eks. sårbarhedsskannere.

14.3 Testdata

14.3.1 Sikring af testdata

Sikring af testdata
Der skal være en procedure for at beskytte driftsdata, der anvendes til tests.
Proceduren bør adressere: regler for adgang, godkendelsesprocedure for overførsel af driftsdata til testmiljø, sletning af driftsdata efter endt test og log over kopiering og brug af driftsdata til test.

Som udgangspunkt må der ikke benyttes personoplysninger i test. Såfremt der undtagelsesvis gøres brug af virkelige persondata til test, skal omfanget begrænses mest muligt. Hvis det er muligt bør, der anvendes syntetiske personoplysninger eller ske anonymisering af data.

Testdata, der indeholder virkelige data, skal beskyttes i overensstemmelse med deres klassifikation.
Hvis det ikke er muligt at undgå at bruge personoplysninger i testmiljøet, skal personoplysningerne enten beskyttes med de samme tekniske og organisatoriske foranstaltninger i testmiljøet, som de beskyttes med i driftsmiljøet, eller der skal foretages en risikovurdering, som kan guide iværksættelsen af alternative foranstaltninger.

Foreløbig procedure for beskyttelse af driftsdata, de anvendes til tests:

Håndtering af testdata
Det skal formelt godkendes, inden data fra driftsmiljøet kopieres til et testmiljø.
Kopiering og brug af data fra driftsmiljøet til test skal logges for at sikre kontrolsporet.
Data til test skal udvælges, kontrolleres og beskyttes omhyggeligt og i henhold til deres klassifikation.
Formelle adgangskontrolprocedurer skal også omfatte testapplikationssystemer.

Sletning af testdata
Testdata skal fjernes inden systemer sættes i endelig drift.
Særlige applikationskonti, brugernavne og adgangskoder, anvendt i forbindelse med udvikling og test, skal slettes før en applikation sættes i drift.

15 Leverandørforhold

15.1 Informationssikkerhed i leverandørforhold

15.1.1 Informationssikkerhedspolitik for leverandørforhold

SDU benytter i varierende grad leverandører til udvikling, vedligeholdelse, drift og support.

Der skal laves en procedure, som præciserer de kontroller, der skal rettes mod leverandøren såvel som de kontroller relateret til interaktion med leverandører:

- Identifikation og dokumentation af leverandører
- Håndtering af leverandøren i hele livscyklussen
- Fastlæggelse og dokumentation af leverandørens adgang
- Sikkerhedsmæssige minimumskrav til adgang baseret på risikovurdering
- Proces for overvågning af om de fastlagte sikkerhedskrav efterleves af leverandøren
- Kontrol med informationers integritet
- Beskrivelse af de typer af pligter leverandørerne skal efterleve
- Håndtering af sikkerhedsbrud forbundet med leverandøradgang
- Aftaler om beredskab m.v. for at sikre parternes tilgængelighed
- Awareness om leverandørprocedurer hos de ansatte, som er ansvarlige for indkøb og de medarbejdere, som samarbejder med leverandører
- Udformning af aftaler med leverandører, som afspejler ovenstående krav
- Håndtering af forandringer i aftaler med leverandører – herunder flytning af systemer og data

Vurdering og godkendelse af outsourcing-leverandør
Informationssikkerhedschefen skal deltage i vurdering og godkendelse af større outsourcing-leverandører.
Leverandøren skal kunne dokumentere et tilfredsstillende sikkerhedsniveau.
Leverandøren skal kunne dokumentere sit sikkerhedsniveau f.eks. i form af revisorerklæring, intern auditrapport eller it-revisionsrapport.

Anskaffelse, udvikling og vedligeholdelse ved outsourcing
Leverandøren skal have passende formelle procedurer baseret på best practices på området (change- og patch management-procedurer).

Fortrolighedserklæring for tredjepart
I de tilfælde, hvor tredjepart formodes at få adgang til fortrolige eller følsomme informationer, indgås formel aftale indeholdende en fortrolighedserklæring/tavshedserklæring.

