
Sikkerhedspolitik for Teknologisk Institut.

Company	Teknologisk Institut
Address	Gregersensvej 1
Zip City	DK-2630 Taastrup
Telephone	7020 2000
Fax	

Policy name:	Sikkerhedspolitik
Created:	08-09-2006
Last edited:	01-12-2006
Last edited by:	Frederik Helweg-Larsen

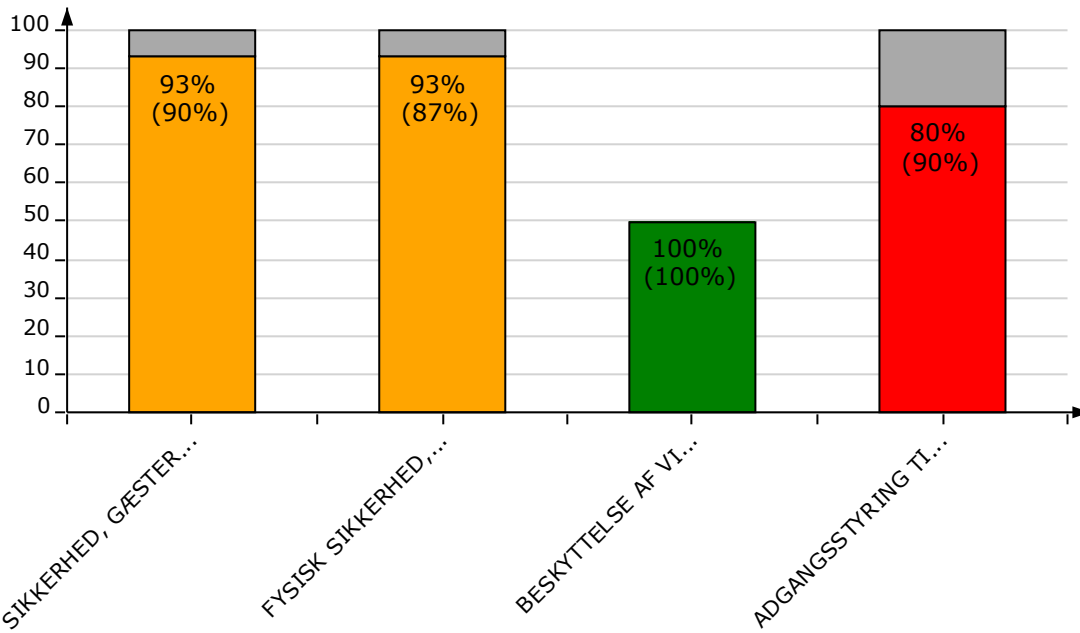
Based on the Danish Standard DS484, 2005

Management summary

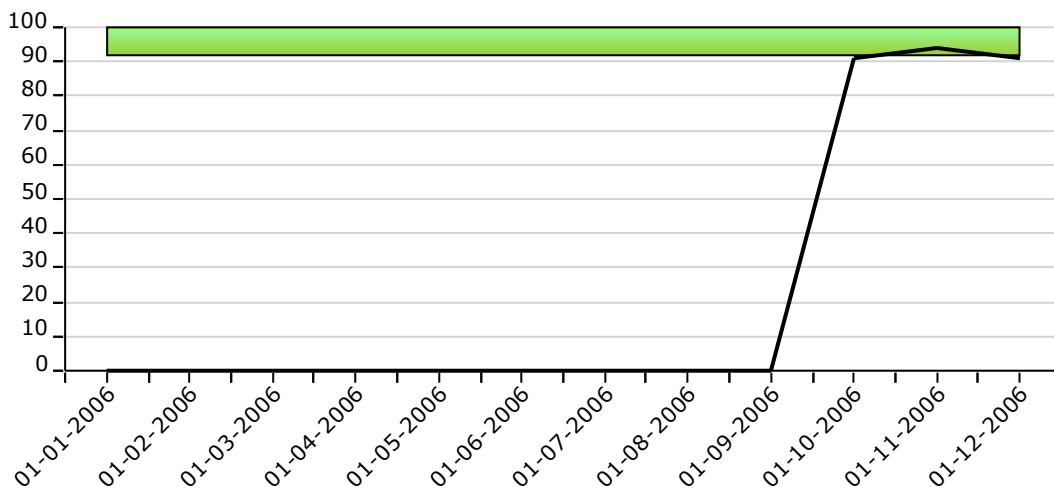
Conclusion:

