

OVERORDNET IT-SIKKERHEDSPOLITIK FOR ROSKILDE UNIVERSITETSCENTER

1 INDLEDNING

Roskilde Universitetscenter ønsker med denne overordnede it - sikkerhedspolitik at tilkendegive, at Universitetet prioriterer it-kvalitet og i særdeleshed it-sikkerhed meget højt.

Beskyttelsen er vendt mod såvel naturgivne som menneskeskabte risici. Alle personer opfattes som potentiel kilde til brud på sikkerheden, og ingen persongruppe er derfor hævet over sikkerhedsbestemmelserne.

2 IDENTIFIKATION AF IT-SIKKERHED

It-sikkerhed drejer sig om beskyttelse af samtlige ressourcer – såvel direkte it-ressourcer som indirekte, f.eks. bygningsressourcer - der indgår i eller bidrager til universitetets elektroniske data-behandling og kommunikation, herunder ekstern datakommunikation.

Begrebet it-sikkerhed omfatter på Roskilde Universitetscenter følgende tre hovedelementer:

1. Fortrolighed

Informationer beskyttes mod uautoriseret adgang og misbrug under behandling, transmission og opbevaring. Faciliteter til dette skal være til rådighed og anvendes efter konkret behov.

2. Integritet

Korrekt funktion af alle systemer med minimeret risiko for fejl i data og manipulation med data.

3. Tilgængelighed

En høj driftssikkerhed for alle systemer, med høje opetidspcenter og minimeret risiko for større nedbrud og tab af data.

Den følgende gennemgang af grundprincipperne skal betragtes som en kort specifikation af minimums sikkerhedskrav på Roskilde Universitetscenter.

Principperne vil blive præciseret i IT-sikkerhedshåndbogen.

3 2004-00-130/0025 GYLDIGHEDSOMRÅDE OG OMFANG

- 1) IT-sikkerhedspolitikken er bindende for samtlige ansatte, studerende og alle andre, der anvender Roskilde Universitetscenters it-aktiver og dertil relaterede fysiske rammer.
- 2) IT-sikkerhedspolitikken omfatter alle it-aktiver ejet af eller placeret på Roskilde Universitetscenter. Således såvel fysiske ressourcer, edb-udstyr, kommunikationsudstyr, som data og programmel – både indkøbte standardprogrammer og programmer udviklet på universitetet.
- 3) IT-sikkerhedspolitikken tillader forskellige sikkerhedsniveauer baseret på den specifikke anvendelse af it-aktiverne, på trusselsbilledet, på omkostningerne ved sikring, og på konsekvenserne af sikkerhedsbrud.

IT-sikkerhedspolitikken godkendes af Universitets øverste ledelse. IT-sikkerhedspolitikken vurderes løbende og ændres efter behov.

4 MÅLSÆTNING

Roskilde Universitetscenter har som målsætning at leve op til vidtgående krav til driftssikkerhed og kvalitet i forbindelse med it-udstyr og it-tjenester og dertil relaterede fysiske rammer.

Lovgivningens krav skal som minimum overholdes, systemerne skal være brugervenlige dvs. uden unødige sikkerhedsforanstaltninger, og dokumenter og andre data der har særligt behov for det, skal behandles fortroligt.

Disse mål skal etablere et passende sikkerhedsniveau, der tillige med overholdelse af lovgivningens krav er fastlagt ud fra en vurdering af risici og omkostninger.

Universitetet ønsker dog som minimum at lave op til de basale krav i Dansk Standards Norm for edb-sikkerhed (DS 484-1, 1. udgave 2000-01-21).

5 GRUNDPRINCIPPER FOR IT-SIKKERHED PÅ ROSKILDE UNIVERSITETSCENTER

5.1 Overordnede forhold

5.1.1 Ansvar og kompetence

Rektor har ansvaret for it-sikkerheden. Rektor kan delegere opgaver og ansvar vedrørende de enkelte funktionsområder, samt vejledning og instruktion af medarbejdere, studerende og andre.