Persondata ved outsourcing
Ved behandling af persondata, skal outsourcing-partneren skriftligt tilkendegive at vedkommendes IT-sikkerhed er tilstrækkelig, evt. i form af en revisionsrapport eller CIS-benchmarks, og der skal laves en databehandleraftale.

Leverandøren skal have passende formelle procedurer baseret på Best practices på området (change- og patch management-procedurer).

15.1.2 Håndtering af sikkerhed i leverandøraftaler

Sikkerhed i leverandøraftaler

Der bør udarbejdes leverandøraftaler, som omfatter følgende forhold:

- En beskrivelse af de informationer, der gives adgang til – inkl. hvordan adgangen gives
- Hvis informationerne er klassificeret, bør klassifikationen afspejles i kontrakten med leverandøren
- Krav om at lovgivningsmæssige krav efterleves
- Kontroller, som skal implementeres – f.eks. mht. adgangskontrol, overvågning, audit og rapportering
- Præcisering af den accepterede anvendelse af information
- Betingelser for autorisation til adgang hos leverandøren og evt. en liste over medarbejder med adgang
- Sikkerhedspolitikker, procedurer og kontroller, som er relevante for den konkrete aftale
- Procedurer for sikkerhedsbrud
- Evt. screening af leverandørens medarbejdere og krav til træning hos leverandøren i forhold til specifikke sikkerhedsprocedurer
- Krav til underleverancer
- Kontaktpersoner
- Ret til audit af leverandørens processer og kontroller relateret til aftalen
- Fejl og konfliktløsning
- Årlig revisionsrapport om effektiviteten af kontrollerne
- Leverandørens forpligtelser til at overholde andre af organisationens sikkerhedskrav

Håndtering af sikkerhed i procedurer for leverandøraftaler

Relevante sikkerhedskrav skal identificeres og aftales med leverandører, der har adgang til, behandler, opbevarer eller leverer IT-infrastruktur til organisationens informationsaktiver.

Inden datakommunikationsforbindelse etableres til en samarbejdspartners it-systemer, skal der udføres en risikovurdering. Den skal mindst omfatte

- hvilke 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 SDU's it-aktiver, skal der i hvert enkelt tilfælde udarbejdes en skriftlig aftale, der pålægger samarbejdspartneren at overholde SDU's informationssikkerhedsregler.

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 osv., med eksterne partnere. Sikringsforanstaltningerne skal afstemmes med karakteren af de udvekslede data, herunder brug af vpn, ftp, kryptering mv.

Sikkerhed ved samarbejde med tredjepart
Eksternt service- og rådgivningspersonale pålægges tavshedspligt i henhold til den underskrevne fortrolighedserklæring. Straffelovens § 152 er også gældende.

Misligholdelse, ekstern cloudløsning
SDU skal sikre, at servicen kan afbrydes i tilfælde af misligholdelse, ved brud på sikkerheden, eller hvis løsningen indebærer en uacceptabel risiko for SDU's informationer og netværk.
SDU skal have en "exit-strategi" på plads i tilfælde af misligholdelse.

Kontrakt om ekstern cloud-løsning
Aftale med ekstern cloud-udbyder sker på grundlag af udbyderens standardkontrakt.
SDU skal sikre, at kontrakten som minimum tager højde for de lovgivningsmæssige krav, f.eks. vedr. personoplysninger.
SDU skal sikre, at aftalen indeholder væsentlige sikkerhedselementer, såsom roller, opfyldelse af sikkerhedskrav, beredskab, hændelseshåndtering, behandling af data omfattet af lovgivning, brugerstyring, fysisk sikkerhed, beskyttelse af informationer både fysisk og logisk, sletning og udfasning af udstyr og forhold ved aftalens ophør. Dette kan evt. ske via en tillægsaftale.

Misligholdelse, cloudløsning
SDU skal sikre, at servicen kan afbrydes i tilfælde af misligholdelse, ved brud på sikkerheden, eller hvis løsningen indebærer en uacceptabel risiko for SDU's informationer og netværk.
SDU skal have en "exit-strategi" på plads i tilfælde af misligholdelse.