Company is **NON COMPLIANT**

Overall Security Compliance:



Security Compliance History



Index**1 INDLEDNING**

<i>1.1 Hvorfor informationssikkerhed</i>
<i>1.2 Denne IT-sikkerhedspolitik og DS 484</i>
<i>1.3 Vurdering af sikkerhedsrisici</i>
<i>1.4 Valg af sikkerheds- og sikringsforanstaltninger</i>
<i>1.5 Virksomhedens specifikke sikkerhedsretningslinier</i>
<i>1.6 Dispensation fra IT-sikkerhedspolitikken</i>
<i>1.7 Risikohåndtering</i>
<i>1.8 Beredskabsplan</i>
<i>1.9 Hvordan er IT-sikkerhedspolitikken udarbejdet</i>
<i>1.10 Relevant lovgivning</i>
<i>1.11 Ansvar for vedligeholdelse</i>
<i>1.12 Gyldighedsområde og omfang</i>
<i>1.13 Gyldighedsdato og -periode</i>

2 VIRKSOMHEDENS IT-SIKKERHEDSPOLITIK

<i>2.1 Virksomhedens IT-sikkerhedspolitik</i>
---	-------

3 ORGANISERING AF IT-SIKKERHED**3.1 Interne organisatoriske forhold**

<i>3.1.1 Ledelsens rolle</i>
<i>3.1.2 Funktionsadskillelse</i>
<i>3.1.3 System- og dataejere</i>
<i>3.1.4 IT-sikkerhedsadministration</i>
<i>3.1.5 IT-drift</i>
<i>3.1.6 Brugernes ansvar</i>

3.2 Eksterne organisatoriske forhold

<i>3.2.1 Kontakt til myndigheder</i>
<i>3.2.2 Samarbejde med leverandører, konsulenter med flere</i>
<i>3.2.3 IT-sikkerhed i relation til kunder/kundebetjening</i>
<i>3.2.4 Fagligt samarbejde med grupper og organisationer</i>

3.3 Koordinering af IT-sikkerhedstiltag

<i>3.3.1 Linieorganisationen</i>
<i>3.3.2 IT-sikkerhedskoordinator</i>
<i>3.3.3 IT-sikkerhedsudvalg</i>

3.4 Virksomhedens IT-aktiver

<i>3.4.1 Registrering af informationsaktiver, dataklassifikation mv.</i>
<i>3.4.2 Registrering af systemaktiver, basisprogrammel</i>
<i>3.4.3 Registrering af systemaktiver, kommunikation</i>
<i>3.4.4 Registrering af systemaktiver, forretningsprogrammel</i>
<i>3.4.5 Registrering af fysiske aktiver, mærkning mv.</i>
<i>3.4.6 Ejerskab</i>

