Professionshøjskolen UCC

it sikkerhed

UCC IT-Sikkerhedspolitik

2011
IT

It-sikkerhedspolitik i UCC

It-sikkerhedspolitikken gælder for alle medarbejdere (uanset ansættelsesforhold), studerende og gæster, der anvender UCC's it-resurser.

Som bilag er anbragt en ordliste, der en række termer og definitioner.

It-sikkerhedspolitikken for UCC er godkendt af direktionen i december 2011.

Indholdsfortegnelse

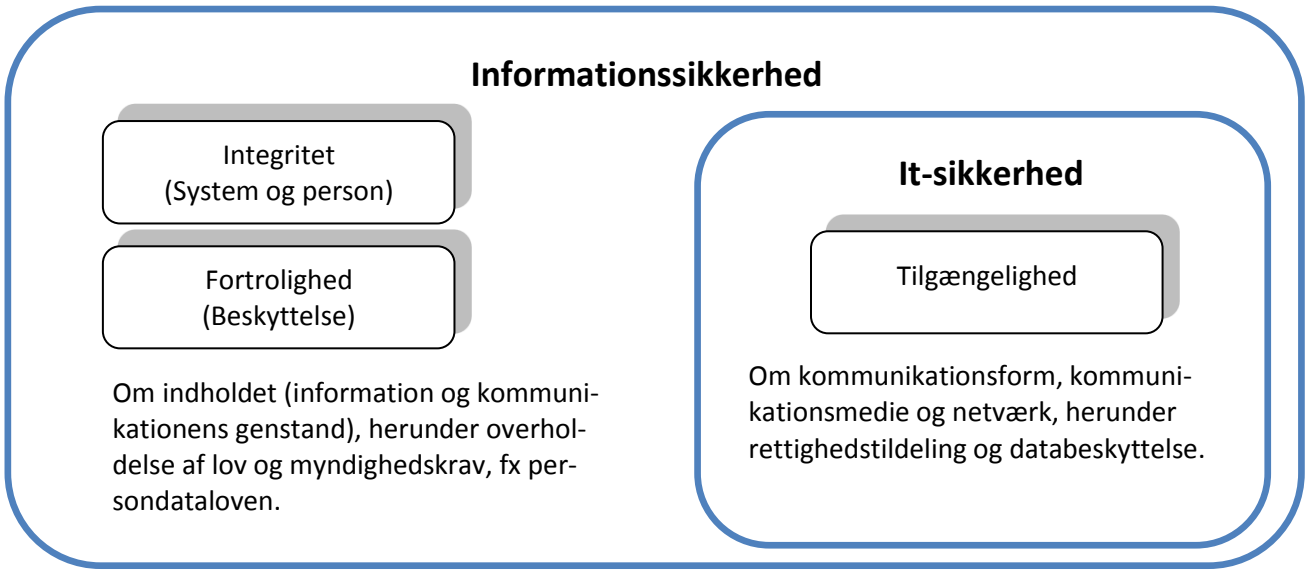
1. Indledning

Den øverste ledelse har det overordnede ansvar for it-sikkerheden hos UCC. Ansvaret varetages normalt ved at nedsætte et tværorganisatorisk it-sikkerhedsudvalg, som har til formål at sikre, at den gældende it-sikkerhedspolitik bliver realiseret og efterlevet.

It-sikkerhedspolitikken skal udformes med baggrund i gældende regler, og så vidt muligt baseres på best practice og gældende lovgivning. Dvs. at it-sikkerhedspolitikken skal være en del af grundlaget for at driften af professionshøjskolen UCC drives i overensstemmelse med lov om professionshøjskoler for videregående uddannelser jfr. bekendtgørelse nr. 849 af 8. september 2009 og bekendtgørelse nr. 1491 af 12. december 2007.

Afgrænsning af it-sikkerhed

Ved it-sikkerhed forstår UCC den del af informationssikkerhed, der drejer sig om tilgængelighed. Informationssikkerhed opnås ved at implementere, overvåge, revurdere og løbende ajourføre et passende sæt af beskyttelsesforanstaltninger. Den består af politikker, praksis, procedurer, organisatoriske tiltag og system- eller maskintekniske funktioner. I forbindelse med informationssikkerhed skelnes der mellem hovedbegreberne *integritet*, *fortrolighed* og *tilgængelighed*. Det er derfor kun sidstnævnte begreb, som er den overvejende genstand for it-sikkerhedsområdet i UCC. Dette er illustreret i nedenstående model:



Når begrebet *tilgængelighed* er valgt i forbindelse med it-sikkerhed, skyldes det, at fx firewall, antivirus, backup og den netværksmæssige infrastruktur er væsentlige områder. Der er altså tale om beskyttelse af systemer til information, kommunikation og lagring, men *ikke* om det konkrete informations- og kommunikationsindhold eller begrænsninger i distribution. Når elementerne 'integritet' og 'fortrolighed' er fravalgt, skyldes det, at der pt. endnu ikke er taget stilling til igangsætning af arbejdet vedrørende det bredere område informationssikkerhed.

Begrundelse for nødvendigheden af it-sikkerhed

Systemer og -netværk er væsentlige aktiver i UCC. At definere, etablere og vedligeholde en passende it-sikkerhed kan være afgørende for UCC's konkurrencedygtighed, rentabilitet, omdømme og efterlevelse af gældende lovgivning.

En troværdig it-sikkerhed er desuden en afgørende forudsætning for både en digital administration og anvendelse af it i undervisningen. Samtidigt giver det øgede antal adgangsmuligheder, fjernarbejdspladser og nye services for både studerende og medarbejdere en øget sårbarhed, da det ikke længere er muligt at forlade sig på traditionelle, centrale sikringsforanstaltninger.

Formulering af sikkerhedsbehov

Det er pga. ovenstående af afgørende betydning, at UCC definerer sine sikkerhedsbehov. Der kan tages udgangspunkt i tre hovedkilder:

- UCC's egen risikovurdering baseret på UCC's forretningsstrategi og -målsætning. Her vurderes trusselsbilledet, UCC's sårbarhed og de forretningsmæssige konsekvenser, et potentielt uheld måtte have.
- Eksterne krav til UCC, dets samarbejdspartnere og dets leverandører. Disse krav kan være lovgivning, bekendtgørelser, forordninger, samarbejdsaftaler eller hensyn til det omgivende samfund.
- Interne krav afledt af UCC's egne kvalitetskrav for at støtte en specifik forretningsmålsætning.

Opgørelse af sikkerhedsbehov

Sikkerhedsbehov identificeres ved en metodisk vurdering af sikkerhedsrisici. Udgifterne til sikringsforanstaltninger skal holdes op mod forretningsmæssige tab ved sikkerhedsbrud, fx dårligt omdømme ved en given sikkerhedsbrist. Resultatet af risikovurderingen indgår i UCC's it-sikkerhedsudvalgs risikostyring. It-sikkerhedsudvalget prioriterer de enkelte risici og beslutter, hvilke sikringsforanstaltninger, der skal iværksættes. Det vil i mange tilfælde være nødvendigt at gennemføre risikovurderingen i flere trin for at bevare det samlede overblik.

Endelig skal det understreges, at en risikovurdering skal gentages regelmæssigt og ved større organisatoriske eller teknologiske ændringer.

Valg af sikringsforanstaltninger

Når UCC's sikkerhedsbehov og risici er afdækket, og risiciene er prioriteret, skal de basale sikringsforanstaltninger og relevante, skærpede sikringsforanstaltninger udvælges og implementeres. 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. For at sikre deres effektivitet skal de skal altid suppleres med en ledelsesmæssig overvågning og en løbende ajourføring.

2. Formål

Dette dokument skal

- udgøre et generelt grundlag for UCC's sikkerhedsmålsætning med henblik på udvikling, implementering, indførelse og effektiv styring af sikkerhedsmæssige kontroller, forholdsregler og sikringsforanstaltninger.
- være generel referenceramme for UCC's interne og eksterne brug af it-faciliteter.
- skabe tillid til UCC's anvendelse af it både internt og eksternt.
- være referenceramme ved anskaffelse og kontrahering af it-produkter og tjenesteydelser.

3 Risikovurdering og –håndtering

Der skal være forståelse for de trusler, institutionen kan blive udsat for, og for institutionens sårbarheder. Styringen af sikkerhedsarbejdet tager udgangspunkt i et sikkerhedsstyringssystem (**ISMS –** "Information Security Management System"), der rettes til, således at det udelukkende omfatter arbejdet med it-sikkerhed.

Overordnet risikovurdering

Som grundlag for ajourføring af UCC's tekniske og organisatoriske it-sikkerhedsforanstaltninger, foretager it-sikkerhedsudvalget en gang årligt en overordnet risikovurdering. Vurderingen baseres blandt andet på dokumentation for de lov- og myndighedskrav, UCC er underlagt i forbindelse med it-anvendelsen. Disse krav skal afspejles i et forretningsmæssigt klassifikationssystem:

- Kontinuerlige risikovurderinger, især ud fra et forretningsmæssigt perspektiv
- UCC skal være i stand til at imødekomme nuværende og kommende trusler på sikkerhedsområdet, både i eksterne såvel som interne arbejdsprocesser og i forhold til anvendelse af ny teknologi
- UCC skal være i stand til at agere, uanset hvilke sikkerhedsmæssige problemstillinger, der kan opstå.

Risikoanalyse

Der skal udarbejdes en detaljeret risikoanalyse for alle forretningskritiske systemer, dvs. systemer, som er klassificeret i kategori 1 eller 2 (se 'risikokategori' i ordlisten).

Analysen skal belyse sandsynligheden for, at it-aktiverne udsættes for trusler, både tilfældige, forsætlige og uforsætlige hændelser som f.eks.:

- destruktion af faciliteter,
- uautoriseret afsløring af adgangsdata,
- afbrydelse af driftsafvikling og netværkskommunikation

Risikoanalysen for hvert enkelt system består af:

- en konsekvensvurdering, som foretages af systemejerne (der repræsenterer de forretningsmæssige krav) og
- en sandsynlighedsvurdering, som foretages af både system- og teknikejere.

Analyserne samles i en risikorapport, som skal foreligge inden for den termin, som er angivet i UCC's ISMS. På baggrund af vurderingens anbefalinger træffer ledelsen beslutning om eventuelle ændringer af system-konfiguration, sikkerhedspolitik og andre sikkerhedstiltag.

Ledelsen kan også beslutte at justere de forretningsmæssige forventninger til systemerne.

4. Overordnede retningslinjer

4.1 Formulering af it-sikkerhedspolitik

Det overordnede ansvar for UCC's it-sikkerhed er fastlagt i UCC's overordnede it-sikkerhedsstrategi. For at opnå optimal sikkerhed skal følgende forudsætninger være til stede:

- UCC's ledelse skal have fokus på it-sikkerhed, arbejde med kontinuerlig risikostyring og følge indberetninger fra it-sikkerhedsudvalget
- For at sikre den forretningsmæssigt nødvendige integritet, tilgængelighed og fortrolighed omkring systemer, skal der skabes et tværorganisatorisk ansvar for it-sikkerhed, bl.a. gennem udpegelse af formelle systemejere uden for it-afdelingen.
- It-sikkerhed skal etableres som et fælles ansvarsområde på alle niveauer i organisationen.
- Sikkerhedsmål og -aktiviteter skal baseres på og være i overensstemmelse med den vedtagne it-sikkerhedspolitik.
- Der skal være forståelse for de trusler, institutionen kan blive udsat for, og for institutionens sårbarheder.
- Medarbejdere og studerende skal gøres bekendt med reglerne for den interne it-sikkerhed.
- Klare retningslinjer for it-sikkerhedspolitik og -standard skal fordeles til alle berørte persongrupper, herunder eksterne samarbejdspartnere, gæster m.fl.
- Generel sikkerhedshåndtering skal være anderkendt hos ledelsen, på lige fod med organisationens øvrige styring.

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

Offentliggørelse af it-sikkerhedspolitik

It-sikkerhedspolitikken skal offentliggøres og formidles til alle relevante interessenter, herunder alle medarbejdere og studerende. Der laves en "Læs let"-udgave af it-sikkerhedspolitikken, som henvender sig specifikt til denne målgruppe.

Godkendelse af it-sikkerhedspolitik

It-sikkerhedspolitikken skal efter indstilling i it-sikkerhedsudvalget godkendes af ledelsen.

Sprog for it-sikkerhedspolitik

It-sikkerhedspolitikken skal som udgangspunkt kun eksistere på dansk, som er hovedsproget i organisationen. It-sikkerhedsudvalget kan beslutte, hvilke elementer af it-sikkerhedspolitikken, der evt. skal oversættes til andre sprog.

Omfang af it-sikkerhedspolitik

It-sikkerhed er defineret som de samlede foranstaltninger til at sikre tilgængelighed. Foranstaltninger inkluderer tekniske, proceduremæssige og lovmæssige kontroller.

4.2 Løbende vedligeholdelse

Revision af it-sikkerhedspolitik

På basis af risikovurderingen og den overordnede it-sikkerhedspolitik ajourføres nærværende beskrivelse af it-sikkerhedsforanstaltningerne inden for den termin, der er angivet i UCC's ISMS.

Vedligeholdelse af it-sikkerhedspolitik

It-sikkerhedskoordinatoren har ansvaret for, at organisationens it-sikkerhedspolitikker, regler, procedurer og tilhørende dokumentation bliver vedligeholdt, jf. kommissoriet for it-sikkerhedsudvalget.

5 Organisering af it-sikkerhed

Ansvarsplacering, kontrakter med partnere og andre aftaler er områder, som har vital indflydelse på it-sikkerheden.

5.1 Interne organisatoriske forhold

Ansvarsplacering, udmøntning af de generelle retningslinjer i specifikke forretningsgange og instruktioner, samt den løbende opfølgning, skal pålægges it-sikkerhedsudvalget og skal indgå i sikkerhedsimplementeringen.

