11. marts 2004
E2 2004-1451-1
MK 33 92 86 32

IT-universitetet i København
Glentevej 67
2400 København NV

Til orientering for:
Kt.chef Niels R. Korsby
Videnskabsministeriet

UDKAST

1. Rigsrevisionen har undersøgt om IT-anvendelsen på IT-universitetet kan understøtte opgavevaretagelsen, herunder aflæggelsen af et korrekt regnskab. Rigsrevisionen har indsamlet og vurderet en række oplysninger vedrørende IT-universitetets IT-anvendelse. Ved vurderingen er der taget hensyn til de enkelte områders risikoniveau og væsentlighed i forhold til den samlede IT-anvendelse. Det er Rigsrevisionens vurdering, at den generelle IT-sikkerhed samlet set ikke er helt tilfredsstillende.

2. Grundlaget for vurderingen er, at det nuværende niveau for IT-styring (fx strategi, risikovurdering og politikker) ikke er tilstrækkeligt og dækkende for IT-universitetets behov, og at der med hensyn til den generelle IT-sikkerhed (system-, data- og driftssikkerheden) er fundet forhold, som bør rettes eller overvejes nærmere.

3. I vedlagte detailrapport er der en beskrivelse af forhold, som Rigsrevisionen har bemærket ved denne gennemgang. Hver bemærkning indeholder oplysning om de konstaterede forhold, mulige fremtidige konsekvenser for IT-aktiviteterne samt Rigsrevisionens forslag til afhjælpning af de konstaterede forhold.

4. Rigsrevisionen anmoder om IT-universitetets kommentarer til rapporten. Rigsrevisionen skal i øvrigt henvise til rigsrevisorlovens § 16, hvoraf det fremgår, at der gælder en svarfrist på 6

uger. I det omfang svaret giver Rigsrevisionen anledning til at foretage sig yderligere, vil IT-universitetet blive orienteret herom senest 4 uger fra modtagelsen af svaret.

Med venlig hilsen

Michael Kubel
spec.kons.

UDKAST

Bilag til følgebrev og rapport om IT-revision

Rigsrevisionen giver på grundlag af rapportens bemærkninger og anbefalinger en sammenfattende vurdering af IT-anvendelsens muligheder for at kunne understøtte opgavevaretagelsen på væsentlige (kritiske) områder efter følgende skala:

- Meget tilfredsstillende
- Tilfredsstillende
- Ikke helt tilfredsstillende
- Ikke tilfredsstillende

Vurderingen Meget tilfredsstillende gives, hvis gennemgangen alene har givet anledning til anbefalinger uden væsentlig betydning for det nuværende generelle It-miljø.

Vurderingen Tilfredsstillende gives, hvis gennemgangen indeholder anbefalinger til forhold som bør rettes, men hvor systemerne samlet set skønnes at kunne understøtte afviklingen af de væsentligste (kritiske) systemer.

Vurderingen Ikke helt tilfredsstillende gives, hvis gennemgangen har givet anledning til omtale af forhold, som bør rettes fordi forholdene muligvis kan betyde, at brister i den generelle IT-sikkerhed kan give problemer ved afviklingen af de væsentligste (kritiske) systemer.

Vurderingen Ikke tilfredsstillende gives, hvis gennemgangen har vist flere forhold, som kan udgøre en væsentlig risiko for kvaliteten i den generelle it-sikkerhed og dermed en væsentlig risiko ved afviklingen af de væsentligste (kritiske) systemer.

UDKAST

RIGSREVISIONEN 11. marts 2004

IT-revisionsenheden

Rapport vedrørende IT-revision på IT-universitetet i København

UDKAST

	Rigsrevisionens bemærkninger	Rigsrevisionens anbefalinger
1	***Væsentlighed:*** **Meget vigtigt** ***Titel:*** **IT-styring** Rigsrevisionen har bemærket, at der ikke foreligger en af ledelsen godkendt IT-strategi, en overordnet risikovurdering og en IT-sikkerhedspolitik for ITU. MULIG RISIKO: En manglende overordnet ledelsesmæssig styring giver risiko for, at IT-anvendelsen på længere sigt ikke vil kunne understøtte forretningsprocesserne.	Det anbefales, at ITU snarest udarbejder en IT-strategi, en risiko-analyse og en sikkerhedspolitik. Inspiration til udarbejdelsen kan hentes i Dansk Standards "Norm for edb-sikkerhed - del 1" (DS484-1: 2000), som ifølge regeringsbeslutning af 12. januar 2004 skal være obligatorisk for alle statsinstitutioner efter en 3- årig ind-køringsperiode. Nærmere oplysninger herom kan ses på www.oio.dk <http://www.oio.dk> under emnet "Standard for IT-sikkerhedsprocesser i staten".