4 MEDARBEJDERE OG IT-SIKKERHED

4.1 Før ansættelse

4.1.1 *Clearing af ansøgere*

4.1.2 *Tavsheds- og hemmeligholdelseserklæringer*

4.2 Under ansættelsen

4.2.1 *Fysiske nøgler, ID-kort, tokens mv.*

4.2.2 *Omgang med virksomhedens IT-aktiver*

4.2.3 *Personlige password (kodeord) og andre koder*

4.2.4 *Uddannelse af medarbejdere - i relation til sikkerhed*

4.2.5 *Medarbejdernes opmærksomhed omkring sikkerhed*

4.2.6 *Nøglemedarbejdere - et ledelsesansvar*

4.2.7 *E-mail med forpligtelser for virksomheden*

4.2.8 *E-handel med forpligtelser for virksomheden*

4.2.9 *Medarbejdernes brug af offentlig tilgængelige computere*

4.2.10 *Privat anvendelse af virksomhedens Internet forbindelse*

4.2.11 *Privat anvendelse af virksomhedens e-mail faciliteter*

4.2.12 *Privat download og kopiering af musik, spil, pornografi mv.*

4.2.13 *Privat e-handel fra virksomhedens systemer*

4.2.14 *Brug af kameraer og mobilkameraer i virksomheden*

4.2.15 *Brug af TV-overvågning i virksomheden*

4.2.16 *Brug af lydoptagelser i virksomheden*

4.3 Efter ansættelsen

4.3.1 *Overdragelse af data og ejerskaber ved fratræden*

4.3.2 *Inddragelse af IT-rettigheder ved fratræden*

4.3.3 *Returnering af lånte IT-aktiver ved fratræden*

4.3.4 *Inddragelse af IT-rettigheder, aktiver mv. ved bortvisning*

5 SIKKERHED, GÆSTER OG SAMARBEJDSPARTNERE

5.1 Generelt for alle ikke-ansatte

5.2 Faste daglige partnere

5.2.1 *Rengøringspersonale* 10

5.2.2

Håndværkere

5.2.3 *Vareleverandører*

5.3 Faste IT-partnere

5.3.1 *Systemkonsulenter*

5.3.2 *Maskinteknikere*

5.3.3 *Systemudviklere*

5.4 Periodiske gæster

5.4.1 *Salgskonsulenter*

5.4.2 *Eksterne mødedeltagere*

5.4.3 Vikarer

5.4.4 Praktikanter

6 FYSISK SIKKERHED, SIKRING OG KONTROL

6.1 Bygningsmæssige forhold

6.1.1 Virksomhedens perimetersikring 10

6.1.2 Virksomhedens bygningsikring

6.1.3 Adgang til virksomhedens bygning(er)

6.1.4 Adgang til IT- og andre teknikrum

6.1.5 Adgang til og sikring af IT-kontorer

6.1.6 Sikring af hjemmearbejdspladser

6.1.7 Adgang og sikring af møde- og undervisningslokaler

6.1.8 Adgang og sikring af fællesområder

6.1.9 Adgang og sikring i forbindelse med lejere i bygning

6.1.10 Sikkerhedsforhold i forbindelse med ombygning

6.1.11 Alarmer, vagt og vægterrundering

6.2 IT-udstyr og andet teknisk udstyr, forsyningssikkerhed

6.2.1 Placering af IT- og teknikrum i bygning

6.2.2 Krav til placering af IT-udstyr i teknikrum

6.2.3 Strømforsyning og alarmering ved strømproblemer

6.2.4 Køling og ventilation - alarmering ved svigt

6.2.5 Sikring mod fugt- og vandskader - alarmering

6.2.6 Brandsikring og -alarmering

6.2.7 Sikring af kabler og krydsfelter

6.3 Anskaffelse, vedligehold og kassation

6.3.1 Anskaffelse, godkendelsesprocedurer

6.3.2 Serviceaftaler, reservedelssituation

6.3.3 Installation af hardware og software

6.3.4 Omflytning eller fjernelse af udstyr

6.3.5 Salg af IT-udstyr

7 SIKKERHED UNDER DRIFT / PRODUKTION

7.1 Operationelle forhold, batchproduktion

7.1.1 Driftsplanlægning

7.1.2 Driftsdokumentation

7.1.3 Driftsafvikling

7.1.4 Driftsovervågning og -kontrol

7.1.5 Driftsrapportering

7.1.6 Forsyning og lagring af forbrugsmaterialer

7.1.7 Ændringsstyring - Change Management.....