It-sikkerhedsudvalget skal endvidere vurdere brud på sikkerheden, nye trusler og sårbarheder samt nye muligheder for sikringsforanstaltninger. It-sikkerhedsudvalget skal også sikre, at disse informationer tilgår ledelsen og indgår i den løbende ajourføring af den overordnede risikovurdering.

Direktionens rolle

Direktionen har det overordnede ansvar for it-sikkerheden hos UCC; ansvaret er dog uddelegeret til it-sikkerhedsudvalget. Direktionen skal støtte UCC's it-sikkerhed ved at udlægge klare retningslinjer, herunder sikkerhedsniveau, have fokus på it-sikkerhed, samt sikre en præcis placering af ansvar.

Koordination af it-sikkerheden

It-sikkerheden koordineres af it-koordinatoren i nært samråd med it-sikkerhedsudvalget samt relevante enheder i it-afdelingen. Rammerne for koordinatorens styring er fastlagt af it-sikkerhedsudvalget og dokumenteres i alle vedtagne styringsværktøjer vedr. it-sikkerhed.

Sikkerhedsorganisation

UCC's it-sikkerhedsudvalg er det forum for it-sikkerhed, som har ansvaret for at sikre, at strategien for it-sikkerhed er synlig, koordineret og i overensstemmelse med UCC's mål. It-sikkerhedsudvalget har ansvaret for den operationelle sikkerhed på UCC's it-systemer, i form af udarbejdelse og godkendelse af it-politikker og –processer. Ansvaret omfatter fx ikke, at medarbejdere og studerende overholder it-sikkerhedspolitikken.

Ansvarsplacering

Der skal placeres en system- og teknikansvarlig for alle it-systemer og al teknik i UCC.

Der skal findes et ajourført register over institutionens kritiske systemer og deres ansvarlige (systemejere). For flerbrugersystemer påhviler ansvaret for sikkerheden som hovedregel den person, der har ansvaret for de data, som systemet indeholder.

For arbejdscomputere skal som hovedregel gælde, at den registrerede bruger er ansvarlig for sikkerheden af de systemer, som computeren har adgang til.

Det vil typisk være systemejeren, som skal foretage konsekvensanalyse i forbindelse med systemets risikovurdering. I praksis kan dette foregå i et samarbejde mellem den systemansvarlige, der håndterer disse data, og teknikejeren (it-afdelingen eller en ekstern leverandør), som har ansvaret for installation og konfiguration af systemet.
Teknikejeren har ansvaret for den daglige drift af systemet.

En afdelingsledelse har ansvar for, at afdelingens medarbejdere anvender det enkelte it-system efter de forskrifter, der kan være beskrevet i it-systempapiret.

It-stamblad

For hvert it-system skal it-afdelingen i samarbejde med systemejeren udarbejde et it-stamblad, som jævnligt vedligeholdes. It-stambladet skal udover faktuelle oplysninger som; Systemansvarlig, Teknikansvarlig, Servicetelefon og Kontraktnumre blandt andet indeholde en klassificering af systemet, der foretages af it-sikkerhedsudvalget.

Periodisk opfølgning

It-sikkerhedsudvalget har ansvaret for at igangsætte og koordinere følgende aktiviteter:

- Ajourføring af den overordnede risikovurdering: Årligt, skal være afsluttet inden for den termin, der er angivet i UCC's ISMS.
- Ajourføring af nærværende beskrivelse af it-sikkerhedsforanstaltninger: Årligt, skal være afsluttet inden for den termin, der er angivet i UCC's ISMS.
- Forslag til ajourføring af sikkerhedspolitik: Årligt, skal være afsluttet inden for den termin, der er angivet i UCC's ISMS.
- Ad hoc forslag til ajourføring af it-sikkerhedspolitikken, hvis eksterne hændelser eller krav giver anledning til dette. It-sikkerhedsarbejdet i UCC's forskellige afdelinger m.v. indgår i den årlige planlægning og opfølgning på lige fod med andre sikkerhedsaktiviteter. It-sikkerhedsudvalget har ansvaret for kontrol og konsekvenser i forbindelse med de foreslåede ændringer.

Fagligt samarbejde med grupper og organisationer

It-sikkerhedsudvalget har ansvaret for at holde sig orienteret om den generelle udvikling på it-sikkerhedsområdet, og for at videregive relevant information inden for UCC regi. It-sikkerhedsudvalget kan til dette formål tage kontakt til andre organisationer, men må i den forbindelse ikke viderebringe oplysninger der kan misbruges til angreb på UCC's it-sikkerhed.

Kontakt med relevante myndigheder

Der er etableret en procedure for håndtering af bevismateriale og eventuelt kontakt med relevante myndigheder.

Forsikring mod hændelser

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

Fortrolighedserklæring ved ansættelse

Alle it-medarbejdere skal senest ved ansættelsestidspunktet underskrive en fortrolighedserklæring; denne kan være en del af ansættelseskontrakten.

5.2 Eksterne samarbejdspartnere

UCC vil i fornødent omfang benytte ekstern assistance.

Fortrolighedserklæring for tredjepart

I de tilfælde, hvor der benyttes ekstern assistance, og hvor denne formodes at få adgang til interne informationer, skal der underskrives en fortrolighedserklæring.

Sikkerhed ved samarbejde med tredjepart

Eksternt service- og rådgivningspersonale pålægges tavshedspligt i henhold til den underskrevne fortrolighedserklæring.

Eksternt personales fysiske tilstedeværelse i datacentret, netrum og lignende, hvor der forefindes systemer i klasse 1 eller 2, skal være overvåget af en it-medarbejder, med mindre der er etableret andre særlige sikkerhedsregler, f.eks. videoovervågning.

Der kan dog af system- og / eller teknikejer dispenseres fra dette krav for eksternt personale med særlig tilknytning til UCC.

Sikkerhed ved samarbejde med partnere

Det kan udgøre en risiko at give en samarbejdspartners medarbejdere adgang til interne faciliteter, blandt andet fordi samarbejdspartnerens styring af sikkerhed kan være utilstrækkelig.

Systemejere har ansvaret for, at it-sikkerhedsrelaterede emner bliver behandlet og inkluderet, når en kontrakt udarbejdes. Systemejeren har ansvar for at videreformidle gældende krav og regler til eksterne samarbejdspartnere. Samarbejdspartnere skal dokumentere, at de overholder disse krav og regler.

Samarbejdsaftaler

For at sikre at UCC's sikkerhedsmålsætning ikke kompromitteres, skal ethvert formaliseret, eksternt samarbejde være baseret på en samarbejdsaftale. I forbindelse hermed kan der oprettes konti for eksterne samarbejdspartnere.

Gæstekonti

UCC tillader gæster (dvs. personer, der ikke har nogen formel tilknytning til UCC) at få adgang til gæstenetværket, når deres behov er relevant for UCC's virke.

Som hovedregel er gæstekonti personlige, men der kan dispenseres ved korte konferencer. Den enkelte bruger skal identificeres på tilfredsstillende måde inden udlevering af gæstekonti.

Gæstekonti skal have en løbetid på maximalt 1 måned og bliver derefter automatisk spærret ved anvendelsen af programmet 'Gæstebruger'.

Gæstekonti udleveres af enten receptionister eller andre medarbejdere, som har tilladelse fra it-sikkerhedskoordinatoren og it-sikkerhedsudvalget.

Gæsteudstyr

Alle, der har en brugerkonto, kan få deres computer tilsluttet til UCC's **interne netværk** (gæstenetværk).

5.3 Outsourcing

Outsourcing

Aftaler om outsourcing indgås mellem den eksterne partner, systemejeren og it-afdelingen. Forslag om outsourcing af it-systemer skal tages op på it-sikkerhedsudvalgsmøder.

Ved outsourcing af it-systemer skal systemejeren hente information om outsourcing-partnerens sikkerhedsniveau og godkende, at UCC's sikkerhed samlet set ikke forringes af outsourcingen, inden indgåelse af en kontrakt.

Outsourcing-partnere

Inden indgåelse af aftaler skal sikkerhedsniveauet hos partneren afklares og sammenlignes med de krav, der stilles til it-sikkerhed i UCC. Outsourcing-partneren bør skriftligt tilkendegive, at vedkommendes it-sikkerhed er tilstrækkelig.

Ekstern revision af outsourcing-partnere

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

6. Styring af systemer og teknik

It-systemer skal beskyttes, uanset om det er fx produktionsudstyr eller computere. Det er derfor nødvendigt at identificere, klassificere og placere ejerskab for alle systemer og teknik.

6.1 Fortegnelse over systemer og teknik

It-aktiver skal identificeres.

Der skal for alle UCC's it-systemer udpeges en ansvarlig systemejer.

Når omfanget af sikringsforanstaltninger for it-systemer og tilhørende teknik er fastlagt, besluttes det, hvordan sikringsforanstaltningerne skal administreres. Herudover skal det besluttes hvordan beskyttelsen revurderes og justeres i forhold til løbende ændringer.

Registrering af it-udstyr

UCC's kritiske, fysiske it-aktiver skal identificeres og klassificeres. Der skal træffes foranstaltninger til sikring af disse aktiver i henhold til deres klassifikation.

It-afdelingen har ansvar for implementering af sikringsforanstaltningerne.

Der udarbejdes opgørelser over hvert enkelt it-aktiv.

Det dokumenteres, hvilke sikringsforanstaltninger der skal beskytte it-aktiverne, hvilke regler ejeren og andre skal følge for at sikringen er effektiv og hvorledes der skal følges op med kontrolforanstaltninger. Det er dokumenteret, hvorledes sikringsforanstaltningerne implementeres, revurderes og vedligeholdes.

Ved en konkret vurdering kan der udføres supplerende sikringsforanstaltninger mod uautoriseret fjernelse, fx mekanisk og/eller elektronisk tyverisikring.

Arbejdspladsudstyr

Alt it-udstyr over et vist minimumsbeløb, som anskaffes af UCC, skal registreres. I forbindelse hermed registreres brugeren, der har ansvaret for udstyret.

Udstyr skal afmeldes i henhold til bestemmelserne i: "Instruks vedr. registrering og udskiftning / afhændelse af apparatur m.m.".

6.2 Ejere af systemer og teknik

Sikkerhedsansvar for systemer og teknik

Der skal udarbejdes en liste over alle it-systemer, der anvendes i UCC. It-sikkerhedsudvalget har i samarbejde med systemejere ansvar for at vedligeholde listen.

Listen skal angive henholdsvis teknikejer og systemejer for hver enkelt system, samt en beskrivelse af ansvar og opgaver vedrørende systemet.

Ansvar for sikkerheden på it-platforme

For alle it-systemer, der er klassificeret som enten kategori 1 eller 2-systemer, skal der udarbejdes et it-stamblad.

Inden hver ændring af it-stambladet foretages en back up af den tidligere udgave, som placeres fysisk adskilt fra systemerne. Hver enkelt systemejer skal godkende opgraderinger og konfigurationsændringer på sit system.

Ansvar for adgangsrettigheder

Chefer og ledere har ansvaret for, at den enkelte medarbejder tildeles netop de brugerrettigheder, som medarbejderens stilling og arbejdsopgaver berettiger til. Proceduren for tildeling af rettigheder afhænger af klassificeringen af det enkelte system. Den systemansvarlige fastsætter regler for tildeling af rettigheder.

Administration af internet-domænenavne

Ansvaret for registrering af domænenavne ligger hos it-chefen eller en medarbejder udpeget af it-chefen.

6.3 Adfærdsregler

Der skal forefindes instrukser vedr. adfærdsregler for:

- Brug af UCC's it-udstyr
- Brug af internet
- Brug af UCC's e-mail
- UCC's trådløse netværk

7. Medarbejdersikkerhed

Menneskelige fejl samt misbrug, berigelse, bedrageri og lignende udgør generelt den største trussel mod it-sikkerheden. Disse risici imødegås ved følgende indsatser:

- Anvendelse af formålstjenlige procedurer ved ansættelse af personale (inkl. vikarer)
- Uddannelse i it-sikkerhed
- Funktionsadskillelse i det omfang, det er muligt
- Regler for servicepersonales adgang til it-aktiver

De personer, der færdes på UCC, kan inddeles i følgende grupper:

- medarbejdere herunder vikarer,
- studerende,
- eksterne samarbejdspartner og konsulenter, herunder it-servicepersonale, samt
- gæster.

Alle disse persongrupper er forpligtiget til at overholde it-sikkerhedsreglerne.

7.1 Sikkerhedsprocedure før ansættelse

Ansættelsesproceduren følger UCC's normale procedurer. Personalepolitikken skal desuden indeholde følgende elementer:

- Fortrolighedserklæring ved ansættelse
- Baggrundscheck af medarbejdere
- Straffeattest
- Indhold i ansættelsesaftalen
- Ansvar for sikkerhed

Beslutningen om ibrugtagning af disse elementer er placeret hos lederen i den enhed, hvor personen skal ansættes.

7.2 Ansættelsesforholdet

7.2.1 Ledelsens ansvar

Det er ledelsens ansvar, at alle medarbejdere:

- er tilstrækkeligt informeret om deres roller og ansvar i forbindelse med sikkerhed, før de tildeles adgang til UCC's systemer og data.
- er gjort bekendt med nødvendige retningslinjer, således at de kan leve op til UCC's it-sikkerhedspolitik.
- bliver motiverede til at leve op til UCC's it-sikkerhedspolitik og retningslinjer.
- opnår et opmærksomhedsniveau i spørgsmål vedrørende it-sikkerhed, der er i overensstemmelse med deres roller og ansvar på UCC.