5.1.2 Handlepligt

Et særligt ansvar/handlepligt påhviler medarbejdere, som arbejder med etablering, drift og vedligeholdelse af it-udstyr og it-tjenester, samt videreudvikling af disse.

Ansvar og kompetence, herunder omfanget af delegation vil blive nærmere beskrevet i universitetets IT-sikkerhedshåndbog.

5.1.3 Medarbejdere, studerende og andre

Alle ansatte, studerende og gæster har et medansvar for it-sikkerheden og vil til støtte herfor blive holdt informeret om sikkerhedsmæssige problemer og tiltag, der har betydning for mulighederne for at kunne leve op til dette ansvar i forbindelse med den pågældendes arbejdsområder.

Medansvaret omfatter også en handlepligt til at gøre opmærksom på konstaterede brister i it-sikkerheden.

5.1.4 Funktionsadskillelse

It-sikkerheden baseres som hovedregel på princippet om funktionsadskillelse således, at en og samme person ikke udfører og godkender en given operation. Dette er en væsentlig forudsætning for forebyggelse og begrænsning af virkningerne af enkeltpersoners uheld, fejl eller bevidst negative aktiviteter.

Funktionsadskillelse skal ske efter vurdering af hvilke systemer og operationer, der er kritiske for universitetets virksomhed.

Såfremt en funktionsadskillelse ikke kan ske, fastsættes andre kontrolforanstaltninger.

5.1.5 Uafhængighed af nøglepersoner

Der skal tilstræbes uafhængighed af enkeltpersoner gennem etablering af personbackup for de medarbejdere som er alene om at dække specialer eller systemer af væsentlig betydning for Roskilde Universitetscenters virksomhed.

5.1.6 Adgangsforhold

Adgang til Roskilde Universitetscenters systemer - såvel fysisk som logisk - skal reguleres, så målsætningen om et højt sikkerhedsniveau kan opnås. Alle it-aktiver, dvs. bygninger, lokaler, maskiner, programmel, data og databærende medier skal i nærmere specificeret omfang være beskyttet mod uautoriseret adgang. Adgangsbegrænsningen udføres så vidt muligt ved hjælp af elektronisk adgangskontrol som dels kan give alarmer ved uautoriseret adgang, dels gennem logning danne grundlag for efterkontrol.

De nærmere retningslinjer for kontrol med såvel fysisk som logisk adgang til it-aktiver - fastlægges i IT-sikkerhedshåndbogen – og skal omfatte:

- Regler for hvem der må disponere over hvilke aktiver.
- Regler for hvordan adgangstilladelser tildeles og trækkes tilbage, herunder hvilke situationer der giver anledning til at tilladelsen inddrages.
- Regler for overvågning, logning, efterkontrol, opfølgning og ledelsesrapportering.

5.1.7 Anskaffelse og udvikling

Ved anskaffelse af hardware og software og ved udvikling af edb-systemer skal det fremgå af kravspecifikationen, at systemerne lever op til målsætningerne i IT-sikkerhedspolitikken herunder, at der foreligger den nødvendige dokumentation herfor.

5.1.8 Dokumentation af sikkerhedsprocedurer

Dokumentation af it-sikkerhedsprocedurer og udført kontrolarbejde vedrørende disse procedurer ajourføres løbende og udbygges efter behov.

5.2 Fortrolighed

Det er målet at sikre opretholdelse af den nødvendige fortrolighed med hensyn til dokumenter eller andre data der kræver dette. Der skal derfor være adgang til faciliteter, der sikrer dette i et passende omfang.

Medarbejdere og studerende, som uberettiget får adgang til fortrolige dokumenter eller andre data på universitetets systemer, skal respektere kravet om fortrolighed. Det er de pågældendes pligt at gøre de sikkerhedsansvarlige opmærksomme på denne mulighed for uberettiget adgang til fortrolige dokumenter eller data.

