

09.12.07

IT-Politik

***Retningslinjer og regler
for medarbejderes, studerendes
og kursisters brug af
it-faciliteter hos
University College Lillebælt***

Indhold

Formål	3
It-faciliteter	4
Gode råd til brugernes om it-sikkerhed	5
Generelle it-regler for medarbejdere	7
Retningslinier for medarbejders brug af e-mail og kalender	8
Adgang til brugernes personlige data og dokumenter	10
Retningslinier for studerende, kursister og gæster	11
Hvad er uacceptabel brug af it-faciliteter?	12
Hvordan håndteres mistanke om uacceptabel brug af It-faciliteter?	14

Formål

Formålet med IT-politikken er:

- Beskrive de retningslinier og regler der gælder for medarbejderes og studerendes brug af University College Lillebælts it-faciliteter, herunder regler for arbejdsrelateret og privat brug af mail- og kalendersystem.
- At henvise til gældende lovgivning *) på området.
- At sikre at retningslinier og regler på området er aftalt og kommunikeret.

University College Lillebælts IT-politik er baseret på en grundlæggende tillid til at medarbejdere og studerende udviser personlig ansvarlighed i brugen af vores It-faciliteter, og at hver enkelt bruger gør sig bekendt med vores IT-politik og gældende lovgivning på området *).

IT-politikken beskriver også, hvad der sker, når det i enkeltsager skal afklares om IT-politikken retningslinier og regler ikke er overholdt.

*)

Persondataloven:

<http://www.datatilsynet.dk/publikationer/pjece/persondataloven.htm>

Offentlighedsloven:

<http://147.29.40.90/GETDOCI/ACCN/A19850057230-REGL>

Forvaltningsloven:

<http://147.29.40.90/GETDOCI/ACCN/A19850057130-REGL>

Lov om ophavsret:

<http://www.ophavsret.dk/Ophavsret/ophavsretsloven.htm>

Om IT-strategiske spørgsmål

For god ordens skyld skal det præciseres, at nærværende IT-politik ikke beskriver forretnings- og uddannelsesspecifikke strategier og målsætninger på it-området.

IT-politikken omhandler alene de generelle og lovgivningsrelaterede rammer for medarbejderes og studerendes brug af University College Lillebælts it-faciliteter.

It-faciliteter

Hvilke it-faciliteter er omfattet af IT-politikken?

- Internt datanetværk, der binder alle lokationer i University College Lillebælt sammen, herunder trådløs adgang på alle lokationer.
- Adgang til internet.
- Windows PC'ere (stationære og bærbare) og tilhørende udstyr.
- Fastnettelefoner og mobiltelefoner/smartphones/PDA'ere.
- Netværksprintere, hvor der anvendes adgangskoder ved udskrift af fortrolige dokumenter.
- Fælles- og personlige drev på netværket – herunder fjernadgang hertil.
- Standard Office programpakke - inkl. Outlook mail- og kalenderprogram, WebMail samt OutlookAnywhere.
- Fagsystemer, bl.a.:
 - Journal-, sags- og dokumenthåndteringssystem
 - Studie- og kursusadministrationssystem (SIS)
 - Økonomisystem (XAL/NavisionStat)
 - Bibliotekssystem (Integra)
 - Hjemmesidesystem/CMS (Composite)
 - E-læringsplatform (og evt. andre samarbejds- og konferencesystemer)
 - Videokonferencesystem (endnu ikke valgt)
 - IT-ServiseDesk-system.
- Rutiner for hurtig PC-systemgendannelse til oprindelig standardkonfiguration.
- Publicering på nettet, herunder evt. personlige arbejds/studierelaterede hjemmesider, pædagogiske logbøger, portfolios, blogs, wikies o.lign.

Gode råd til brugernes om it-sikkerhed

IT-sikkerhed bliver du først opmærksom på, når det ER gået galt - når du sletter dokumentet ved et uheld, eller computeren bliver lukket ned af en virus, mens du har allermest travlt.

IT-sikkerhed er også dit ansvar!

1. Brug din sunde fornuft når du bruger IT – det kan redde dig fra mange ærgrelser og spildt arbejdstid. Det stærkeste kort i beskyttelsen af din computer og dine vigtige dokumenter er din sunde fornuft - så du behøver ikke at være ekspert!
2. Stop aldrig din PC's antivirussystem.

Adgangskode

3. Brug en sikker adgangskode. Adgangskoden er den vigtigste beskyttelse mod misbrug af dine data og din person - vælg den med omhu – og lav den jævnlige om.
4. Vær varsom med din pc. Den er en mulig adgangsvej til alle University College Lillebælts systemer og data. Forlad aldrig din PC uden at logge ud af systemet og låse skærmen. Selv den bedste adgangskode er nytteløs, hvis du går fra din maskine uden at logge ud.
5. Udlevér aldrig din adgangskode til andre - den er strengt personlig. Lad aldrig Windows eller andre programmer huske dine adgangskoder. En god adgangskode indeholder mindst 8 tegn og er en blanding af tal og bogstaver - brug ikke æ, ø og å.