7.2.2 Uddannelse

Uddannelse i sikkerhedspolitikken

Alle nye medarbejdere skal ved tiltrædelsen modtage en henvisning til UCC's it-sikkerhedspolitik. Chefen for den ansættende enhed har ansvaret for, at nyansatte medarbejdere instrueres i UCC's regler for it-sikkerhed og konsekvenserne - for UCC og for medarbejderen - af brud på sikkerhedsreglerne.

Desuden skal alle medarbejdere modtage information om de vigtigste elementer i UCC's it-sikkerhedspolitik. Alle it-brugere skal løbende modtage informationer om overholdelse af UCC's it-sikkerhedspolitik.

Sikkerhedsuddannelse for it-medarbejdere

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

7.2.3 Sanktioner

Overtrædelse af eller forsøg på brud med reglerne for it-sikkerhed kan medføre disciplinære foranstaltninger.

Disciplinære foranstaltninger skal iværksættes efter en samlet vurdering af overtrædelsens omfang og karakter.

Der kan i visse tilfælde ligeledes blive tale om politianmeldelse og eventuelt erstatningskrav for forvoldt skade.

Medarbejdere

For medarbejdere behandles overtrædelsen af reglerne i overensstemmelse med UCC's personalepolitiske retningslinjer og almindelige ansættelsesretlige regler.

HR-afdelingen skal altid konsulteres, inden der tages stilling til de disciplinære foranstaltninger.

Studerende, eksterne samarbejdspartner og konsulenter, herunder it-servicepersonale og gæster

For studerende kan overtrædelse af reglerne for it-sikkerhed medføre brug af følgende sanktioner:

- mundtlig påtale,
- skriftlig advarsel,
- inddragelse af brugerrettigheder i kortere eller længere perioder,
- hel eller delvis bortvisning fra UCC.

Beslutning om sanktioner træffes normalt af den lokale leder.

Det er for studerende vedkommende et lokalt ansvar at træffe afgørelse om sanktioner.

Der arbejdes pt. på udarbejdelse af "Ordensregler for studerende ved Professionshøjskolen UCC", indtil disse foreligger, afgør uddannelseschef – leder sanktionens størrelse.

7.3 Ansættelsens ophør

7.3.1 Returnering af it-udstyr ved aftrædelse

Medarbejderen skal aflevere alt udleveret it-udstyr ved samarbejdets ophør. Udstyret skal afleveres til it-afdelingen

7.3.2 Inddragelse af rettigheder ved fratrædelse

Der forefindes en opdateret procedure for inddragelse af rettigheder i forbindelse med fratrædelse eller afskedigelse af personale. Dette er beskrevet i: "It-politik og -proces ved ophør af ansættelsesforhold ved UCC", der er placeret på UCC's fælles intranet.

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

7.3.3 Fortrolighedserklæring ved fratrædelse

Ved fratrædelse skal der gøres opmærksom på gældende fortrolighedsaftaler.

7.3.4 Adgang til medarbejders personlige data

Adgang til en medarbejders personlige data kan i forbindelse med langvarig sygdom eller ophør på en leders foranledning videregives til en anden medarbejder.

8. Fysisk sikkerhed

Fysisk sikkerhed og adgangsregler er naturlige elementer i UCC's sikkerhedspolitik. Fysisk sikkerhed omfatter blandt andet døre, vinduer, alarmer, samt tyverisikring af UCC's fysiske aktiver, eksempelvis it-udstyr. Systemer til adgangskontrol er ligeledes et element af fysisk sikkerhed, der sikrer, at kun personer med legalt ærinde får adgang til UCC's private og særligt sikrede områder.

8.1 Sikre områder

Det skal vurderes, hvordan en bygning og dens omgivelser hensigtsmæssigt kan opdeles i sikkerhedsområder i henhold til it-funktionernes forskellige sårbarhed.

Indretning og placering af it-funktioner skal tilrettelægges således, at de forskellige personalekategorier kan færdes i bygningen, uden at sikkerhedsregler tilsidesættes.

Offentlige områder

UCC's bygninger er som undervisningsinstitution åbne og tilgængelige uden kontrol i en stor del af døgnet. Bygningerne må derfor betragtes som halvprivat sikkerhedsområde, dvs. "at det kun i begrænset omfang er muligt at kontrollere personers adgang".

Bygningsskallen er som udgangspunkt aflåst i tidsrummet kl. 22:00 - 07:00 på hverdage, samt i weekender og helligdage, men bygningsskallen kan være ikke-aflåst som følge af forskellige retningslinjer på UCC's lokationer eller arrangementer om aftenen og i weekender.

Når bygningerne er aflåst, foregår adgang for autoriserede brugere enten via ADK-systemet eller med nøgle.

Adgang til datacenter og krydsfelter

Placering af de administrative it-systemer og netværkskomponenter er angivet i it-beredskabsplanen. Adgang til datacenter og krydsfelter tildeles kun autoriserede it-medarbejdere, eller ved adgang overvåget af it-medarbejdere.

Adgang til datacentre og it-klargøringsrum

It-chefen er ansvarlig for godkendelse af personale, der har adgang til de sikre områder. Dette ansvar kan uddelegeres til ledere i it-afdelingen.

Sikre områder skal placeres, så gennemgang gennem et højere klassificeret rum ikke er nødvendig for at nå til et mindre klassificeret rum.

Adgangen skal beskyttes med kodelås med individuelle koder for de enkelte medarbejdere.

It-aktiver skal beskyttes mod risiko for ødelæggelse og forstyrrelser fra omgivelserne. Som fx trusler fra ild, røg, vandskade, støv, vibrationer, kemiske påvirkninger, forstyrrelser i infrastrukturen eller elektromagnetisk stråling.

Reserveanlæg, udstyr eller datamedier med sikkerhedskopier skal opbevares i sikker afstand fra hovedanlæg, adskilt med barrierer.

Aflåsning af krydsfelter og lignende teknikrum

Krydsfelter skal placeres i aflåste skabe.

Indbrudsalarmer

UCC skal anvende tilstrækkelige alarmsystemer i alle lokaler med it-udstyr, der indeholder fortrolige informationer.

Overvågning i sikre områder

It-afdelingen skal sikre, at arbejde i sikre områder så vidt muligt bliver overvåget.

Optageudstyr i sikre områder

Uautoriseret optageudstyr er ikke tilladt i sikre områder.

Oplysninger om sikre områder

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

Sikring af kontorer, lokaler og udstyr

Vinduer i lokaler, hvor der foregår it-driftsafvikling, skal lukkes, når lokalerne forlades uden overvågning.

Hvor en risikovurdering angiver det, skal sikringen af vinduer i de underste etager suppleres med mekanisk beskyttelse.

Registreringen af indbrud skal udløse en reaktion, som er afstemt efter it-aktivernes værdi og de foreliggende mekaniske sikringsforanstaltninger.

UCC'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.

Brug af personlige adgangskort

Personers adgang til og ophold i sikkerhedsområder skal registreres og kontrolleres i henhold til reglerne i UCC's ISMS.

Nøgle og/eller adgangskort skal udleveres mod kvittering. Modtageren skal instrueres om, at det kun er til eget personligt brug, og at bortkomst straks skal meldes. Personer, der får udleveret nøgle og/eller adgangskort, skal registreres.

Personale der fratræder, skal have deres adgangsmuligheder inddraget.

Miljømæssig sikring af datacenter

Datacenter, krydsfelter og tilsvarende områder skal på forsvarlig vis sikres mod miljømæssige hændelser som brand, vand el. lign.

Aflåsning af lokaler og bygninger

It-anlæg, it-funktioner, installationer og udstyr til energiforsyning, telekommunikation og sikringsanlæg skal beskyttes mod sikkerhedstrusler, ulykker fra omgivelserne, samt mod uautoriseret adgang.

Nøgle- og låsesystemer skal være konstruerede, så de yder beskyttelse mod uautoriseret adgang til lokaliteter med adgangsbegrænsning.

Ansvar for den fysiske adgangskontrol

It-sikkerhedskoordinatoren har det overordnede ansvar for administration af den fysiske adgangskontrol til it-områder.

Gæsters adgang

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

8.2 Beskyttelse af udstyr

Placering af udstyr

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

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

Systemer skal så vidt muligt fordeles på flere datacentre, så at et alvorligt uheld i et rum ikke standser al it-aktivitet.

Centralt netværksudstyr er i et vist omfang dubleret og fordelt i flere datacentre.

Automatisk overvågning af datacentre skal etableres, så forsyningssvigt registreres så tidligt som muligt, for at minimere generne på it-udstyr.

Opsyn med mobile enheder

Mobile enheder, som fx bærbare computere, tablets, PDAer og mobiltelefoner, bør anvendes med omtanke. Eksempelvis kan en efterladt mobil enhed udgøre en it-sikkerhedsrisiko.

Adgang til data på bærbare computere skal beskyttes med et login-password.

Sikring af kabler

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

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

Forsyningssikkerhed

Leverandørens krav til omgivelsesbetingelser (temperatur, luftfugtighed, støvindhold m.v.) for it-systemer skal overholdes. Om nødvendigt skal der installeres ventilations- og/eller køleanlæg.

UCC's datakommunikation såvel internt som eksternt skal, så vidt det er muligt inden for økonomiske og tekniske rammer, sikres mod bevidst ødelæggelse via 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 el-forsyning skal være tilgængelige og kendte af autoriseret personale.

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

Leverandørens krav til spændingskvalitet og jordforbindelse skal opfyldes.

It-udstyr skal el-forsynes fra egen gruppe.

Beskyttelse mod udstråling

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

Der er ikke truffet særlige forholdsregler mod elektromagnetisk aflytning.

Kameraer

Der må ikke fotograferes i UCC's særlige sikkerhedsområder uden tilladelse fra it-chefen eller it-sikkerhedskoordinatoren.

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, jf. persondataloven, herunder licenserede og brugerprogrammer ikke kommer uden for UCC. Dette sker enten ved at datamediet bliver slettet eller ved destruktion.

Der henvises endvidere til "Lov om personoplysninger".

For beskadigede datamedier, der indeholder følsomme eller fortrolige data, skal dataejeren afgøre, hvorvidt datamediet skal destrueres totalt eller repareres. Ved reparation skal der indhentes tavshedserklæring fra reparatøren. Skal reparationen ske i udlandet skal Datatilsynet være orienteret inden forsendelsen ud af Danmark, jfr. "Lov om personoplysninger".

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

Vedligeholdelse af udstyr og anlæg

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

Udstyr, herunder 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.

Servicetelefon- og kontraktnumre skal være anført i det enkelte systems it-stamblad.

Brandsikring

Datacenteret skal sikres med veldimensioneret brandslukningsudstyr.

Datacenteret må ikke benyttes som lager for brændbare materialer. Farlige eller brandfarlige materialer skal lagres i sikker afstand fra sikre områder.

Gennembrydning mellem brandceller skal sikres med godkendt brandtætning.

UCC's bygninger er i overvejende grad forsynet med ABA-anlæg. Hvor der er etableret ABA-anlæg, er den tilhørende varsling udført i henhold til forskrifterne.

Brandslukningsanlæg skal som minimum være håndslukningsanlæg, som placeres let tilgængeligt, så en begyndende brand hurtigt kan slukkes. Typen på håndslukkere (kulsyre, pulver, vand, inertgas) skal tilpasses slukningsformålet. Håndslukkere skal være godkendt og mærket i henhold til Dansk Standard. Slukningsudstyret skal kontrolleres regelmæssigt.

Personalet skal informeres om udstyrets tilstedeværelse og instrueres i brugen af det.

UCC har ikke etableret lynbeskyttelse.

Tyverimærkning af it-udstyr

Alle computere skal have en permanent beskyttelsesmærkning med UCC som ejer.

Køling

Datacenter 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, som giver akustisk og visuelt signal ved tilstande uden for grænseværdierne.

Nødstrømsanlæg

It-udstyr i klasse 1 skal el-forsynes via nødstrømsanlæg (UPS). Den nuværende UPS kan udelukkende anvendes til nedlukning.

Man bør overveje, om It-udstyr i klasse 2 skal forsynes via nødstrømsanlæg.

9. Styring af netværk og drift

Vedligeholdelse og opdatering af it-systemer er nødvendigt for at opretholde et passende sikkerhedsniveau for UCC. Drift af it-systemer indebærer elementer af overvågning af systemernes helbredstilstand, opdatering og sikkerhedskopiering af data.

De fleste it-systemer i dag er afhængige af netværk, og derfor er administration, opbygning, sikring og vedligehold af netværk vitalt for UCC. Den trussel, som uautoriseret adgang udgør, gør det nødvendigt at have klare regler for brugen af UCC's netværk samt overvågning af infrastrukturen.

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

9.1 Operationelle procedurer og ansvarsområder

Lederen af It Infrastrukturenheden har ansvaret for, at driftsafvikling på it-systemer og netværk er styret og defineret. Styringen skal understøttes af driftsinstruktioner og reaktionsprocedurer til imødegåelse af uønskede hændelser.

Funktionsadskillelse skal gennemføres, så vidt det er hensigtsmæssigt og muligt, for at reducere risici på grund af skødesløshed eller overlagt misbrug.

Der skal gennemføres rutinemæssige procedurer for sikkerhedskopiering af data, samt drifts-, hændelses- og fejllogning. Hvor procedurerne foreskriver det, skal udstyr og lokaler m.m. overvåges.

9.1.1 Driftsafvikling

Der skal være procedurer for, hvordan og hvornår driftsafvikling skal foregå. Medarbejdere i Infrastrukturenheden skal instrueres og trænes i driftsafvikling af de enkelte it-systemer og eventuelle tilsluttede netværk.

Disse medarbejdere skal instrueres i, hvad der skal sikkerhedskopieres, hvor ofte det skal ske, hvor kopierne skal opbevares og for hvilken periode. Desuden skal de instrueres i de genstarts- og reetableringsprocedurer, der skal tages i anvendelse, hvis der opstår fejl i driftsafviklingen.