7.2 Særligt for drift hos ekstern serviceleverandør

7.2.1 Definition af leverancen, inkl. sikkerhedsaspekter

7.2.2 Overvågning og revision af serviceleverandør

7.3 Kritiske komponenter, klassifikation og registrering

<i>7.3.1 Kritiske hardware komponenter</i>	
<i>7.3.2 Kritiske softwarekomponenter</i>	
<i>7.3.3 Kritiske program- og datakomponenter</i>	
<i>7.3.4 Kritiske licensnøgler, password mv.</i>	
<i>7.3.5 Kritisk drift, alternative muligheder - beredskab</i>	

7.4 Programanvendelse

<i>7.4.1 Anvendt programmel i virksomheden</i>	
<i>7.4.2 Download og installation af programmel</i>	
<i>7.4.3 Beskyttelse mod skadevoldende programmer (AE)</i>	
<i>7.4.4 Beskyttelse mod skadevoldende programmer (ME)</i>	
<i>7.4.5 Sikring mod computervira (AE)</i>	
<i>7.4.6 Sikring mod computervira (ME)</i>	
<i>7.4.7 Sikring mod adware og spyware</i>	
<i>7.4.8 Sikring mod spam - indgående</i>	
<i>7.4.9 Sikring mod spam - internt</i>	
<i>7.4.10 Sikring mod spam - udgående</i>	

8 BESKYTTELSE AF VIRKSOMHEDENS DATA**8.1 Fysisk databeskyttelse**

<i>8.1.1 Sikring af system- og konfigurationsfiler</i>	
<i>8.1.2 Sikkerhedskopiering og opbevaring af datakopier</i>	
<i>8.1.3 Sikkerhedsarkivering jvf. lovgivning</i>	
<i>8.1.4 Sikkerhedskopiering ved teknologiskift</i>	
<i>8.1.5 Anvendelse af sikkerhedskopier fra dataarkiv</i>	
<i>8.1.6 Kontrol af datakopier i sikkerhedsarkiv</i>	
<i>8.1.7 Sikkerhed omkring brug af databærende medier</i>	
<i>8.1.8 Behandling af kasserede databærende medier</i>	

8.2 Databeskyttelse i forbindelse med udveksling af data

<i>8.2.1 Forsendelse og transport af databærende medier</i>	
<i>8.2.2 Elektronisk distribution af forretningsinformation</i>	
<i>8.2.3 Datasikkerhed i forbindelse med print</i>	
<i>8.2.4 Datasikkerhed i forbindelse med brug af telefax</i>	
<i>8.2.5 Udveksling af data med offentlige instanser</i>	
<i>8.2.6 Sikring ved overførsel af data til udlandet</i>	
<i>8.2.7 Anvendelse af kryptering</i>	

9 SIKRING AF VIRKSOMHEDENS NETVÆRK OG KOMMUNIKATION**9.1 Operationelle forhold, netværksdrift**

<i>9.1.1 Netværksdokumentation</i>	
<i>9.1.2 Netværksovervågning og -kontrol</i>	
<i>9.1.3 Driftsrapportering, netværksdrift</i>	