15.1.3 Forsyningskæde for informations- og kommunikationsteknologi

Krav til forsyningskæden

- Leverandøren bør formidle sikkerhedskrav og sikkerhedspraksis til alle underleverandører.
- Der bør implementeres en overvågningsproces til validering af efterlevelsen af disse krav.
- Der bør sikres identifikation og audit af særlig kritiske komponenter.
- Der bør sikres, at komponenter virker som forventet og ønsket.
- Der bør sikres compliance med lovgivning gennem forsyningskæden.

Netværksleverandører skal kunne levere:
De i forhold til følsomheden af de behandlede data nødvendige teknologiske muligheder for autentifikation, kryptering og overvågning.

De nødvendige tekniske opsætninger til at sikre opkoblinger i overensstemmelse med samarbejdsaftalen.
Det nødvendige sikkerhedsniveau i hele leverandør-forsyningskæden.

Netværkssikkerhed, outsourcing-leverandør
Leverandøren skal sikre en hensigtsmæssig opbygning af netværk, firewall, segmentering, kryptering mm.
SDU skal sikre at leverandørens opbygning af netværk og netværkssikkerhed har et passende sikkerhedsniveau. Vurdering kan ske på baggrund af sårbarhedsvurdering, IT-revisorerklæring eller leverandørens interne auditrapport.
Leverandøren skal foretage periodiske test af netværk og firewall, fx. penetrationstest. Disse kan udføres af tredjepart.

15.2 Styring af leverandørydelser

15.2.1 Overvågning og gennemgang af leverandørydelser

Overvågning og audit, cloudløsning
Udbyderen skal kunne dokumentere et passende sikkerhedsniveau, eksempelvis revisionserklæring, intern audit, ISO 27001-certificering, outsourcing-revisionserklæring (ISAE16, 3402) eller tilsvarende.
Udbyderen skal kunne levere rapportering for, i hvilken grad aftalte servicemål er opfyldt.

Overvågning og audit af outsourcing-leverandør
Leverandøren skal levere rapportering for, i hvilken grad aftalte servicemål er opfyldt.

SDU kan foretage audit af leverandøren, alternativt kan intern auditrapport, it-revisionsrapport, årlig risikovurdering eller it-outsourcing-erklæring indgå i overvågningen. Behandler leverandøren personoplysninger på vegne af SDU laves der tilsyn med databehandler jf. retningslinjen herfor.

Periodiske service-statusmøder skal omhandle sikkerhedsrelaterede emner såsom sikkerhedshændelser og resultater af KPI'er.

Overvågning af serviceleverandøren
SDU skal regelmæssigt overvåge serviceleverandørerne, gennemgå de aftalte rapporter og logninger samt udføre egentlige revisioner for at sikre, at aftalen overholdes, og at sikkerhedshændelser og -problemer håndteres på betryggende vis.
Systemejeren har det overordnede ansvar for tilsyn med serviceleverandørerne. De aftalte rapporter og logninger gennemgås løbende for at sikre at aftalen overholdes, og at sikkerhedshændelser og -problemer håndteres på betryggende vis.

15.2.2 Styring af ændring af leverandørydelser

Styring af ændringer hos serviceleverandøren
SDU skal sikre, at ændringsstyring af serviceleverandørens ydelser følger samme retningslinjer som universitetets egne.

16 Styring af informationssikkerhedsbrud

16.1 Styring af informationssikkerhedsbrud og forbedringer

16.1.1 Ansvar og procedurer for informationssikkerhedsbrud

Brud på persondatasikkerheden
Der er i dokumentet "Retningslinje for behandling af brud på persondatasikkerheden" defineret ansvar for de afdelinger, som tager del i håndteringen af persondatabrud. Ydermere er der angivet hvilken rolle de enkelte afdelinger spiller i håndteringen.
Både ansvar og rollefordeling er uddybet yderligere i de deraf følgende vejledninger.