Der skal forefindes driftsafviklingsprocedurer for alle Kategori 1 it-systemer, som drives af UCC.

Driftsansvar

It-medarbejdere i Infrastrukturenheden er ansvarlige for drift, administration og sikkerhed på netværket og de fælles it-systemer, herunder efterlevelsen af sikkerhedspolitikker, regler og procedurer.

Dokumentation

It-afdelingen har ansvaret for, at alle systemer og it-relaterede forretningsgange er dokumenterede.

Indkaldelse af medarbejdere i vagtordning og ekstra personale

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

Deaktivering af beskyttelsesmekanismer

Det er under ingen omstændigheder tilladt at deaktivere eller omgå UCC's beskyttelsesmekanismer, herunder deaktivering af antivirus-produkter, adgangskontrol eller lignende.

9.1.2 Styring af ændringer

Retningslinjer for ændringer

Der opstår jævnligt behov for, at basisprogrammer til operative systemer og netværkssystemer ændres. Det kan fx være nødvendigt at opdatere til en ny udgave, eller der kan være behov for at tilføje nye programmer eller systemer for at støtte driftsafvikling, netværk og brugersystemer.

Ved sådanne ændringer skal det kontrolleres, at it-sikkerheden for de enkelte brugersystemer ikke forringes. For det enkelte it-systemer skal der forefindes en opdateret fortegnelse (it-stamblad) over:

- de operativsystemer og andre programmer, som it-systemet anvender til styring og kontrol. Fortegnelsen kan indeholde en henvisning til de respektive leverandørers dokumentationer af programmer og de tilhørende dokumentationer af driftsinstrukser.
- de brugersystemer og netværk, som it-systemet styrer og kontrollerer, inklusive henvisninger til de respektive driftsinstrukser.

Information om udførte ændringer skal formidles til interessenter.

Systemejeren har ansvaret for, at al basissoftware er afprøvet og godkendt, inden det sættes i drift. Systemejeren har ansvaret for, at systemets it-stamblad bliver ajourført.

Der udarbejdes en samlet oversigt på baggrund af it-stambladene. Denne oversigt benyttes ved den it-systemsansvarliges vurdering af CERT's og andre sikkerhedsorganisationers og leverandørers anbefalinger til sikkerhedsrettelser. Dette gælder for det kørende basissoftware og de kørende applikationer.

Enhver opgradering og sikkerhedsrettelse skal være aftalt mellem systemejer og teknikejer for at sikre, at der ikke er evt. kompatibilitetsproblemer mellem nye versioner af basissoftware og applikationer. Ved større opgraderinger skal it-sikkerhedskoordinatoren inddrages.

Planlægning, test og godkendelse af ændringer

Ændringer skal planlægges og afprøves, inden de sættes i drift. Systemejeren kan i samarbejde med teknikejeren beslutte at der undtagelsesvis ikke skal gennemføres en afprøvning inden en idriftsættelse.

Ændringernes konsekvenser skal vurderes inden idriftsættelse.

Ændringer skal igennem en formaliseret godkendelsesprocedure inden idriftsættelse.

Systemejeren kan opstille krav til og kriterier for nye systemers godkendelse, inden de tages i brug. Nye systemer, såvel hardware som software, skal afprøves, inden de godkendes.

Styring af ændringer hos serviceleverandører

UCC skal sikre, at ændringsstyring af en serviceleverandørs ydelser følger samme retningslinjer som UCC's egne.

Ændringer i forretningskritiske systemer

Alle ændringer i forretningskritiske systemer udføres efter godkendt procedure. Alle procedurer skal indeholde en alternativ plan til reetablering af det forretningskritiske system. Vilkårene for aktivering af den alternative plan skal ligeledes fremgå af proceduren.

Sikring af serversystemer

Servere skal konfigureres i henhold til gældende standarder.

Sikring af arbejdscomputer inden ibrugtagning

Alle arbejdscomputere skal sikres inden brug. Minimum sikring indebærer installation af seneste sikkerhedsrettelser for operativsystemet og antivirusprogram.

UCC's arbejdscomputere opdateres løbende vha. centralt administrationssoftware. Der tages ikke backup af arbejdscomputerne. I øvrigt henvises til det materiale, der beskriver back up og restore procedurer i UCC.

Softwareopdateringer generelt

UCC's it-medarbejdere skal holde sig informeret om alle programrettelser til alle programmer, der anvendes i UCC. Når det vurderes, at rettelserne påvirker den samlede sikkerhed positivt, skal it-medarbejderne sikre, at de bliver installeret på alle computere, som de har ansvaret for.

9.1.3 Funktionsadskillelse

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

Adgang til produktionsdata

Idet systemadministratorers har adgang til fortrolige oplysninger skal alle systemadministratorer registreres.

Sikring af forretningskritiske systemer

Forretningskritiske systemer skal beskyttes ved hjælp af funktionsadskillelse, så risikoen for misbrug af rettigheder minimeres. Hvor funktionsadskillelse ikke er muligt, skal kompenserende tiltag implementeres.

9.1.4 Adskillelse mellem udvikling, test og drift

Adskillelse af udvikling, test og drift

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

Til it-systemer i kategori 1 er der oprettet separate udviklings-/testmiljøer, hvor nyudviklede/nyanskaffede faciliteter samt fejlrettelser kan afprøves inden overførsel eller installation i produktionsmiljøer. Systemer, hvor der ikke kan opsættes realistiske testmiljøer, skal afprøves inden for de aftalte service-vinduer.

9.2 Ekstern serviceleverandør

Ved brug af eksterne serviceleverandørers styring af driftsafvikling skal risici identificeres. Sikkerhedsforanstaltninger skal aftales og fremgå af driftsservicekontrakten. Anvendelsen af ekstern databehandling skal ske efter Persondatalovens retningslinjer.

Sikkerhedsregler skal i hvert enkelt tilfælde aftales med eksterne serviceleverandører. Hvis de skal have adgang til systemerne, skal de underskrive UCC's godkendte fortrolighedsaftale. Det vil være ønskeligt med en revisorerklæring fra den eksterne leverandør.

9.3 Styring af driftsmiljøet

Sikkerhed i systemplanlægning

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

Inden ibrugtagning skal driftsafviklingssystemer, netværk og brugersystemer afprøves. Testen skal godkendes af både systemejer og teknikejer.

Ved større ændringer af eller anskaffelse af nye kritiske systemer udarbejdes en kravspecifikation som grundlag for en evt. tilbudsgivning / udbudsforretning. Der etableres en projektorganisation for gennemførelsen af tilbud / udbudsforretningen, samt efterfølgende test, godkendelse og implementering.

Ved systemer, UCC har anskaffet i fællesskab med andre institutioner (f.eks. Økonomi, Løn og Studieadministration), skal styring, test og implementering gennemføres i et samarbejde med disse institutioner.

Ved systemændringer og - opdateringer skal afprøvning som hovedregel ske ved en grundig afprøvning af et testsystem med samme funktionalitet som produktionssystemet i henhold til kravene for systemets klassificering.

Afprøvning skal ske i samarbejde mellem systemejer og teknikejer. Produktionssystemerne ændres/opgraderes og afprøves med så få ulemper for brugerne som muligt.

Kapacitetsplanlægning

It-systemernes dimensionering skal afpasses efter kapacitetskrav. Belastning skal overvåges, således at opgradering og tilpasning kan finde sted løbende. Dette gælder især for forretningskritiske systemer.

It-afdelingen vurderer løbende i samarbejde med systemejerne kapacitetsbehov for netværk og maskinel.

Reservekapacitet skal koordineres, og kravene til reservekapacitet skal med fastlagte mellemrum revurderes.

Integration af informationssystemer

Hvis integration af et informationssystem resulterer i en forøget risiko, skal denne vurderes og godkendes af it-sikkerhedsudvalget.

9.4 Skadelige programmer og mobil kode

It-systemer er sårbare over for uautoriserede indgreb eller ændringer. Derfor skal de beskyttes mod indvirkninger fra ondsindede programmer (trojanske heste, orme, logiske bomber, virus, mv.) – i daglig tale vira. Beskyttelse mod vira hviler grundlæggende på brugernes opmærksomhed på sikkerheden. Derfor skal brugerne instrueres i beskyttelse mod vira.

Ejere af it-aktiver skal være på vagt over for vira. Især skal behovet for sikringsforanstaltninger, som kan opdage og beskytte mod vira, overvejes. Flytbare datamedier af fremmed oprindelse skal - ligesom data modtaget via eksterne netværk - kontrolleres for virus, inden de anvendes på systemerne. Eneste undtagelse er data fra it-systemer, der med sikkerhed vides at være fri for virus.

Virusbekæmpelsesplanen består af følgende elementer:

- al elektronisk post til og fra UCC skannes for spam i UCC's centrale mailgateway eller lignende.
- alle arbejdscomputere og lokale servere har, hvor det er muligt, antivirussoftware. Dette giver en aktiv beskyttelse idet alle filer automatisk skannes, når de åbnes, og bliver blokeret i tilfælde af fare for smitte.
- På arbejdscomputere og lokale servere skal permanente filer skannes.

Der skal være et virusberedskab, som dagligt administrerer overvågningssystemet og analyserer alle alarmer fra virusbeskyttelsen.

Antivirus-produkter på arbejdscomputere

Hvor det er muligt skal it-udstyr, der er tilsluttet UCC's datanet, have et aktivt og opdateret antivirusprogrammel installeret. Dette gælder også udstyr, som tilsluttes netværket via fjernopkobling, f.eks. hjemmefra.

Antivirus-produkter på servere

Der skal så vidt muligt være installeret antivirus-beskyttelse på alle serversystemer.

Styring af antivirus

It-afdelingen skal kunne styre antivirus-software på alle systemer fra en central lokation. Med styring menes tvungen opdatering, scanning og oprydning.

9.5 Sikkerhedskopiering

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

- hvilke data og programmer, der skal sikkerhedskopieres,
- hvor hyppigt data og programmer skal sikkerhedskopieres og i hvor mange eksemplarer,
- at den backupansvarlige har ansvaret for, at sikkerhedskopierne opbevares betryggende.

Sikkerhedskopier skal gives samme fysiske beskyttelse som it-aktiverne, de sikrer. Sikkerhedskopiens anvendelighed skal testes med jævne mellemrum.

Sikkerhedskopiering af data på serversystemer

It-afdelingen er ansvarlig for sikker lagring og backup af data på serverudstyr.

For it-systemer, hvor der stilles særlige myndighedskrav om opbevaring af data i længere tid, skal der udarbejdes en udvidet backup-procedure.

Overvågning af procedurer for sikkerhedskopiering

Muligheden for at reetablere data fra backup-systemer skal regelmæssigt testes i et testmiljø. Endvidere skal reetablering testes efter system- eller procesændringer, som kan påvirke backup-rutiner.

Sikkerhedskopiering af data på andre systemer

På arbejdscomputere anbefales det, at brugerdata ikke lagres lokalt på computeren. Brugerdata skal lagres på filservere i mapper for personlige eller fælles data. Hvis ejeren alligevel vælger at lagre data lokalt, er det dennes ansvar, at der forefindes sikkerhedskopier.

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

Opbevaring af sikkerhedskopier på ekstern lokation

Backup-systemer til reetablering af forretningskritiske systemer skal placeres i sikker afstand fra produktionssystemet.

I øvrigt henvises til beskrivelse af back up- / restore-procedurer, som er godkendt at it-sikkerhedsudvalget.

9.6 Netværkssikkerhed

It-afdelingen har ansvaret for det totale netværk. It-afdelingen skal løbende sørge for at gøre status over belastningen af datanettet og budgettere nødvendige udbygninger.

Sikring af netværk

UCC's datanet skal overvåges med et overvågningssystem. Der føres statistik over trafikken på datanettets hoveddele vha. et webbaseret program.

Trafikken på UCC, dvs. data fra de centrale netværksenheder, logges i UCC's firewall. De indsamlede logs skal bl.a. bruges til:

- at afsløre detaljer i tilfælde af hacking eller andet misbrug af UCC'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 UCC's netværk.
- at løse driftsmæssige problemer med opkoblinger gennem firewall'en.

Adgang til aktive netværksstik

Adgang til aktive netværksstik skal kontrolleres.

Det skal sikres, at der ikke forefindes ubenyttede, aktive netværksstik i offentligt tilgængelige rum som gange, kantiner og lignende.

Installation af netværksudstyr

Det er ikke tilladt at installere netværksudstyr på UCC's netværk uden forudgående sikkerhedsgodkendelse fra it-afdelingen.

Tilslutning af udstyr til netværk

Generelt må kun it-afdelingen koble udstyr på det interne netværk, men it-afdelingen kan uddelegere retten til at opkoble udstyr.

Fjernstyring og administration

Adgangen til fjernadministration af de forretningskritiske, interne applikationer tillades efter godkendelse fra medarbejderens chef/leder.

Beskyttelse af diagnose- og konfigurationsporte

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

Opdeling af netværk

UCC's netværk er opdelt i et antal virtuelle netværk (VLAN), hvor al trafik mellem de enkelte VLAN's skal kontrolleres af den centrale firewall.

Rutekontrol

It-afdelingen skal begrænse routning imellem forskellige netværkssegmenter, således at kun nødvendig trafik videresendes.

Opsætning af udstyr, der ruter trafik, skal forhåndsgodkendes eller installeres af it-afdelingen.

Kryptering af administrative netværksforbindelser

Forbindelser, der benyttes til it-administration, skal krypteres, hvis de benytter offentlige eller usikre netværk, fx internet.

Firewall-funktioner på servere

Alle servere med indbygget firewall-funktionalitet skal benytte denne til at sikre, at der kun gives adgang til nødvendige services.

Personlige firewalls

Alle arbejdscomputere skal benytte firewalls.