2	***Væsentlighed:*** **Vigtigt** ***Titel:*** **Beredskabsplan** Rigsrevisionen har bemærket, at ITU ikke har en samlet beredskabsplan for IT-anvendelsen. ITU´s ledelse har således ikke taget stilling til, hvilke systemer og data, der er kritiske for driften, og hvor længe et nedbrud i de forskellige systemer højst må vare, uden at dette medfører alvorlige problemer og/eller risiko for tab. MULIG RISIKO: En manglende ledelsesmæssig stillingtagen til beredskabsplanen kan medføre risiko for, at en reetablering af normal drift bliver vanskelig, mere ressourcekrævende og tager længere tid, end hvis ledelsen på forhånd har gjort sig overvejelser om, hvordan reetableringen skal løses. Endvidere er der risiko for, at reetableringen alene løses ud fra tekniske kriterier og ikke ud fra de kriterier, som bedst muligt tilgodeser de forretningsmæssige behov.	Det anbefales, at ITU's ledelse - på baggrund af en risikovurdering - vurderer behovet for en samlet beredskabsplan. I så fald bør der tages stilling til, hvilke systemer og data, der er kritiske og kravene til reetableringstid. Beredskabsplanen bør være operationel, så den mere præcist omhandler de beslutninger, handlinger og disses rækkefølge, som det er aktuelt at tage stilling til i en nødsituation. Planen bør være fysisk tilgængelig (papirform).

UDKAST

3	***Væsentlighed:*** **Vigtigt** ***Titel:*** **Fysisk sikkerhed - adgang til serverrum** ITU har oplyst, at IT-driftspersonalet, betjente (intern service) og rengøringspersonale har adgang (nøgler) til serverrummene. MULIG RISIKO: Svagheder i den fysiske sikkerhed medfører risiko for, at udstyr kan stjæles eller ødelægges. Derved mister ITU tilgængeligheden til sine IT-ressourcer, og muligvis kan data komme i uvedkommendes besiddelse.	Det anbefales, at ITU begrænser kredsen af personer, der har adgang til serverrummene, og at det er IT-chefen, der godkender, hvem der må have adgang.

UDKAST

4	***Væsentlighed:*** **Vigtigt** ***Titel:*** **Sikkerhedskopier - adgangsret og opbevaring** Sikkerheden i forbindelse med opbevaring af daglige sikkerhedskopier og backupsæt er ikke tilstrækkelig, da alle IT-driftsmedarbejdere og betjente (intern service) generelt har adgang til kopi af driftsdata og alle backupsæt. Ligeledes er sikkerheden vedrørende opbevaring af originale program-cd'er (licenser), kildekoder mv. utilstrækkelig, idet disse er tilgængelige (i mapper) i IT-afdelingen. MULIG RISIKO: Backupsæt kan gå tabt ved en fejl eller ved bevidste/ubevidste handlinger, og placeringen indebærer risiko for samtidig ødelæggelse af driftsdata og backupsæt. Manglende sikringsforanstaltninger omkring adgang til originale program-cd'er kan medføre et erstatningsansvar i tilfælde af brud på licensrettigheder, fx ved at programmer mv. kopieres (stjæles) eller misbruges.	Det anbefales, at daglige sikkerhedskopier anbringes på internt arkiv af IT-driftsmedarbejderen. Endvidere anbefales det, at backupsæt anbringes på eksternt arkiv af en til formålet udpeget datamediebibliotekar, der ikke samtidig må være driftsmedarbejder. Udlevering af backupsæt fra det eksterne arkiv må kun ske efter skriftlig tilladelse fra IT-chefen. Endelig anbefales det, at ITU begrænser adgangen til originale program-cd'er mv., fx ved at opbevare disse i boks.