Proces for håndtering af brud på persondatasikkerheden
Ovennævnte vejledninger angiver den generiske proces for håndteringen af persondatabrud.
Processen styres af egenudviklet platform baseret på SharePoint, som tillige indeholder dokumentation for håndtering af det enkelte brud, samt foranstaltninger og om bruddet er anmeldt til Datatilsynet.

Informationssikkerhedsbrud
Større hændelser der påvirker SDU's it-ydelser føres der hændelseslog over, hvor hændelsen og de iværksatte tiltag beskrives. Disse afrapporteres til Udvalget for databeskyttelse og informationssikkerhed.

16.1.2 Rapportering af informationssikkerhedshændelser

Medarbejdere har adgang til information og informationssikkerhedsbrud på sdunet.dk/gdpr. På denne side findes også link til formular til indberetning af brud.
Det tilskyndes at alle hændelser, som kan have konsekvenser for fortrolighed, integritet og tilgængelighed af personhenførbare oplysninger anmeldes.

SDU IT forestår den indledende afdækning af brud, samt dokumentering. Ligeledes registrerer SDU IT persondatabrud, som indberettes sekundært som følge af øvrige sager indsendt til Servicedesk.
Der henvises i øvrigt til retningslinje for behandling af persondatabrud.
Informationssikkerhedshændelser som ikke indeholder personhenførbare oplysninger registreres som hændelser i SDU IT's hændelseslog alt efter alvorlighed. Se 16.1.4.

16.1.3 Rapportering af informationssikkerhedssvagheder

Hvis opdagede svagheder kan resultere i persondatabrud, bør disse anmeldes på samme vis som egentlige brud. Herefter kan eventuelle foranstaltninger igangsættes af relevant aktør. Tilsvarende er relevant for informationssikkerhedshændelser der ikke indeholder personhenførbare oplysninger, disse registreres alt efter alvorlighed på SDU IT's interne hændelseslog.

Sårbarhedsscanninger
SDU laver daglige interne og eksterne sårbarhedsscanninger. Disse udføres af SecOps, der laver anbefalinger til hærdninger. Såfremt hærdningen medfører væsentlig påvirkning af brugerne inddrages Team Sikkerhed, hvor tiltaget drøftes inden der tages endelig stilling til tiltaget. Såfremt sikkerhedstiltagene er meget omfattende eller indgribende i brugernes vanlige rettigheder, løftes beslutningen til udvalget for informationssikkerhed og databeskyttelse.

16.1.4 Vurdering og beslutning om informationssikkerhedshændelser

Vurderingen af persondatabrud foretages i SDU RIO på baggrund af den anmeldelse der er foretaget af bruger og kvalificeret af SDU IT.
Dokumentation foretages i egenudviklet system baseret på SharePoint.

Væsentlige driftshændelser registreres af SDU IT, der fører log og de hændelser, der har karakter af informationssikkerhedsbrud. Det IT-chefen der beslutter, hvilke hændelser der føres til loggen.

16.1.5 Håndtering af informationssikkerhedsbrud

SDU IT håndterer hændelser lige som daglig drift forstået på den måde, at det er de samme medarbejdere i SDU IT, der afhjælper evt. hændelser, som også forestår den normale daglige drift. Se desuden kap. 17 om beredskab.

Håndtering af brud på persondatasikkerheden
Informationssikkerhedsbrud anmeldt af medarbejdere behandles indledningsvist af SDU IT (Servicedesk), som sikrer tilstrækkelig dokumentation af bruddet. Om nødvendigt tages kontakt til medarbejder for at opklare eventuelle tvivlsspørgsmål eller manglende informationer i den oprindelige anmeldelse.
SDU IT forestår også den tekniske afhjælpning af den grundlæggende problemstilling, således forstået, at ulykken stoppes.
Herefter oversendes sagen til SDU RIO, som foretager den juridiske vurdering af bruddet, samt eventuel indberetning til Datatilsynet.
SDU RIO dokumenterer ligeledes relevante handlinger i egenudviklet løsning baseret på SharePoint.

Sluttelig håndteres læring af det enkelte brud ved SDU Digital, Compliance, som kan kontakte den enkelte afdeling, med henblik på at undgå lignende brud fremadrettet.