9.6.1 Trådløse netværk

Al trådløst netværk skal udelukkende etableres af it-afdelingen.

Brug af trådløse lokalnetværk

Brug af trådløse netværk tillades for alle med gyldigt brugernavn/kodeord.

Der er etableret trådløst netværk på alle UCC's geografiske lokationer. Dette omfatter:

- medarbejdernet
- studerende net
- gæstenet

Brugerne af de trådløse gæstenetværk er selv ansvarlige for beskyttelse af deres klienter, da de indbyggede sikkerhedsfaciliteter ikke er slået til på access-punkterne.

Det trådløse gæstenetværk betragtes som et usikkert, ubeskyttet netværk. Dette netværk anvendes af private computere og giver begrænsede rettigheder til anvendelse af resurser. Anvendelse af netværk for medarbejdere og studerende kræver, at computeren er medlem af domænet. Anvendelse af disse netværk giver adgang til de samme resurser som de trådede netværk.

Adgang til trådløse netværk for gæster

Gæster, hvis identitet er kendt, må få udleveret et kodeord til gæstenettet og tilslutte eget udstyr til netværket, forudsat at udstyret ikke generer andre systemer. Dette sker ved oprettelse af en 'Gæstebrugerkonto', samt ved oprettelse af fælles gæstekonti i forbindelse med korte konferencer.

9.7 Elektroniske forretningsydelser

Offentligt tilgængelig information

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

9.8 Logning og overvågning

Alle væsentlige systemer skal så vidt muligt overvåges og logges. Driftslogning etableres med henblik på kontrol og eftersporing.

Det fysiske driftsmiljø i datacentret skal overvåges.

Datanet og flerbrugersystemer overvåges via et centralt overvågningssystem, som i tilfælde af kritiske fejl alarmerer den systemansvarlige/vagthavende it-medarbejder via SMS/e-mail.

Kapacitetsovervågning

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

Overvågning af systemanvendelse

Overvågningsniveauet skal bestemmes ud fra en risikovurdering for det individuelle system, og alle overvågningsaktiviteter skal beskrives.

Af driftstekniske, sikkerhedsmæssige og/eller afregningsmæssige årsager, sker der en løbende, automatisk registrering af alle aktiviteter på de fleste it-systemer. Denne overvågning sker automatisk og kræver ikke brugernes godkendelse.

Ved mistanke om misbrug har systemadministratorer og de netværksansvarlige ret til at overvåge aktiviteterne, herunder ind- og udgående e-mail, uden på forhånd at informere brugerne herom. En sådan overvågning kan kun ske med den lokale chefs forudgående tilladelse.

Hvor lovgivning kræver det, skal anvendelsen af it-systemer registreres med henblik på afklaring af uregelmæssigheder.

Systemlogs fra alle it-systemer, der er klassificerede i kategori 1, skal opsamles på de enkelte servere. Som minimum skal al "logon"-information logges, dvs. adgang til applikationer/services på systemet.

Logs skal opbevares online på de enkelte servere, og de skal indgå i den normale backup procedurer.

Overvågning af netværk

It-afdelingen skal have den nødvendige viden om og redskaber til overvågning af UCC's netværk, for eksempel fejlretning, detektering og sporing af sikkerhedshændelser.

It-afdelingen skal løbende overvåge netværket med henblik på at opdage og registrere sikkerhedsbrud.

Der skal føres statistik over trafikmængden på netværket. Målingerne foretages på de primære netværks- og serverforbindelsers routerinterfaces. Trafik til og fra arbejdscomputere måles kun ved særlige behov.

Overvågning af internetforbindelser

It-afdelingen skal løbende overvåge internetforbindelser med henblik på at opdage og registrere elektroniske angreb.

Registrering af driftsstatus

Fejl, som opstår i forbindelse med driftsafvikling af kritiske systemer, skal logges og rapporteres. Udbedring af fejl skal dokumenteres.

Brugerne skal holdes orienteret om fejl og status på fejlretning via UCC's driftsstatus-hjemmeside. Denne side skal være tilgængelig, selv når der er nedbrud på UCC's øvrige it-systemer. Der skal være klare instruktioner og procedurer for logning og behandling af rapporterede fejl. Ejeren af et brugersystem skal godkende afhjælpninger.

Fejlrettelser skal gennemgås for at sikre, at fejlene er blevet rettet tilfredsstillende, herunder at sikkerhedskontrollerne ikke er blevet kompromitteret, og at de indgreb, der er sket, er autoriserede.

Tilgængelighedshændelser

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

Skanning af netværk og systemer

For at opretholde et tilfredsstillende sikkerhedsniveau skal der skannes efter uønskede åbne porte, vira, uønskede tjenester m.v. Skanning må kun udføres af it-medarbejdere eller efter aftale med eksterne samarbejdspartnere.

Skanning på it-systemer skal normalt annonceres til de berørte områders systemejere passende tid i forvejen. Hvis skanning af netværkssegmenter ikke foretages af netværksansvarlige for de pågældende segmenter, skal det annonceres til de netværksansvarlige passende tid i forvejen.

Skanning skal udføres på en sådan måde, at belastning på netværk og systemer ikke forhindrer systemernes drift.

Det er ikke tilladt at skanne eksterne netværk fra UCC's netværk.

Opfølgningslogning

Sikkerhedshændelser, fejlhændelser og væsentlige brugeraktiviteter på UCC's systemer i kategori 1 og 2 skal logges.

Uønskede hændelser skal så vidt muligt kunne spores.

Administratorlog

Aktiviteter udført af systemadministratorer og –operatører, samt andre med særlige rettigheder, skal logges.

Fejllog

Fejllogs fra alle it-systemer, der er klassificeret i kategori 1, skal opsamles på den centrale logserver, hvor de skannes automatisk for uregelmæssigheder. Rapporter sendes til den vagthavende it-medarbejder.

Beskyttelse af log-oplysninger

Log-faciliteter og log-oplysninger skal beskyttes mod manipulation og tekniske fejl.

Tidssynkronisering

Driftsanlægs 'ure' skal være synkroniserede med eksterne tidsservere af hensyn til korrekte registrerings- og logningsinformationer.

Revisionsspor

Brugertransaktioner bør indgå på linie med de øvrige systemlogninger dels for efterfølgende sporing og dels for en efterkontrol af evt. uautoriserede søgninger, fremvisninger eller anden databehandling. Logningen bør indeholde følgende data:

- Tidspunkt
- Lokationsinformation – afdeling og maskinidentifikation
- Brugeridentifikation – en entydig angivelse af den pågældende bruger
- Reference til transaktionstypen.

Der skal foretages logning af relevante transaktioner dels på operativsystemniveau (fx log on og log off) og dels i de enkelte delsystemer.

Logning kan bruges både til løbende kontrol af transaktioner for at finde sikkerhedsbrud og til efterfølgende opsporing som opfølgning på konstaterede sikkerhedsbrud.

Der skal efter nærmere fastsatte retningslinier foretages rutinemæssig gennemgang af loggen for at identificere uregelmæssigheder.

Logningerne kan inddeles i niveauer svarende til deres grad af brud på IT-sikkerheden:

- Niveau 1 – autoriseret adgang af en godkendt bruger (intet brud)
- Niveau 2 – uautoriseret eller unormal adgang af en godkendt bruger
- Niveau 3 – adgang uden normal log on (alvorligt brud).

10. Adgangsstyring

Adgangen til at udføre handlinger på UCC's it-systemer skal beskyttes af autorisationssystemer. Systemerne har til formål at sikre mod uautoriserede ændringer, ordrer, fejl og svindel. UCC's medarbejdere skal medvirke til beskyttelse af it-aktiverne gennem korrekt brug af autorisationssystemerne.

10.1 De forretningsmæssige krav til adgangsstyring

Systemer til styring af adgangskoder

Så vidt muligt skal der benyttes it-systemer, som automatisk kan styre kravene til adgangskoder angivet i afsnittet "Adgangskoder og metoder"

Sikker log-on

Log-on-grænsefladen skal give mindst mulig information om det system, man forsøger at opnå adgang til. Det samme administratorkodeord bør ikke anvendes på maskiner inden for og uden for UCC's firewall.

Retningslinjer for adgangsstyring

Retningslinjerne skal omfatte følgende punkter:

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

Adgangen til netværk skal administreres af it-afdelingen.

Adgang til fælles systemer, infrastruktur og ydelser skal administreres af it-afdelingen.

Brugerrettigheder til fælles administrative systemer (SIS, ØSS, Navision, m.fl.) skal tildeles af den pågældende systemansvarlige.

Der skal foreligge en præcis beskrivelse af, hvordan en bruger oprettes og nedlægges. (Medarbejderes konti bør principielt ikke slettes, men blot spærres for at undgå genbrug af kontonavnet).

Registrering af brugere

Hver medarbejder skal udstyres med et "over tid unikt"-brugernavn, således at forveksling aldrig kan forekomme. Derudover skal det sikres med en adgangskode, som skal overholde den aftalte policy for medarbejderes adgangskoder.

Der skal oprettes en postkasse til medarbejderen i UCC's fælles postsystem.

Afhængigt af medarbejderens arbejdsopgaver kan vedkommende have adgang til programmer og dele af netværk med egne autorisationssystemer, fx SIS, ØSS, Navision.

Såfremt en bruger glemmer sit kodeord, skal Servicedesk på betryggende måde sikre sig brugerens identitet inden udlevering af et nyt kodeord. Brugeren kan også vælge at henvende sig til en administrativ medarbejder, som har rettigheder til at tildele et nyt kodeord.

Al it-anvendelse skal i videst muligt omfang kunne spores tilbage til en person.

Der skal findes procedurer for registrering og afmelding af alle brugere og alt it-udstyr over et givent beløb. Dette kan læses i:

- It-politik og -proces ved ophør af ansættelsesforhold i UCC
- "Instruks vedr. registrering, afhentning og udskiftning / afhændelse af computere m.m.".

Enhver bruger og ethvert it-udstyr skal tildeles en entydig identifikation, som skal være den samme i al den tid, brugeren eller udstyret har adgangsrettigheder. Identifikationen må normalt ikke tildeles nogen anden person eller noget andet udstyr.

En rettighed er en specifikation af en brugers tilladelse til at anvende specifikke funktioner i et it-system, som benyttes af flere brugere. Systemrettigheder som tilknyttes basissoftware (herunder operativsystemer, brugerprogrammer, databasesystemer, hjælpeprogrammer og netværksstyresystemer) skal identificeres. Personkategorier og udstyr, som kan få behov for rettigheder, skal ligeledes identificeres.

En medarbejder, der tildeles systemrettigheder for at kunne udføre sine arbejdsopgaver, må kun udnytte disse rettigheder til de angivne formål. Medarbejderen skal være klar over, at enhver form for information, medarbejderen får adgang til under udførelsen af disse arbejdsopgaver, er fortroligt og ikke må misbruges.

Tildeling og ændring af rettigheder skal registreres, og deres anvendelse skal kontrolleres og revurderes regelmæssigt. Det er afdelingschefens ansvar, hvad den enkelte bruger får adgang til. Brugerne skal informeres om, hvilke adgangsrettigheder, de får tildelt. Brugerens misbrug af rettigheder vil blive betragtet som sikkerhedsbrud, der medfører sanktioner.

Identifikation af brugerprofiler for eksterne brugere

Brugernavne skal udarbejdes efter en standard navnekonvention. Dette gælder også for gæster, konsulenter og lignende, så at det er enkelt at identificere dem.

Standardkodeord må ikke anvendes på UCC's systemer. Disse skal ændres eller slettes.

Medarbejderes omplacering

Ved omplacering af medarbejdere skal alle rettigheder for pågældende bruger revurderes af medarbejderens nærmeste leder.

Gennemgang af brugerprofiler

Der skal etableres en opfølgningsprocedure, således at systemejere af it-systemer kan foretage en regelmæssig gennemgang (mindst én gang pr. år) af adgangsrettigheder med tilhørende rettigheder. Formålet er at afdække, om uønskede adgangsrettigheder er opnået uden om de gældende vilkår.

Det er afdelingschefens ansvar, at de tildelte rettigheder ajourføres ved ændring af medarbejdernes arbejdsopgaver, herunder sletning ved medarbejderens fratrædelse.

10.2 Administration af brugeradgang

Systemejerne har ansvaret for, at der opstilles procedurer til kontrol af tildeling af adgangsrettigheder til it-systemer. Procedurerne skal omfatte alle brugerkategorier og hele den periode, hvori adgangsrettighederne er gældende, dvs. fra registrering til formel afmelding af en bruger.

Særlig opmærksomhed skal rettes mod de personer, der tildeles rettigheder, som giver dem mulighed for at omgå et it-systems kontroller.

Retningslinjer for skift af kodeord

Retningslinjer for opbygning, håndtering og krav til skift af kodeord er beskrevet i **'Beskrivelse af UCC's politik for kodeord'.**

10.3 Brugerens ansvar

Uautoriseret brugeradgang må ikke kunne forekomme. For at opnå et tilpas sikkerhedsniveau, skal autoriserede brugere følge de vedtagne retningslinjer for håndtering af kodeord m.v.

Alt hvad der foretages via brugerens brugernavn, er entydigt brugerens ansvar.

Brug af kodeordsbeskyttet pauseskærm

Alle arbejdscomputere aktiverer automatisk kodeordsbeskyttet skærmlås efter et bestemt tidsrum. Medarbejderne bør dog selv aktivere skærmlåsen, når de forlader deres arbejdscomputer. Systemejerne kan dog fastsætte andre regler end denne i systemejerpapiret. I et sådan tilfælde er det systemejerpapirets retningslinjer, som er gældende.

Opbevaring af kodeord til administrativ adgang

Kodeord for administrativ adgang til systemer, som er medtaget i UCC's beredskabsplan, skal opbevares i forseglet kuvert i et aflåst og brandsikkert pengeskab.