UDKAST

5	***Væsentlighed:*** **Vigtigt** ***Titel:*** **Driftsinstrukser og driftsovervågning** Bortset fra Navision Stat har ITU stort set ingen driftsinstrukser for den daglige drift af de væsentligste systemer, fx med hensyn til sikkerhedskopiering, administration af system- og dataejerskaber, bruger-administration og driftsovervågning. MULIG RISIKO: Manglende retningslinjer for den daglige administration og drift af de væsentligste systemer medfører afhængighed af de personer, der i dag løser opgaverne. Det kan også betyde, at opgaverne ikke løses med hensyn til forudsat/forventet indhold, omfang og kvalitet.	Det anbefales, at ITU udarbejder retningslinjer for den daglige systemdrift herunder kravene til dokumentation, fx med hensyn til: • Sikkerhedskopiering (omfang, hyppighed, placering, adgangsret, læsbarhed). • System- og dataejerskaber (fx KursusBase, Optag, mit.ITU, HSAS mv.). • Brugeradministration/logisk adgangskontrol (netværk, systemer (fx KursusBase, Optag, mit.ITU, HSAS mv.) og data). • Driftsovervågning (fastsættes ud fra en risikovurdering, bør ske regelmæssigt og dokumenteres i et fornuftigt omfang).

UDKAST

6	***Væsentlighed:*** **Vigtigt** ***Titel:*** **Firewall - overvågning og penetrationtest** ITU har foretaget en fornuftig segmentering af netværket, der indebærer en adskillelse af de forskellige netværkssegmenter (fx forskere, studerende m.fl.) og adgang til ressourcer på netværket. IT-afdelingen har oplyst, at man planlægger at etablere yderligere 2 segmenter i form af et L-Net (laboratorium) og et DMZ-net. IT-afdelingen varetager vedligeholdelsen af regelsættet i firewall'en. ITU mangler dog nogle retningslinjer for administration og overvågning af firewall'en. MULIG RISIKO: Manglende retningslinjer for administration af adgangen til/fra internettet og andre eksterne kilder medfører dels afhængighed af de personer, som i dag løser opgaven, og dels risiko for, at firewall'ens funktion ikke er afstemt med organisationens behov. Manglende overvågning af firewall'en medfører risiko for, at organisationens ledelse ikke kan reagere tilstrækkeligt effektivt på eventuelle svigt eller fjendtlige handlinger fra omverdenen.	Det anbefales, at ITU udarbejder nogle retningslinjer for den daglige drift og overvågning. Endvidere anbefales det, at firewallsikkerheden afprøves ved penetration tests af et uafhængigt firma, specielt når vedligeholdelsen varetages af nogle få personer.

UDKAST

7	***Væsentlighed:*** **Mindre vigtigt** ***Titel:*** **Systemadministratorrettigheder** Der er 13 medarbejdere i IT-afdelingen, der har fulde system-administratorrettigheder. MULIG RISIKO: Systemadministratorrettigheder, der er større end nødvendigt til løsning af opgaverne, medfører risiko for kompromittering af system-, data- og driftsikkerheden - enten ved bevidste eller ubevidste handlinger eller ved fejl.	Det anbefales, at ITU overvejer om tildelingen af systemadministra-torrettigheder bør begrænses, så nogle få medarbejdere har fulde administratorrettigheder, mens andre har begrænsede administra-torrettigheder, som er tilpasset opgavernes karakter.

UDKAST

8	***Væsentlighed:*** **Mindre vigtigt** ***Titel:*** **Change management** ITU foretager løbende opdatering af driftsmiljøet (fx patching, hot fixes og service packs), og ITU har forskellige udviklingsopgaver vedrørende selvbetjenings- og studieadministrative systemer. Der er ikke udarbejdet skriftlige change management procedurer, som kan reducere personafhængigheden, sikre kvaliteten af systemændringer og disses dokumentation herunder en hensigtsmæssig adskillelse af udviklings-, test- og driftsmiljøet. MULIG RISIKO: Manglende change management procedurer for programudvikling og idriftsættelse af ændrede programmer medfører dels afhængighed af de personer, som udvikler programmer, dels risiko for at programmerne bliver vanskelige at vedligeholde på grund af manglende brug af standarder eller mangelfuld dokumentation. Endvidere giver manglende procedurer risiko for, at programmer idriftsættes uden tilstrækkelig afprøvning, hvilket kan give driftsforstyrrelser og/eller tab af data.	Det anbefales, at ITU udarbejder procedurer for change management, der sikrer kvaliteten af systemændringer, disses dokumentation og en hensigtsmæssig adskillelse af udviklings-, test- og driftsmiljø.

UDKAST