9.1.4 Ændringsstyring, netværk - Change Management	
9.1.5 Logning af aktiviteter og fejlrapportering	
9.2 Sikring af virksomhedens kommunikationslinier	
9.2.1 Sikring af virksomhedens kommunikationslinier	
9.2.2 Virksomhedens telefoncentral	
9.2.3 Virksomhedens brug af IP telefoni	
9.2.4 Netværkstopologi og konfiguration	
9.2.5 Internetopkobling og brug af firewall	
9.2.6 Internetopkobling og brug af firewall (OLD)	
9.2.7 Filtrering af indgående datastrøm gennem firewall	
9.2.8 Filtrering af udgående datastrøm gennem firewall	
9.2.9 Dial-in / dial-out	
9.2.10 Sikring af service- og diagnose porte	
9.2.11 Anvendelse og sikring af trådløse forbindelser	
9.2.12 Sikring i forbindelse med opkobling fra fjernarbejdspladser	
9.2.13 Brug af mobiltelefoni til dataoverførsel	
9.2.14 Sikring ved brug af netværksanalyser	
9.3 Drift af netværk eller web-sites hos ekstern serviceleverandør	
9.3.1 Definition af leverancen, inkl. sikkerhedsaspekter	
9.3.2 Overvågning og revision af serviceleverandør	
10 ADGANGSSTYRING TIL SYSTEMER OG DATA	
10.1 Administration af brugeradgang og rettigheder	
10.1.1 Overordnet styring af adgang til IT-systemerne	11
10.1.2 Tildeling af IT-adgange og rettigheder	
10.1.3 Opbygning af password (kodeord) (AE)	
10.1.4 Opbygning af password (kodeord) (ME)	
10.1.5 Tildeling af fælles bruger adgang	
10.1.6 Tildeling af periodiske rettigheder	
10.1.7 Ændring af IT-rettigheder ved funktions- eller afdelingsskift	
10.1.8 Overdragelse af IT-ejerskaber ved funktions- eller afdelingsskift	
10.1.9 Begrænsning af logon forsøg (AE)	
10.1.10 Begrænsning af logon forsøg (ME)	
10.1.11 Password - nulstilling	
10.1.12 Arbejdsstationer, ubemandede (AE)	
10.1.13 Arbejdsstationer, ubemandede (ME)	
10.1.14 Revision og kontrol af bruger konti	
10.1.15 Revision og kontrol af brugernes rettigheder	
10.1.16 Fysisk sikring af uovervåget IT-udstyr	
10.1.17 Logisk sikring af uovervåget IT-udstyr	
10.1.18 Logning af brugeraktiviteter 1 (AE)	
10.1.19 Logning af brugeraktiviteter 2 (AE)	

<i>10.1.20 Logning af brugeraktiviteter (ME)</i>
10.2 Styring af adgang til netværk	
<i>10.2.1 Identifikation og autentifikation af brugere</i>
<i>10.2.2 Identifikation af anvendt netværksudstyr</i>
<i>10.2.3 Styring af brugsperioder, automatisk afbrydelse</i>
10.3 Styring af adgang til operativ- og lignende systemer	
<i>10.3.1 Fabrikspassord på maskiner og i systemer</i>
<i>10.3.2 Brug og kontrol af nød koder</i>
<i>10.3.3 Brug af systemværktøjer</i>
<i>10.3.4 Identifikation og autentifikation af brugere (basissystemer)</i>
<i>10.3.5 Identifikation og autentifikation af brugere (forretningssystemer)</i>
<i>10.3.6 Styring af brugsperioder, automatisk afbrydelse</i>
11 SYSTEM- OG PROGRAMUDVIKLING, VEDLIGEHOLDELSE MV.	
11.1 Standard programmel	
<i>11.1.1 Anskaffelse og evaluering - programmel</i>
<i>11.1.2 Licensforhold og -kontrol</i>
<i>11.1.3 Test, godkendelse og igangsætning</i>
<i>11.1.4 Vedligeholdelse, opgradering 1</i>
<i>11.1.5 Vedligeholdelse, opgradering 2</i>
11.2 Generelt for udvikling af applikationer	
<i>11.2.1 Definition af udviklingsopgaven, inkl. sikkerhedsaspekter</i>
<i>11.2.2 Systemets sikkerhedsmæssige aspekter</i>
<i>11.2.3 Definition af systemets indbyggede kontroller</i>
<i>11.2.4 Adgangskontrol og brugerstyring i nye applikationer</i>
<i>11.2.5 Opbygning og sikring af systemdokumentation</i>
<i>11.2.6 Rettigheder og ophavsret til design og kode</i>
<i>11.2.7 Versionsstyring og ændringsstyring af programudgaver</i>
<i>11.2.8 Brug af produktionsdata i testforløb</i>
<i>11.2.9 Test, godkendelse og igangsætning af forretningssystemer</i>
11.3 Særligt for ekstern programudvikling	
<i>11.3.1 Kildekode deponering for eksternt udviklede programmer</i>
<i>11.3.2 Leverandørens adgang til produktionsdata i testforløb</i>
11.4 Administration og styring af web-sites	
<i>11.4.1 Styring og kontrol af virksomhedens domænenavne</i>
<i>11.4.2 Ansvar for vedligeholdelse af informationer på web-sites</i>
<i>11.4.3 Ansvar for regler og lovgivning for e-handel via web-sites</i>
<i>11.4.4 Kunders / borgeres adgang til information via web-sites</i>
<i>11.4.5 Sporing (tracking) af kunders adfærd på hjemmesiden</i>
12 STYRING AF SIKKERHEDSHÆNDELSER	
12.1 Advarselssystemer	