10.4 Styring af netværksadgang

Identifikation af netværksudstyr

De enkelte netværksenheder er grupperet i følgende tre kategorier:

1. **Perimeterenheder**: Betegner netværksudstyr, som er koblet direkte til internettet på mindst et interface, fx firewalls, VPN og Dial-in udstyr.
2. **Kerneenheder**: Betegner netværksudstyr, som er en del af UCC's backbone-netværk, fx centrale routere.
3. **Distributions/access-enheder**: Betegner netværksudstyr, som enten distribuerer trafikken mellem backbone-netværket og de enkelte organisatoriske enheder på UCC, eller netværksudstyr, som distribuerer trafikken i en enkelt organisatorisk/geografisk enhed, fx fordelingsswitche i lokale krydsfelter.

Det er kun medarbejdere i it-afdelingen/it-infrastruktur, der har administrativ adgang til alle tre kategorier.

Beskyttelse af diagnose- og konfigurationsporte

Forbindelser til diagnoseporte skal sikres mod uautoriseret anvendelse, og adgangen skal kontrolleres. Der skal udarbejdes en procedure, så diagnoseporte kun er tilgængelige i en tidsbegrænset periode efteraftale mellem ejeren og den eksterne leverandørs tekniske personale.

Autentificering ved adgang til netværket

Adgangen til det interne netværk fra andre lokationer end UCC skal ske ved brug af brugernavn/kodeord via en krypteret tunnel.

Enhver undtagelse herfra er midlertidig og skal på forhånd godkendes af UCC's it-sikkerhedskoordinator.

Retningslinjer for brug af netværkstjenester

Brugere skal kun have adgang til de tjenester, de er autoriseret til at benytte.

Anvendelse af sociale netværk

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

10.5 Styring af systemadgang

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

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

Begrænset netværkstid

UCC's systemer er i princippet tilgængelige døgnet rundt med undtagelse af planlagte systemservices og systemopgraderinger. Disse lægges i de aftalte servicevinduer og/eller annonceres på it-afdelingens hjemmeside.

Automatiske afbrydelser

Når sessioner har været inaktive i en given periode skal de så vidt muligt termineres automatisk.

Brug af systemværktøjer

Adgangsrettigheder og de tilhørende rettigheder til at anvende systemhjælpeværktøjer skal begrænses og kontrolleres. Enhver form for fjernkontrol med en brugers it-system bør i hvert enkelt tilfælde godkendes af den pågældende bruger.

Udvidede adgangsrettigheder

De udvidede adgangsrettigheder til UCC's infrastruktur, som fx giver adgang til at rette i UCC's Active Directory, må kun tildeles i meget begrænset omfang og alene ud fra et arbejdsbetinget behov.

Tildeling af udvidede adgangsrettigheder til administrering af hostede systemer og applikationer, som vedligeholdes af it-afdelingen, skal alene ske ud fra et arbejdsbetinget behov. Disse adgangsrettigheder tildeles udelukkende af systemejeren.

Der skal benyttes særlige brugeridentiteter (såkaldte A-konti) til de udvidede rettigheder af hensyn til overvågning og opfølgning.

Skift af administratorkodeord ved fratrædelse

Hvis en person med kendskab til administrative kodeord fratræder, skal disse kodeord så vidt muligt ændres med det samme.

Kodeordsadministration

Systemerne skal så vidt muligt indeholde kodeordsadministration, der sikrer, at kodeord for servicekonti så vidt muligt overholder reglerne for hensigtsmæssige kodeord.

Ændring af kodeord til servicekonti

Kodeord til servicekonti skal ændres, hvis udenforstående får kendskab til disse, herunder administratorer, som ophører i UCC.

Administrative kodeord skal følge samme minimumsregler som øvrige kodeord.

Administration af arbejdscomputere

Alle medarbejdere har administratoradgang til deres arbejdscomputere. Medarbejderne er forpligtiget til ikke at misbruge denne rettighed, herunder installation af ulovligt eller skadeligt software, samt ændring af computerens sikkerhedsopsætning.

10.6 Mobilt udstyr og fjernarbejdspladser

Fjernarbejdspladser

Fjernarbejdspladser tillades, når sikkerhedspolitikken i øvrigt overholdes.

Antivirusprogrammer

Antivirusprogrammer skal være installeret på mobile arbejdspladser og fjernarbejdspladser. Det er brugerens ansvar, at softwaren holdes opdateret.

Adgang til netværket

Adgangen til UCC's netværk må kun ske via sikkerhedsgodkendte løsninger.

Privat udstyr må kun tilkobles UCC's trådløse gæstenet og er derudover ikke tilladt på netværket.

Adgang til applikationer på UCC's netværk

Adgang til fjernadministration af forretningskritiske, interne applikationer tillades efter godkendelse fra den medarbejderens chef/leder.

11. Anskaffelse, udvikling og vedligeholdelse af it-systemer

Indkøb, udvikling og implementering af nye it-systemer i UCC skal foregå kontrolleret for at undgå en unødvendig forøgelse af risikoen for it-sikkerhedsbrud. Sikkerhedsovervejelser bør altid indgå i implementering af it-løsninger.

Sikkerhedskrav til it-systemer, inklusive krav til reetableringsprocedurer, skal identificeres allerede i de indledende analysestadier for at skabe et optimalt løsningsgrundlag.

Sikkerheden i basissoftwaren og brugersystemer skal supplere hinanden.

11.1 Sikkerhedskrav til it-systemer

Anskaffelsesprocedurer

Det skal sikres, at nyanskaffelser ikke giver anledning til konflikt med eksisterende krav i sikkerhedspolitikken.

Anskaffelser må ikke give anledning til forøget risiko for sikkerhedshændelser, med mindre at ledelsen accepterer den øgede risiko.

Ethvert nyt system skal risikovurderes inden ibrugtagning.

Specifikation af sikkerhedskrav

Krav til sikringsforanstaltninger i nye it-systemer eller ændrede, eksisterende it-systemer skal specificeres som en del af den dokumenterede kravspecifikation til it-systemet. Sikringsforanstaltningerne skal også overvejes ved evaluering af et standardsystem.

Kravene til it-sikkerhed og kontrol skal reflektere den værdi, som informationsaktiverne tillægges, og de ødelæggelser, der kan opstå som følge af manglende sikkerhed.

Indbyggede sikringsforanstaltninger i it-systemer skal dokumenteres i alle relevante brugermanualer og driftsafviklingsinstruktioner. Sikkerhedsforanstaltningerne vurderes årligt under hensyntagen til registrerede hændelser og det generelle trusselsbillede.

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

Områder for kravspecifikation

Kravspecifikation skal i forhold til it-sikkerhed inddrage følgende områder:

- Adgangskontrol.
- Logning og overvågning af alle væsentlige hændelser.
- Beskyttelse imod fortrolighedskrænkelser, i det omfang systemet skal behandle fortrolige eller personhenførbare informationer.
- Overholdelse af relevante love eller kontrakter.
- Mulighed for backup af data og systemet.
- Mulighed for genetablering efter kritiske, uforudsete fejlsituationer.
- Krav til viden og uddannelse af driftspersonale.

11.2 Styring af driftsmiljøet

Sikring af testdata

Testdata skal beskyttes og kontrolleres. Brug af virkelige persondata til test skal begrænses og så vidt muligt anonymiseres.

Kontrolleret adgang til kildekode

Adgangsrettigheder til kildekoder og objektkoder skal løbende kontrolleres for at minimere risikoen for utilsigtede ændringer.

Migreringsstyring

Hver gang programmer overføres til driftsmiljøet, skal de kontrolleres for at beskytte it-systemernes eksekverbare programmer og for at registrere fejl og uautoriserede ændringer. Kontrollen indebærer, at alle ændringer gennemføres via en formaliseret Change Management-proces.

Systemudvikling udført af en ekstern leverandør

I forbindelse med systemudvikling udført af en ekstern leverandør bør UCC som udgangspunkt kræve:

- adgang til at overvåge udviklingsprocessen,
- afleveringstest,
- dokumenteret, løbende kvalitetssikring,
- deponering af kildekode,
- ophavsrettighed på kildekode.

Krav i nærværende regelsæt samt reglerne for offentlige indkøb skal følges.

11.3 Sikkerhed i udviklings- og hjælpeprocesser

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

Ændringer i standardsystemer

Ændringer i standardsystemer skal begrænses for at fastholde driftsstabilitet. Med undtagelse af ændringer i parametre og specialopsætninger skal modifikation af standardprogrammer undgås. Under særlige omstændigheder skal følgende punkter overvejes:

- risikoen for, at indbyggede kontroller og pålidelighedsprocesser kan blive kompromitteret,
- sandsynligheden for, at modifikationen kræver leverandørens indforståelse,
- muligheden for, at den ønskede ændring kan leveres af leverandøren som en opdatering,
- risikoen for, at ændringen kan medføre, at UCC bliver ansvarlig for fremtidig programvedligeholdelse.

Herudover skal det originale standardprogram gemmes, og alle ændringer skal foretages på en entydigt identificeret kopi. Ændringerne skal dokumenteres, så de eventuelt kan foretages på fremtidige versioner.

Ændringsstyring

Der skal føres kontrol med implementering af udvidelser og ændringer af brugersystemer for at minimere fejl og misbrug. Sikkerheds- og kontrolprocedurer må ikke kompromitteres.

Der skal findes procedurer til udvidelses- og ændringskontrol af brugersystemer. Tilpasninger, opsætninger eller ændringer skal ske i henhold til retningslinjerne for brugersystemets anvendelse.

Den systemansvarlige har ansvar for at foretage tilpasning, opsætning eller ændring af programparametre eller alternativt sikre, at kun programleverandøren udfører dette som serviceopgave.

It-systemets brugere må ikke have adgang til tilpasninger eller opsætninger.

Implementering af ændringer skal foretages på et aftalt tidspunkt.

Sikring af applikationsudviklingsmiljøerne

Udviklingsmiljøer skal sikres mod trusler så som uautoriseret adgang, ændringer og tab. Data skal sikres efter følsomhedsniveau.

Adgangskontrol for kildetekst

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

Sikkerhed i applikationsudvikling

Sikkerhed skal inkluderes som en integreret del af alle udviklingsprojekter.

Sikring af udviklingsmiljøer

Udviklingsmiljøer skal særligt sikre integritet i udviklingsprocessen, herunder sikring mod tab af data.

Gennemgang af systemer efter ændringer

Når driftsmiljøerne ændres, skal kritiske forretningssystemer gennemgås og testes for at sikre, at UCC's daglige drift ikke kompromitteres.

11.4 Sårbarhedsstyring

Godkendelse af nye eller ændrede systemer

It-afdelingen skal etablere en godkendelsesprocedure for nye systemer og nye versioner af eksisterende systemer.

Rettelser til operativsystemer og applikationspakker

It-afdelingen skal løbende vurdere tilgængelige sikkerhedsrettelser til anvendte software, for eksempel "patches" eller "hot-fixes". Udrulning/installation skal foretages efter behov.

Større operativsystemopdateringer, for eksempel "service packs"

Når større opdateringer, for eksempel "service packs", til anvendte operativsystemer er gjort tilgængelige fra leverandører, skal it-afdelingen vurdere, om disse skal installeres.

Større opdateringer skal testes grundigt for kompatibilitet med anvendte applikationer, inden opdateringerne installeres i produktionsmiljøet.

Større applikationspakkeopdateringer, for eksempel "service packs"

Når større opdateringer til anvendte applikationer er gjort tilgængelige fra leverandører, skal it-afdelingen vurdere, om disse skal installeres.

Større opdateringer skal testes i et testmiljø, inden opdateringerne installeres i produktionsmiljøet.

12. Styring af it-sikkerhedshændelser

12.1 Rapportering af it-sikkerhedshændelser og svagheder

Alle brugere af it-systemer skal instrueres om, at de har pligt til og ansvar for at rapportere mistænkelige hændelser så hurtigt som muligt til Servicedesk / 9999. Medarbejdere, samarbejdspartnere og eksternt service- og rådgivningspersonale skal informeres om rapporteringsprocedurer og de typer af hændelser, der kan forekomme. Hændelserne kan være sikkerheds- og lovbrud, sikkerhedssvagheder, program- og funktionsfejl.

Ansvar og forretningsgange for sikkerhedshændelser

Der skal udarbejdes procedurer, som kan sikre en effektiv og hurtig reaktion på hændelser, som kan true it-sikkerheden. Medarbejdere i It Drift og support, samt brugerne, skal instrueres om, at alle har ansvar for at reagere ved tegn på sikkerhedstruende eller tabsgivende hændelser under driftsafviklingen.

Forholdsregler og alarmering ved kriser, hændelser af fysisk karakter og virtuelle angreb er beskrevet i dokumentsættet ”Beredskabsstyring”.

Rapportering af formodede sikkerhedshændelser

Ved konstatering af brud eller formodede brud på it-sikringsforanstaltninger skal rapportering straks ske til Servicedesk / 9999.

Rapportering af sikkerhedshændelser

It-sikkerhedskoordinatoren skal rapportere om hændelser af betydning for sikkerheden til it-sikkerhedsudvalget

Rapportering af programfejl

Brugere, som observerer programfejl skal rapportere dette til Servicedesk / 9999.

12.2 Håndtering af sikkerhedsbrud og forbedringer

Proces for reaktion på hændelser

It-sikkerhedskoordinatoren har ansvar for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser.

Kontrol og opfølgning på sikkerhedsbrud

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

Indsamling af beviser

Hvis et sikkerhedsbrud afstedkommer et retsligt efterspil så skal der indsamles, opbevares og præsenteres et fyldestgørende bevismateriale. Dette er beskrevet nærmere i "Beredskabsstyring - hændelseshåndtering".