Enkeltbrugere og brugergrupper skal endvidere have mulighed for at opnå en individuelt specificeret grad af fortrolighed med hensyn til egne dokumenter og andre data, f.eks. via. individuel adgangskontrol og/eller kryptering.

Den individuelle fortrolighed kan dog brydes af medarbejdere med særlig bemyndigelse, hvis de under udførelsen af deres arbejde får begrundet mistanke om, at bestemte brugere eller brugergrupper overtræder reglerne for brug af de it-faciliteter, som universitetet stiller til rådighed, eller i øvrigt overtræder regler i dansk lovgivning. Hvis de pågældende medarbejdere i denne sammenhæng støder på krypterede filer, kan de forlange at de fremvises i klartekst (dvs. ukrypteret). Alle sådanne brud på fortroligheden indrapporteres til ledelsen

5.3 Integritet

For at sikre at universitets it-systemer til enhver tid fungerer i overensstemmelse med specifikationerne, og at behandlede og genererede data er korrekte og komplette, skal:

- de nødvendige kontroller indbygges i systemerne under udviklingsprocessen eller være til stede ved anskaffelsen,
- der ved systemudvikling, ændringer og ajourføringer følges en fastlagt procedure, og krav vedrørende kvalitetssikring og dokumentation skal overholdes.

5.4 Tilgængelighed

Driftsforstyrrelser imødegås gennem:

- Dublering af kritiske systemer
- Regelmæssig sikkerhedskopiering i overensstemmelse med de fastlagte procedurer.
- Procedurer for hurtig udbedring af skader, omgåelse, omkobling eller tilsvarende som sikrer at systemerne lever op til aftaler om driftssikkerhed.
- Forebyggende foranstaltninger, herunder sikring mod hacker- og virusangreb, samt strømsvigt og vand- og brandskader.

Der afgives regelmæssigt rapporter til ledelsen om hændelser og tiltag til afhjælpning heraf, herunder planlagte forbedringer.

5.4.1 Beredskab

Der skal foreligge beredskabsplaner for:

- skadebegrænsende tiltag
- etablering af midlertidige nødløsninger
- genetablering af en permanent løsning.

Der udarbejdes dog alene beredskabsplaner for de nødsituationer som ledelsen af sikkerhedsarbejdet definerer som kritiske.

Følgende foranstaltninger er en forudsætning for at beredskabsplanerne kan fungere efter hensigten:

- Planerne ajourføres og testes løbende og som minimum en gang om året.
- Sikkerhedskopier og reserveudstyr opbevares i en anden bygning end den, hvor originalmaterialet og udstyr i drift befinder sig.

5.4.2 Katastrofer

Egentlige katastrofer forårsaget af brand- eller vandskader forebygges gennem fysisk sikring og overvågning af bygninger, tekniske installationer og it-udstyr. Foranstaltningerne etableres på basis af en afvejning af risici og omkostninger ved sikkerhedsforanstaltningerne.

6 IT-SIKKERHEDSHÅNDBOG

Med udgangspunkt i denne overordnede IT-sikkerhedspolitik udarbejdes – der som minimum er i overensstemmelse med Dansk Standard (DS 484-1: 2000), Norm for edb-sikkerhed, Basale krav - en IT-sikkerhedshåndbog, der revideres løbende. Håndbogen skal indeholde:

- Universitetets godkendte IT-sikkerhedspolitik (dette dokument)
- Beskrivelse af de overordnede principper for sikkerhedsstyring, herunder oversigt over delegerede opgaver.
- Beskrivelse af den daglige sikkerhedsledelse, herunder sikkerhedsfunktionens opgaver og kompetencer.
- Generelle retningslinjer for it-sikkerheden og de tilhørende procedurer
- Specifikke retningslinjer for it-sikkerheden og de tilhørende procedurer.

Drøftet på møde i Akademisk Råd den 11. maj 2005.

Godkendt af Rektor, Henrik Toft Jensen, den 12. maj 2005.