16.1.6 Erfaring med informationssikkerhedsbrud

Hændelsesloggen indeholder et særskilt punkt til lærings refleksioner på baggrund af hændelsen.

SDU Digital, Compliance overvåger løbende dokumentationen på informationssikkerhedsbrud, og tager hånd om eventuelle foranstaltninger, som måtte findes nødvendige. Hændelseslogs over væsentlige driftshændelser, der har karakter af informationssikkerhedsbrud forelægges desuden Udvalget for informationssikkerhed og databeskyttelse til orientering.
Som beskrevet i Retningslinje for behandling af brud på persondatasikkerheden, vil SDU Digital, Compliance løbende sikre læring af de brud der har været, på baggrund af den dokumentation SDU IT og SDU RIO sikrer. Nærmere beskrivelse af proceduren kan findes i "Vejledningen i håndtering af persondatabrud - Compliance".

16.1.7 Indsamling af beviser

Ved alvorlige informationssikkerhedsbrud, hvor det kan blive nødvendigt at løfte bevisbyrden for angrebet, skal indsamlingen og opbevaringen af beviser følge "Best practice". SecOps analysere selv angrebene og har normalt ikke behov for ekstern understøttelse.

Brud på persondatasikkerheden
Alle indberettede brud dokumenteres i egenudviklet system baseret på SharePoint, herunder også relevante beviser for eventuelle brud. Desuden journaliseres alle sager, som anmeldes til Datatilsynet i SDU's ESDH-system.

17 Informationssikkerhedsaspekter ved nød-beredskabs- og reetableringsstyring

17.1 Informationssikkerhedskontinuitet

17.1.1 Planlægning af informationssikkerhedskontinuitet

For at formindske konsekvenserne af tilsigtede eller utilsigtede hændelser, der påvirker tilgængelighed, integritet og fortrolighed af SDU's it-systemer, skal der gennemføres beredskabsplanlægning til reetablering af forretningskritiske systemer senest før idriftsættelse og i forbindelse med væsentlige ændringer.

SDU arbejder efter princippet, at beredskab er lig daglig drift, hvilket betyder, at det er de samme medarbejdere, der understøtter driften af et it-system til hverdag, der i beredskabssituationer også har ansvaret for at systemet kan køre i nøddrift og genetableres.

It-chefen fungerer som beredskabsleder og beslutter, hvornår en hændelse har karakter af en beredskabshændelse, der kræver sammenkaldelse af beredskabsledelsen og dokumentation i hændelsesloggen.

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 SDU's aktiviteter, samt med hvilke midler aktiviteterne kan fortsætte, indtil reetablering 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 efter forretningskritikaliteten eller om it-systemet understøtter andre forretningskritiske processer.

Et it-system kan efter konkret vurdering betragtes som forretningskritisk, hvis den opfylder én eller flere af følgende kriterier:

- Understøtter samfundskritisk infrastruktur
- Understøtter kritiske forretningsprocesser, der har indflydelse på SDU's økonomi og omdømme
- Påvirker væsentlige dele af universitetets drift herunder mulighed for at kunne understøtte SDU's kerneydelser indenfor undervisning, forskning og videnssamarbejde samt administration af dette.

Der er systemer, der kun er forretningskritiske på bestemte tidspunkter på året, fx ved optagelse af nye studerende eller eksamensafvikling. SDU's beredskab herunder systemer, der er underlagt vagtordning, afspejler dette.

Ramme for beredskabsplaner

Udvalget for informationssikkerhed og databeskyttelse 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.

Beredskabsstyringsproces

It-chefen sikrer i samarbejde med områdechefen for Teknisk Service, at der er sammenhæng mellem SDU's overordnede beredskabsplan og it-beredskabsplanerne. Informationssikkerhedschefen inddrages i arbejdet med henblik på at sikre overholdelse af gældende standarder og anbefalinger.

Forsikring mod hændelser

SDU er en statslig, selvejende institution, som er selvforsikret.