At lære af sikkerhedsnedbrud

It-sikkerhedsudvalget skal etablere et system, som kan kvantificere og overvåge typer af sikkerhedsbrud, herunder deres omfang og omkostninger. Dette er beskrevet nærmere i dokumentsættet "Beredskabsstyring".

Vurdering af tidligere hændelser

It-sikkerhedsudvalget holder møde hvert kvartal, hvor den forgangne periodes hændelser gennemgås. På den baggrund anbefaler it-sikkerhedsudvalget, hvorvidt et it-sikkerhedssystem kan forbedres eller præciseres. Udvalget kan fx fremsætte forslag om opdaterede regler, procedurer og/eller risikovurderinger.

13 Beredskabsstyring

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

For at formindske konsekvenserne af ulykker og fejl i UCC's it-systemer skal en beredskabsplanlægning for reetablering af forretningskritiske systemer udarbejdes. Følgende overvejelser danner grundlag for beredskabsplanlægningen og dens omfang:

- Det skal vurderes, hvordan ulykker og fejl i it-systemerne kan indvirke på UCC's aktiviteter, samt med hvilke midler aktiviteterne kan fortsætte, indtil it-systemerne er reetableret.
- De kritiske systemer skal udpeges og prioriteres indbyrdes.
- Tidsrammer for, hvor hurtigt systemerne igen skal være operationelle efter et uheld, skal fastlægges.

Systemejeren - i samarbejde med it-afdelingen - beslutter, hvilke systemer, der skal udarbejdes beredskabsplaner for, og hvem der har kompetence til at iværksætte dem.

Ramme for beredskabsplaner

It-sikkerhedsudvalget skal fastlægge en ensartet ramme for UCC's beredskabsplaner for at sikre, at alle planerne er sammenhængende og tilgodeser alle sikkerhedskrav. Desuden fastsætter udvalget en prioritering af afprøvning og vedligeholdelse.

Beredskabsplanen skal angive betingelserne for, i hvilke situationer den helt eller delvist skal aktiveres. Den skal præcisere, hvilke persongrupper, som har det overordnede ansvar under en it-beredskabssituation, hvordan de alarmeres, og hvordan den koordinerede indsats organiseres.

Nye planer skal være forenelige med eksisterende nødprocedurer, fx evakueringsplaner og arrangementer af separate it-nødinstallationer, telekommunikation, lokaliteter og personales midlertidige placering.

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.

Nødprocedurer for kritiske processer

Der skal for alle forretningskritiske processer eksistere en opdateret nødprocedure, som kan sættes i drift.

Identifikation af kritiske processer

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

Reetablering af forretningskritiske systemer

For alle forretningskritiske systemer skal der forefindes en plan for reetablering.

Beredskabsstyringsproces

It-sikkerhedsudvalget skal udarbejde og vedligeholde en tværorganisatorisk beredskabsstyringsproces, som skal behandle de krav til it-sikkerhed, der er nødvendige for UCC's fortsatte drift.

Beredskabsplan

Beredskabsplaner skal udarbejdes, afprøves og vedligeholdes for virksomhedskritiske systemer og processer. It-sikkerhedsudvalget er ansvarlig for at koordinere disse aktiviteter og for at lave en årlig statusrapport til direktionen.

Aktivering af beredskabsplanen

Det skal være klart defineret, hvem der har ansvaret for aktivering af beredskabsplaner.

Medarbejdere, som udgør en del af beredskabsplaner, skal være informeret om dette ansvar.

Alle medarbejdere skal være informeret om beredskabsplanernes eksistens og placering.

Uddannelse i beredskabsplaner

It-sikkerhedskoordinatoren har ansvaret for, at medarbejdere modtager tilstrækkelig uddannelse i de aftalte beredskabsprocedurer, inklusive krisehåndtering.

Afprøvning og vedligeholdelse af beredskabsplaner

Beredskabsplanens aktualitet og duelighed skal sikres ved regelmæssig opdatering og afprøvning af planens væsentligste dele. Der skal tages højde for ændringer i UCC's aktiviteter eller organisation, som kan være medvirkende til, at beredskabsplanen ikke længere er aktuel. Medarbejderne skal holdes orienteret om planen.

Afprøvning af beredskabsplaner skal indeholde:

- En skrivebordstest af de forskellige scenarier.
- Simuleringer (med henblik på at træne deltagerne i håndtering af deres roller).
- Teknisk reetablering (sikring af, at tekniske systemer kan reetableres effektivt).

14. Overensstemmelse med lovbestemte og kontraktlige krav

Mange aspekter af UCC's virke kan være omfattet af lovgivning eller være påvirket af kontrakter eller eksterne parters rettigheder.

UCC's systemer skal være i overensstemmelse med lovbestemte og kontraktmæssige krav. Forretningsgange, procedurer og politik for it-sikkerhed skal årligt tages op til revurdering.

14.1 Overensstemmelse med lovbestemte krav

14.1.1 Identifikation af relevant lovgivning

Ledelsen er ansvarlig for at identificere lovgivning, som er relevant for UCC's drift, eller uddelegere dette ansvar til en medarbejder.

Ledelsen er ansvarlig for, at alle eksterne sikkerhedskrav og UCC's håndtering heraf klarlægges, dokumenteres og vedligeholdes løbende.

14.1.2 Ophavsret

Ophavsretligt beskyttet materiale må ikke kopieres uden samtykke fra indehaveren af ophavsretten. Ophavsretten er styret ved udstedelse af licenser.

Ved salg eller videregivelse af it-udstyr skal det sikres, at programlicenserne overføres til de nye brugere. I modsat fald skal de berørte programmer slettes, inden it-udstyret videregives.

Brugerne skal orienteres om, at overtrædelse af bestemmelser i forbindelse med ophavsretsbeskyttelse kan medføre sanktioner og anklage mod UCC og den bruger, som begår overtrædelsen.

Brugeren er personligt ansvarlig for, at licenskravene er opfyldt for det software, denne selv installerer.

Retningslinjer for ophavsrettigheder

Ledelsen har det overordnede ansvar for, at UCC fastholder en passende opmærksomhed på ikke at krænke tredjeparts ophavsrettigheder.

It-afdelingen skal vedligeholde dokumentation for ejendomsretten af licenser.

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

Det skal løbende kontrolleres – fx med stikprøvekontroller – at der kun er installeret autoriserede systemer med autoriserede licenser på UCC's computere.

Som udgangspunkt føres der udelukkende kontrol med det software, som it-afdelingen installerer på computerne.

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

Administration af softwarelicenser

Medarbejdere og studerede, som har autorisation til at anvende kopier af UCC's programmer på deres private udstyr, skal følge de procedurer og kontroller, som generelt er gældende i UCC.

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

14.1.3 Beskyttelse mod misbrug af it-udstyr

Anvendelse af it-faciliteter til uhensigtsmæssige formål uden særlig tilladelse betragtes som uretmæssig. Hvis sådanne aktiviteter identificeres ved overvågning eller på anden måde, skal det påtales umiddelbart, og aktiviteterne skal bringes til ophør.

14.2 Overensstemmelse med sikkerhedspolitik og –retningslinjer

UCC's ledelse skal sikre sig, at dens it-sikkerhedspolitik bliver overholdt, og at vedtagne sikringsforanstaltninger bliver implementeret og fungerer med den tilsigtede effekt.

Til dette formål må ledelsen indføre og vedligeholde et betryggende, internt kontrolsystem for det daglige arbejde, således at medlemmerne af ledelsen på alle niveauer holdes fast til deres ansvar for sikkerheden i egne funktionsområder.

Opfølgning på implementering af sikkerhedspolitikken

Mindst en gang årligt skal der gennemføres en systematisk opfølgning på overholdelsen af it-sikkerhedspolitikken i hele organisationen. Dette initieres af it-sikkerhedsudvalget. Resultatet rapporteres til øverste ledelse.

Hver enkelt chef skal løbende sikre, at it-sikkerhedspolitikken bliver overholdt inden for eget ansvarsområde.

Gennemgang af sikkerhedspolitik

It-sikkerhedsudvalget skal kontrollere, at it-sikkerhedspolitikken er indarbejdet i organisationen og bliver overholdt.

Overtrædelse af sikkerhedsretningslinjerne

Det er ikke tilladt at forsøge at omgå sikkerhedsmekanismer.

Det er ikke tilladt at foretage uautoriseret afprøvning af sikkerheden.

Bevidste eller gentagne overtrædelser vil medføre disciplinære sanktioner.

Det er ledelsens ansvar at sanktioner for brud på UCC's politikker, regler eller retningslinjer håndhæves konsekvent og i overensstemmelse med gældende lovgivning.

14.3 Beskyttelsesforanstaltninger ved revision af it-systemer

Sikkerhed i forbindelse med revision

Revisionskrav og -handlinger i forbindelse med systemer i drift skal planlægges omhyggeligt og aftales med de involverede parter for at minimere risikoen for forstyrrelser af UCC's forretningsaktiviteter.

De personer, som udfører revisionen, skal være uafhængige af det reviderede område.

Beskyttelse af revisionsværktøjer

Adgangen til revisionsværktøjer skal begrænses for at forhindre misbrug.

Bilag - Termer og definitioner

ABA-anlæg

Se 'Automatisk brandalarmeringsanlæg'

Accesspunkt

Er forbindelsespunktet imellem det trådede / kablede netværk på UCC og det trådløse netværk. Via et accesspunkt kan en medarbejders computer få adgang til medarbejdernetværket, mens de studerendes eller eksterne samarbejdspartneres computere kan få adgang til gæstenetværket.

Adgangskontrol - fysisk

Enhver fysisk sikringsforanstaltning mod uautoriseret adgang til et sikkerhedsområde.

Adgangskontrol - logisk

Enhver programmerbar sikringsforanstaltning mod uautoriseret anvendelse af UCC's it-aktiver.

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 UCC's it-aktiver. Se også "Autorisation" og "Rettigheder".

Adgangskode/Kodeord (password)

Kombination af tegn, som benyttes til verifikation af en brugers identitet.

Adgangskort

En identifikationsbærer, der fx er udformet som et plastickort. Kortets dataindhold identificerer den person, kortet er udstedt til.

ADK-systemet

Se 'Adgangskontrolanlæg'

Aktiver

Alt, der har værdi for UCC, også immaterielle værdier som fx it-systemer, data, procedurer og dokumentation. Se også "Informationsaktiver".

Applikationssystem

Se "Informationsbehandlingssystemer".

Arbejdscomputer

Betegnelse på en PC, der benyttes af en enkelt bruger, og som er tilkoblet et netværk, som 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 Brandalarmeringsanlæg (ABA-anlæg)

Anlæg udført i overensstemmelse med forskrift 232 fra Dansk Brandteknisk Institut, som overvåger mod brandkendetegn og alarmerer i tilfælde af ildebrand.

Automatisk Indbrudsalarmeringsanlæg (AIA-anlæg)

Anlæg udført i overensstemmelse med DS 471, der overvåger mod 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, som kan opbevares sikkert og anvendes i tilfælde af, at de originale data er gået tabt.

Backupansvarlig

Person med ansvar for sikkerhedskopiering.

Barriere

Fysisk afgrænsning, som har til formål at adskille områder. Afgrænsningen kan være reel (fx væg) eller symbolsk (fx malet linje på gulv suppleret af adgang forbudt skilt).

Basissystemer

Opdeles i operativsystem(er) og hjælpeprogrammer. Se også "It-systemer".

Beredskabsplan

Indeholder beskrivelser af redningsaktioner, der skal anvendes, hvis der indtræder en forstyrrende afbrydelse af UCC's forretningsprocesser. Planerne beskriver redningsaktionerne, og hvem som skal igangsætte dem.

Der er for UCC udarbejdet en ***BCP – Business Continuity Plan*** og en ***DRP – Disaster Recovery Plan.***

Bibliotek (for data og programmer)

Et system, der registrerer opbevaring af data og programmer. Desuden fører det kontrol med til- og afgang af fx basis- og netværksprogrammer, brugerprogrammer, udviklings- og testprogrammer, programkildekoder og data. Derudover indeholder det en liste over brugere, der har fået tilladelse til at anvende disse. De forskellige biblioteksdele holdes adskilt.

Brugerprogram/system

Se "It-systemer".

Bygningsskallen

Se "Skallen".

Celle

Et barrikaderet lokale inden for et sikkerhedsområde, som er beskyttet med yderligere sikring i form af bygningsmæssig adskillelse og separat adgangskontrol.

Centralt udstyr

It-udstyr, hvor flere arbejdscomputere 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.

CERT

Computer Emergency Response Team, der overvåger it-sikkerheden på bl.a. Forskningsnettet i Danmark, hvor det er en tjeneste fra UNI•C. Link: https://www.cert.dk/

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".

Dataarkiv

Se "Arkiv".

Dataejer

Ejeren af de data, der er placeret i et it-system, fx er en medarbejder eller studerende dataejer for de data, der er placeret i mail-boksen eller filer i personlige- og fællesdrev.

Dataintegritet

Se "Integritet".

Datamedier

Fysiske lagringsmedier, hvorpå der ad elektronisk vej er lagret data. Datemedier kan fx være disketter, bånd, diske, CD-ROM, EPROM og USB-lagringsenheder.

Dekryptering

Den modsatrettede proces af en kryptering.

Diagnoseport

Tilkoblingsstik i it-udstyr til kommunikationsforbindelse med ekstern servicetjeneste. Via kommunikationsforbindelsen kan en servicetekniker fra et andet geografisk sted registrere udstyrets driftstekniske data, statusinformationer og øvrige informationer. Hvis diagnoseporten er aktiv/åben kan der foretages fejlrettelser. Se også "Port".

Digital signatur – NEMID

Den digitale signatur bruges til verifikation af meddelelsens integritet og afsenderens autenticitet.