<i>12.1.1 Forhåndsvarsler om sikkerhedstrusler på vej</i>
12.2 Rapportering	
<i>12.2.1 Rapportering af sikkerhedshændelser</i>
<i>12.2.2 Rapportering af sikkerhedssvagheder og -eksponeringer</i>
<i>12.2.3 Mistanke om - og konstaterede sikkerhedsbrud</i>
<i>12.2.4 Anvendelse af logfiler til investigering</i>
12.3 Forsikringer og ansvar	
<i>12.3.1 Forsikringer</i>
<i>12.3.2 Ansvar ved brug af vagtselskaber</i>
12.4 Kriminelle akter	
<i>12.4.1 Håndtering af kriminalitet (medarbejdere)</i>
<i>12.4.2 Håndtering af kriminalitet (eksterne)</i>
<i>12.4.3 Sikring af og indsamling af beviser</i>
<i>12.4.4 Anvendelse af logfiler til investigering</i>
12.5 Kontroller og revision	
<i>12.5.1 Generel udførelse af kontroller</i>
<i>12.5.2 Intern IT-revision</i>
13 VURDERING AF RISICI, SÅRBARHEDER OG KONSEKVENSER	
<hr/>	
13.1 Forretningsrisici og konsekvenser	
<i>13.1.1 Analyse: Forretningskonsekvenser</i>
<i>13.1.2 Analyse: Årsag/Sandsynlighed</i>
<i>13.1.3 Analyse: Kritiske komponenter</i>
<i>13.1.4 Analyse: Beredskabskrav</i>
14 BEREDSKABSPLANLÆGNING OG KRISESTYRING	
<hr/>	
14.1 Beredskab - fra driftsproblem til krise	
<i>14.1.1 Opfyldelse af beredskabskrav</i>
<i>14.1.2 Etablering af en kriseorganisationen</i>
<i>14.1.3 Plan for situationeskalering</i>
<i>14.1.4 Handlingsplaner for beredskabsgrupper</i>
<i>14.1.5 Periodisk afprøvning af beredskabsplanerne</i>
15 BILAG / ARBEJDSDOKUMENTER	
<hr/>	

5 SIKKERHED, GÆSTER OG SAMARBEJDPARTNERE

5.2 Faste daglige partnere

5.2.1 Rengøringspersonale

Rengøring i IT- og teknikrum skal udføres af kendte faste personer, som har modtaget særlig vejledning og instruktion. Den IT-ansvarlige skal sørge for at rengøringspersonalet er bekendt med relevante sikkerhedsforhold og regler. Den IT-ansvarlige skal være bekendt med dato/tidspunkt for rengøringen. Ved rengøring i særligt følsomme områder bør overvågning overvejes.

Type: Manual Enforcement (ME)

Most recent audit: 30-11-2006

Audited by: Peter Hansen

Compliance target: 90%

Audit result: 80%

No. of test required: 1

No. of test performed:

Expected time use: 90 min

Actual time use: 40 min

Auditor Comments: Der er regelmæssig udskiftning af personalet hos rengøringsfirmaet.