17.1.2 Implementering af informationssikkerhedskontinuitet

Beredskabsplaner for forretningskritiske 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.

Beredskabsplan

Beredskabsplaner skal udarbejdes, afprøves og vedligeholdes for forretningskritiske systemer og processer. SDU IT er ansvarlig for at koordinere disse aktiviteter og afrapporterer til udvalget for informationssikkerhed og databeskyttelse.

Aktivering af beredskabsplanen

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

Nødprocedurer for kritiske processer

Der skal, for alle forretningskritiske processer, eksistere en opdateret nødprocedure, der kan sættes i drift. Nødproceduren skal, hvor det er relevant, tage højde for nødvendigheden for at lave kompenserende kontroller for informationssikkerhedskontroller, som ikke kan opretholdes i en kritisk situation.

Identifikation af kritiske processer

Alle forretningskritiske funktioner og disses relaterede processer, systemer og ejere skal være identificerede og dokumenterede.

Indkaldelse af medarbejdere i vagtordning og ekstra personale

For alle kritiske it-systemer skal der forefindes retningslinjer for tilkald af relevant personale i tilfælde af behov for ekstraordinær drift, sikkerhedshændelser og lignende.

17.1.3 Verificering, gennemgang og evaluering af informationssikkerhedskontinuiteten

Uddannelse i beredskabsplaner

It-chefen har det overordnede ansvar for, at medarbejdere i SDU IT er bekendte med deres rolle i it-beredskabsplanen. I praksis er det informationssikkerhedskoordinatoren/IT-sikkerhedskoordinatoren som 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).

17.2 Redundans

17.2.1 Tilgængelighed af informationsbehandlingsfaciliteter

Retablering af forretningskritiske systemer på ny lokation

For alle forretningskritiske systemer skal der forefindes en plan for retablering på ny lokation.
Beredskabsplanerne skal afspejle muligheden for, at de fysiske lokationer kan være utilgængelige eller ødelagte.

18 Overensstemmelse

18.1 Overensstemmelse med lov- og kontraktkrav

18.1.1 Identifikation af gældende lovgivning og kontraktkrav

Ledelsen er ansvarlig for at identificere lovgivning, der er relevant for universitetets drift.
SDU vedligeholder en oversigt over relevant lovgivning på universitetets virkeområde, der skal overholdes.
https://sdunet.dk/da/undervisning-og-eksamen/uddannelsesunderstoettelse/regelsamling

Status på efterlevelsen af love og regler inden for it-området skal monitoreres løbende og revideres mindst en gang hvert år.

Ledelsen er ansvarlig for, at alle eksterne sikkerhedskrav samt universitetets håndtering af disse klarlægges, dokumenteres og løbende vedligeholdes.

- Informationssikkerhedschefen har ansvar for at orientere udvalget for informationssikkerhed og databeskyttelse om relevante anbefalinger fra myndigheder og sikkerhedsorganisationer indenfor cyber- og informationssikkerhed.

- Databeskyttelsesrådgiveren har ansvar for at orientere udvalget for informationssikkerhed og databeskyttelse om relevante domme, afgørelser og vejledninger indenfor databeskyttelsesområdet.

Organisationens risiko for sanktioner skal kortlægges.

18.1.2 Immaterielle rettigheder

Procedure for beskyttelse af immaterielle rettigheder

Der skal forefindes en procedure for beskyttelse af immaterielle rettigheder.

Identifikation af relevante patenter

Ledelsen er ansvarlig for, at patenter, der influerer SDU's drift, identificeres.

Retningslinjer for ophavsrettigheder

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

SDU skal løbende kontrollere, at der kun er installeret autoriserede systemer med autoriserede licenser i SDU.

Bevidsthed om beskyttelse af immaterielle rettigheder

Brugerne skal holdes orienteret om beskyttelse af immaterielle rettigheder, så ulovlig software ikke anvendes og således at der ikke anvendes ulovlige koder, varemærker, film, billeder, lyd, m.v.