Downloade

At kopiere data (fx programmer) fra en computer koblet på Internettet til ens egen PC.

"Ejer"

For manuelle systemer er der ofte i en virksomhed en naturlig oplevelse af, hvem der er "ejer" af et system og dets informationer, og at "ejeren" har såvel ansvar for som rettigheder til informationerne.

Bogholderen "ejer" de finansielle informationer, salgslederen "ejer" de afsætningsmæssige informationer, og lagerforvalteren "ejer" de beholdningsmæssige informationer. Ansvar for og rettigheder til systemer og informationer bliver ofte mere diffust, når et system digitaliseres. Det er derfor nødvendigt aktivt at sikre, at dette ansvar bibeholdes. "Ejeren" bestemmer, hvilke brugere, der kan anvende et system og dets informationer.

Ekstern bruger / samarmbejdspartner

Dette kan fx være en ekstern konsulent, som er ansat til en opgave i UCC, eller en gæsteforelæser.

Entitet

En uafhængig enhed, som har selvstændig eksistens, fx en node/en person.

Firewall

Se "Logisk filter".

Fortrolighed

Sikkerhed for, at indholdet af en meddelelse ikke kan afsløres af uvedkommende.

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, som er baseret på fysiske eller mekaniske foranstaltninger for imødegåelse af tyveri, indtrængning, hærværk, eller anden ødelæggelse af aktiver. Se også "Tyverisikring, mekanisk".

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".

Hemmeligholdelse

Se ”Fortrolighed”.

Hjælpeprogram

Standardbetegnelse for værktøjsprogrammer, som anvendes til fx redigering, 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, som overføres til eller indrapporteres i et it-system.

Information

Den mening, der tillægges en mængde af data. Se også ”Data”.

ISMS

”Information Security Management System”, dvs. et it-sikkerhedsstyringssystem. Systemet bruges til at styre planlægning, udførelse, kontrol, og korrektion af sikringsforanstaltninger, således at det valgte sikkerhedsniveau fastholdes.

It-aktiv

Omfatter alle de programmer, der anvendes i UCC, de tilhørende data, samt servere og computere.

It-aktiv, kritisk

Et it-aktiv, der truer UCC’s forretning, hvis det ikke fungerer.

It-læringsagent

En repræsentant i de enkelte afdelinger i UCC, som har en særlig interesse for it, og dermed er blevet udnævnt til læringsagent inden for it-området. Læringsagenten står for orientering og vejledning i it til medarbejdere og studerende på afdelingen.

It-systemer

Betegnelsen for en samling programmer til løsning af en samlet mængde opgaver. Grundlæggende opdeles informationsbehandlingssystemer i to hovedgrupper:

- **Basissystemer**, der oftest er hardwareafhængige, består af **operativsystem**(er) og **hjælpeprogram**(mer). Basissystemer, ofte benævnt styresystemer 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, brugerprogrammer og brugere.
  Hjælpeprogrammerne er værktøjer, som 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. Den enkelte bruger kan i nogen grad tilpasse et standardsystems opsætning og funktioner ved at vælge mellem nogle indbyggede parametermuligheder. Ofte sammensættes flere standardsystemer til en integreret programpakke/Office suite.

It-system, kritisk

It-system der i et samarbejde imellem systemejeren og it-sikkerhedsudvalget er kategoriseret i klasse 1.
Dvs. at it-systemet er af yderste vigtighed for driften af UCC og som fx ikke bør have væsentlig nedetid imellem 7:30 og 17:00

It-sikkerhedskoordinator

Person med ansvaret for udarbejdelse af regler og procedurer for sikringsforanstaltninger for UCC's it-sikkerhed.

It-stamblad

It-stambladet udarbejdes for såvel materiel (servere) som systemer (applikationer). It-stambladet skal omfatte de data, som er nødvendige for den daglige drift, sikkerhedsregler og regler for opsætning, service, reparation, samt genetablering af systemerne efter alvorlige fejl og/eller situationer, hvor anlægget skal nyanskaffes.

It-revision

Aktivitet, som kontrollerer, at den ønskede it-sikkerhed i henhold til UCC's politik for it-sikkerhed og forskrifter for it-sikkerhed er til stede og efterleves. Revisionen dokumenteres og forelægges virksomhedens ledelse. It-revisionen udføres af en ekstern revisor.

Junk-mail

Junk-mail kan oversættes til noget i retning af skraldespandspost. Det kan være på papir, på fax eller e-mail. Det er mest udbredt i e-mail, fordi det er let og billigt at sende til mange på én gang. Junk-mail er typisk uopfordrede og useriøse e-mails med tilbud om hvad som helst.

Karakter

Ethvert stort eller lille bogstav, tal eller tegn, der anvendes enkeltstående eller som en tilladelig sekvens.

Kildekode

Et informationsbehandlingsprogram, der er skrevet i et symbolsk og standardiseret programmeringssprog.

Klartekst

Ubeskyttet og umiddelbar læselig tekst.

Klassifikation

Se "Risikokategori"

Kompatibilitet

Den forenelighed, som skal være til stede, for at noget (et system) kan virke sammen med noget andet (andre systemer).

Kopi- / print-kort

Plastikkort med medarbejderens navn og initialer, som kan anvendes på kopi-printere. Der udstedes lignende kort med påført navn og studienummer til de studerende.

Kryptering

Omsætning (kodning) af læsbar klartekst, således at teksten ikke er læsbar for udenforstående, uden at de er i besiddelse af krypteringsforskriften og krypteringsnøglen.

LAN

Se "Lokalnetværk".

Log-off

Er den afsluttende procedure for brugeren af et it-system, hvorved forbindelsen mellem en arbejdscomputer og programmerne afbrydes.

Log-on

Er den nødvendige indledende procedure, hvormed en bruger etablerer sin tilladelse til at anvende en computer og/eller it-systemer.

Lokalnetværk (LAN)

Et netværk, som 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”.

Medarbejder

En person, der er ansat i UCC. For at få adgang til UCC it-resurser, skal medarbejderen være oprettet i stamdatasystemet SIS.

Netværk

Generel betegnelse, der dækker alle typer af sammenhængende datakommunikationsforbindelser mellem centralt udstyr, servere, arbejdsstationer og andet kommunikationsudstyr.

Netværksansvarlig

Person med ansvaret for drift af og sikkerhed i netværket eller segmenter af netværket.

Node

Adresserbart punkt på et datanetværk (fx en arbejdscomputer, printer, switch, netværksomskifter, router).

Objektkode

Et maskinlæsbart program, som umiddelbart kan afvikles på en datamaskine.

Operativsystem

Et grundlæggende program eller programkompleks, som foretager den overordnede styring af alt, hvad der kan afvikles på it-udstyr.

Opgradering

Udskiftning af hidtil anvendt it-udstyr og -systemer med andet kompatibelt materiel, som kan yde mere eller muliggøre bedre rationel anvendelse.

Opkobling

Etablering af en datakommunikationsforbindelse.

Orm

Et selvstændigt program, som 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 stjæler datakraft fra udstyret, som herved overbelastes.

Overvåget område

Et afgrænset område, der fx elektronisk tyveri- og brandovervåges af et automatisk alarmeringsanlæg.

Password

Se ”Adgangskode”.

Penetrering

At skaffe sig mulighed for ulovligt at anvende informationer, data eller datasystemer uden at have den fornødne autorisation og uden at blive opdaget. Se også ”Hacking”.

Personaleansvarlig

En medarbejders nærmeste leder, der har personaleansvar.

Personligt drev

P-drevet, som alle studerende og medarbejdere i UCC har adgang til.

Piratkopiering

At foretage kopiering af et it-program eller information i strid med lovgivningen om licensaftaler.

Port

Generel betegnelse for elektriske kredsløb, der virker som interfaces mellem informationsbehandlingsudstyr, arbejdsstation og andre ydre tilsluttede enheder via datakommunikationsforbindelser.

Print- / kopi-kort

Se ”Kopi- / print-kort”

Protokoller

Regler, som er reguleret af standarder, normer, tekniske metoder og specifikationer, der er fastsat med det formål at kunne fortolke og udveksle data.

Pålidelighed

Egenskab, der sikrer, at den forventede opførsel og de forventede resultater opnås.

Rettigheder

Betegnelsen for de rettigheder, som specificeres for en autoriseret bruger til legalt at anvende en vedtagen mængde af it-ressourcer, herunder data, til sine arbejdsopgaver.

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.

Revision, IT

Se 'It-revision'

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.

Risikokategori

I UCC arbejdes med tre risikokategorier:

1. Angiver at it-systemet altid skal være tilgængeligt, fx vil en ikke-planlagt periode på blot 4-6 timer inden for arbejdstiden, hvor der ikke er adgang til it-systemet, være forretningskritisk for UCC.
2. Angiver at adgangen it-systemet kan være afbrudt i op til 2 dage, uden at den manglende adgang vil være forretningskritisk for UCC.
3. Angives at adgangen til it-systemet kan være afbrudt i længere tid, uden at den manglende adgang vil være forretningskritisk for UCC

Risikostyring

Den ledelsesmæssige styring af virksomhedens indsats for at imødegå forretningsmæssige risici.

Risikovurdering

En overordnet afvejning af virksomhedens risikobillede.

Sikkerhed

Resultatet af alle de sikringsforanstaltninger, der er foretaget for at imødegå de aktuelle trusler.

Sikkerhedsmiljø

Det samlede sæt af sikringsforanstaltninger og kontroller, virksomheden har etableret for at sikre, at sikkerhedspolitikken bliver efterlevet.

Sikkerhedsområder

Alle UCCs' bygninger på de forskellige campusser er opdelt i forskellige sikkerhedsområder. Der skelnes mellem offentlige, halvprivate, private og særlige sikkerhedsområder. Et offentligt sikkerhedsområde er kendetegnet ved fri, ukontrolleret adgang det meste af døgnet. I et halvprivat sikkerhedsområde kan adgang kun kontrolleres i et begrænset omfang, fx ved indgangspartiet. Et privat sikkerhedsområde er kendetegnet ved, at adgang til og ophold i området kontrolleres. Særlige sikkerhedsområder er ligeledes private, men har også skærpede sikkerhedskrav, fx i en begrænsning af adgang og ophold i forhold til personalekategorier.

Sikkerhedsrevision

Se "It-revision".

Sikkerhedsstyring

En løbende proces, hvor ledelsen gennem en systematisk rapportering om ændringer i risikobilledet, observerede svagheder samt konkrete hændelser kan revurdere den fastlagte sikkerhedsstrategi og foretage de fornødne justeringer for at fastholde det ønskede sikkerhedsniveau.

Sikret område

Et område, hvis afgrænsninger er mekanisk/fysisk indbrudssikrede.

Sikringsforanstaltning

En praksis, procedure eller mekanisme, som 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 at foretage selvstændige log-ons til flere specifikke systemer efter den første log-on-procedure.

Skallen

Samtlige af 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 en person prøver at narre brugernavne og kodeord fra autoriserede brugere, fx ved at udgive sig for at være en it-supporter, som 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 ”It-systemer”.

Studerende

Alle, der er under uddannelse i UCC, dvs. studerende på både grund-, efter- og videreuddannelse.

Systemadministrator

Person med ansvaret for drift af og sikkerhed i et eller flere it-systemer.

Systemansvarlig

Den person, der på vegne af systemejerens har ansvaret for systemets data og de applikationer, der håndterer disse data.

Systemejer

En person fra en hvilken som helst afdeling i UCC, som har fået uddelegeret ansvaret for et eller flere it-systemer, der benyttes i den pågældende afdeling.

Systemejerpapir

Dokument, der er udarbejdet i et samarbejde imellem it-afdelingen og systemejeren. Papiret indeholder en række informationer om it-systemet, herunder leverandør forhold, regler for opdateringer, samt bruger-administration. Hvis der skal gælder særlige regler for anvendelse af systemet vil dette være beskrevet her. Et eksempel kan være om kodeordsbeskyttet pauseskærm.

Systemrevision

Se ”It-revision”.

Sårbarhed

Mangel på sikkerhed, som kan medføre uønskede hændelser.

Teknikejer

Er enten it-afdelingen, en it-driftsmedarbejder eller en ekstern samarbejdspartner

Test

Verifikation af kvaliteten af et givent system og/eller program.

Tilgængelighed

Egenskaben at være tilgængelig og anvendelig ved anmodning fra en autoriseret entitet.

Transaktionsspor

Se ”Kontrolspor”.

Trojansk hest

Et program, der ser ud og virker som et almindeligt program, men som indeholder en eller flere uautoriserede programkommandoer eller programsekvenser.

Trussel

En potentiel årsag til en uønsket hændelse, som kan forvolde skade på virksomheden.

Tyverisikring, elektrisk

Sikringsforanstaltning til overvågning af områder eller genstande ved hjælp af et AIA-anlæg.

Tyverisikring, mekanisk

Hensigtsmæssig anvendelse af bygningsdele, låseenheder mv., således at tyveri og utilsigtet gennembrydning 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 til udskrift.

Uønsket adfærd, eksempler på

Det er blandt andet ikke tilladt at: forsøge at læse, slette eller kopiere andres e-mail, forfalske e-mail-adresser, afsende generende, obskøne eller truende meddelelser til andre brugere, afsende junk-mail, kædebreve, spam-mail eller lignende former for meddelelser, anskaffe eller bibeholde brugernavne (bruger-id) under falske forudsætninger, udlåne eller dele "bruger-id/passwords" med andre.

Validering

Kalkulation og kontrol af, at indrapporterede datas værdi er gyldigt. 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 til harddiske, netværk eller andet udstyr via netværk og flytbare datalagringsmedier.

Åbent net

Et netværk, som umiddelbart er offentligt tilgængeligt for alle, der har indgået en anvendelsesaftale, og som har det nødvendige udstyr, fx internet og telefonnettet.