Auditor File:

	Kræves gæstekort	Kræves faste folk på opgaven	Clearing af reng. folk nødvendig	Rengøring bekendt med opgaven	Rengøring fået nødvendig vejledning	Skal rengøring overvåges	Ansvarlig leder
Administration	Nej	Ja	Efter behov	Ja	Ja	Nej	Personalechef
Ekspedition	N/A	N/A	Delvis	N/A	N/A	Delvis	System- / dataejer
Produktion	N/A	N/A	Delvis	N/A	N/A	Delvis	System- / dataejer
Værksteder	N/A	N/A	Delvis	N/A	N/A	Delvis	System- / dataejer
Lagre	N/A	N/A	Delvis	N/A	N/A	Delvis	System- / dataejer
Teknikrum	Ja	Ja	Efter behov	Ja	Ja	Ja	IT-drift

6 FYSISK SIKKERHED, SIKRING OG KONTROL

6.1 Bygningsmæssige forhold

6.1.1 Virksomhedens perimetersikring

Virksomhedens ydre områder skal anlægges på en måde, der sikrer mod uretmæssig adgang, og som samtidig styrer gæsters adgang til og færden ved virksomheden. Perimeteren skal sikres mod uønsket adgang såvel til fods som i køretøj.

Gæster skal ledes til én eller flere sikrede og overvågede indgange. Gårdarealer skal holdes ryddelige og friholdes for materialer, der kan stables og benyttes til indtrængen på etager eller tag. Særligt følsomme områder skal være belyst i døgnets mørke timer, og TV-overvågning skal etableres hvor det er relevant.

Type: Manual Enforcement (ME)

Most recent audit: 23-11-2006

Audited by: Peter Hansen

Compliance target: 90%

Audit result: 80%

No. of test required: 1

No. of test performed:

Expected time use: 180 min

Actual time use: 45 min

Auditor Comments: Gårdarealerne var ikke rydede, og der lå stiger der ikke var låst fast.

Auditor File:

	Sikring mod person indtrængen	Sikring mod rambuk angreb	Gårdarealer ryddet	Ekstern belysning	TV-overvågning	Vagt, vægter kontrol	Ansvarlig leder
Administration	Hegn / mur	Pæle / plantekasser	Ja	Ja	Nej		N/A
Ekspedition	N/A	N/A	N/A	N/A	N/A		N/A
Produktion	N/A	N/A	N/A	N/A	N/A		N/A
Værksteder	N/A	N/A	N/A	N/A	N/A		N/A
Lagre	N/A	N/A	N/A	N/A	N/A		N/A
Teknikrum	N/A	N/A	N/A	N/A	N/A		N/A

10 ADGANGSSTYRING TIL SYSTEMER OG DATA**10.1 Administration af brugeradgang og rettigheder****10.1.1 Overordnet styring af adgang til IT-systemerne**

Adgang til virksomhedens systemer og data skal være rollebaseret og der igennem afspejle de daglige funktioner. Adgang til IT-systemer og data skal gives på need-to-know basis.

Rollerne fastlægges i et samarbejde mellem system- og dataejerne og den IT-ansvarlige. Rollerne, som skal være dokumenterede, vurderes og justeres efter behov, for eksempel i forbindelse med organisationsændringer eller lignende omlægninger i virksomheden.

Type: Manual Enforcement (ME)

Most recent audit: 23-11-2006

Audited by: Peter Hansen

Compliance target: 90%

Audit result: 80%

No. of test required: 10

No. of test performed: 10

Expected time use: 45 min

Actual time use: 60 min

Auditor Comments: Ud af de 10 senest tilkomne brugere var der én der afveg uden af det var dokumenteret. Nye retningslinier skal implementeres, og når dette er bragt på plads, beder afdelingslederen om ny audit.

Auditor File: e1171fe4-acfb-4676-91bc-3f75eff88d34Denne medarbejder er non-compliant.doc

Adgang baseres på	Adgangsforhold ajourføres	Adgang administreres af	Roller administreres af	Skal godkendes af

Netværksadgang	Person	Faste interv.	IT chef	Personalechef	IT sikkerhed
Systemadgang	Rolle	Faste interv.	Systemadministrator	Personalechef	IT sikkerhed
Applikationsadgang	Rolle	Periodisk	Afdelingschef	Personalechef	IT sikkerhed
Dataadgang	Rolle	Periodisk	Afdelingschef	Personalechef	IT sikkerhed