18.1.3 Beskyttelse af registreringer

Lagring og adgangsrettigheder til systemdokumentation

Systemdokumentation opbevares i henhold til slettepolitik eller overføres til arkiv jf. arkiveringslovgivningen.

Lovregulerede data

SDU skal beskytte lovregulerede data mod ændring, sletning, samt uautoriseret adgang.
SDU's lovbestemte data skal opbevares og behandles således at datatab, uautoriseret modifikation og forfalskning undgås.

Retention af logdata

Logning skal gemmes så længe en risikovurdering tilsiger, at der er behov herfor.

Retention af historiske politikker, procedurer og dokumentation af foranstaltninger

Nuværende og historiske politikker, procedurer og dokumentation af foranstaltninger bør gemmes med henblik på at beskytte organisationen mod et fremtidigt retskrav.

18.1.4 Privatlivets fred og beskyttelse af personoplysninger

Der skal fastlægges en organisering af behandling af personoplysninger og fastsættes politikker, procedurer og foranstaltninger for beskyttelse af personoplysninger i overensstemmelse med kravene i ISO27701 og/eller ISO29100.
Roller og ansvar skal være beskrevet.

Udvalget for informationssikkerhed og databeskyttelse godkender overordnede politikker og retningslinjer der vedrører behandling af personoplysninger. Det er den enkelte system- og procesejer, der har ansvar for, at databeskyttelsesreglerne bliver overholdt.

18.1.5 Regulering af kryptografi

Regulering på kryptografiområdet

SDU skal efterleve nationale regler for kryptering. Dette gælder også for medarbejdere, der besøger andre lande, medbringende bærbart og mobilt udstyr. Retningslinjer for anvendelse af IT i ansættelsesforhold er gjort tilgængelig på SDUnet. Det er informationssikkerhedschefens ansvar, at retningslinjerne er tilgængelige, men det er den lokale ledelses ansvar, at medarbejdere overholder retningslinjerne.

18.2 Gennemgang af informationssikkerhed

18.2.1 Uafhængig gennemgang af informationssikkerhed

Uafhængig audit af informationssikkerheden

SDU's ISMS skal være underlagt en, for SecOps, uafhængig audit.

Audit skal omfatte:

- Informationssikkerhedspolitik
- It-sikkerhedsregler - og disses efterlevelse
- It-sikkerhedsprocedurer
- ISMS-processer

SDU har med dannelsen af den Digitale organisation lavet en opsplitning af it- sikkerhedsarbejdet, idet den operationelle it-sikkerhed laves i SDU IT, mens politikker og retningslinjer samt audit laves i SDU Digital Compliance.

Tilsvarende skal intern eller ekstern auditor vurdere om kontrolmål, kontroller, politikker, procedurer og foranstaltninger opfylder de persondataretlige regler. Denne funktion er også placeret i SDU Digital Compliance, hvor også SDU's DPO sidder.

Audit skal gennemføres løbende eller minimum 1 gang om året, eller hvis der sker væsentlige ændringer i SDU's ISMS.

Auditors resultater i form af afvigelser fra de fastlagte tillige med supplerende anbefalinger skal forelægges ledelsen.
Ledelsen skal overveje korrigerende foranstaltninger på baggrund af auditors anbefalinger.

18.2.2 Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder

Revision af sikkerhedspolitik

Den interne audit skal kontrollere, at sikkerhedspolitikken er velimplementeret i organisationen og overholdes. Denne audit skal foretages mindst en gang om året, og audit bør omfatte beskrivelse af årsagen til afvigelser, handlingsplaner, der er nødvendige for at håndtere afvigelserne (korrigerende handlinger) samt en efterfølgende vurdering af effektiviteten af de foranstaltninger, der gennemføres.

18.2.3 Undersøgelse af teknisk uoverensstemmelse

Der skal ske en automatiseret gennemgang af tekniske parametres tilstedeværelse.

Der kan ske egentlige sårbarhedsvurderinger og penetrationstests af systemer. Sådanne tests og vurderinger kan ikke erstatte risikovurderinger.

I forholder til behandling af persondata skal ske en monitorering, således kun tilladte behandlinger kan foretages.