E-mails

6. Håndter e-mails og vedhæftede filer med omtanke. E-mails kan indeholde vedhæftede filer, du ikke bør åbne eller se på. Sund skepsis er dit bedste forsvar.
7. Sørg for at din e-post jævnligt efterses for ny post, og slet evt. spam-mails.

Internet

8. Brug Internet med omtanke. Din adfærd på nettet efterlader mange spor. Materiale, du henter, kan være beskyttet af ophavsret eller indeholde data der er skadelige for din computer.

Dokumenter

9. Gem dine dokumenter på netværkets fællesdrev og dine personlige drev. Når din PC ikke er koblet til University College Lillebælts netværk, så husk at gemme kopier af vigtige dokumenter på en USB-nøgle eller en ekstern harddisk - så du har en sikkerhedskopi at falde tilbage på ved et uheld. Gem dine dokumenter flere steder, så er du mindre sårbar.
10. Hvis du er i tvivl om IT-sikkerhed så kontakt University College Lillebælts IT-ServiceDesk.

IT-sikkerhed – i øvrigt

For at IT-sikkerheden kan opretholdes, er det væsentligt, at alle følger de givne retningslinier og er opmærksom på, at brud på sikkerheden et enkelt sted kan have følger for mange.

IT-systemer, der ejes af University College Lillebælt, skal være tilgængelige for institutionen. Det betyder at, systembrugernavne og tilhørende kodeord, krypteringsnøgler og nøgler til andre sikringsmekanismer, skal deponeres i pengeskabe eller på anden betryggende vis, således at administrator eller andre bemyndigede medarbejdere i givet fald kan få adgang til systemerne, ved den normale systemansvarliges fravær.

De deponerede oplysninger skal ajourføres, når der sker ændringer.

Materiale, der er omfattet af offentlighedsloven eller forvaltningsloven, må ikke opbevares/arkiveres på krypteret form.

Kryptering og efterfølgende dekryptering, der sker (automatisk) mellem afsender og modtager for at sikre datatransporten er ikke omfattet af forbudet mod kryptering.

Husk om sikkerhedskopiering!

Brugernes personlige dokumenter gemt lokalt på PC'en er **IKKE** omfattet af IT-afdelingens sikkerhedskopiering. Sørg derfor for at dine personlige dokumenter også gemmes på dit personlige drev på netværket, hvor IT-afdelingen sørger for daglig sikkerhedskopiering/backup.

Generelle it-regler for medarbejdere

Ved at anvende University College Lillebælts it-faciliteter accepterer alle brugere at opfylde gældende love, herunder nærværende retningslinier og regler, samt evt. lokale bestemmelser.

Alle brugere er ansvarlige for enhver brug af deres personlige adgange og konti og har pligt til at håndtere passwords mv. forsvarligt, således at de ikke utilsigtet kommer andre i hænde.

Brugerne må ikke beskadige, fjerne eller ændre mærkater (fx PC-navn, modelnummer, serienummer, stregkoder) på University College Lillebælts IT-udstyr.

Privat brug

It-faciliteter i University College Lillebælt understøtter institutionens drift. Det er tilladt i begrænset omfang, at It-faciliteterne anvendes til privat brug, forudsat at den private brug fortrinsvis sker udenfor normal arbejdstid og at den ikke forstyrrer eller overbelaster IT-driften.

Brug af fildelingssystemer er ikke tilladt!

IT-udstyr hjemlånt af medarbejdere er omfattet af nærværende IT-politik.

Dokumentformat ved brug af Office2007-pakken

I forbindelse med brugen af Office2007 skal alle brugere gemme Office-dokumenter i formatet "97-2003 dokumentformat", fx Word: *.doc og Excel: *.xls., af hensyn til kompatibilitet med tidligere og eksterne systemer.

Brug af udstyr, herunder installation af programmer

University College Lillebælts PC'ere (og printere), er konfigureret til vores netværk, og vedligeholdes automatisk via netværket, herunder sikkerhedsopdateringer af Windows, Office-pakken og anden software.

Af hensyn til en effektiv og sikker drift er det alene IT-afdelingen der må ændre disse indstillinger, ligesom udstyret alene må serviceres og repareres via IT-afdelingen.

Brugerne må gerne installere andre programmer til egen arbejdsmæssig brug, men det påhviler alene brugeren at sikre at licensregler og tredjepartsrettigheder overholdes for disse programmer.

IT-ServiceDesk hjælper gerne med installation af programmer, både shareware-programmer og licensbaserede programmer.

I tilfælde hvor en større gruppe af brugere har brug for særlige programmer eller programpakker kan IT-afdelingen automatisere installation og vedligeholdelse heraf.

Retningslinier for medarbejderes brug af e-mail og kalender

!	Ang. retningslinjer for behandling af indgående e-post refereres til University College Lillebælts journalvejledning og journalnøgle.
----------	---

E-mail og kalender

- E-mails har status som al anden skriftlig kommunikation i University College Lillebælt. Kalenderaftaler (og kommunikation herom) er at sidestille med e-mails.
- Du skal holde din kalender åben for læsning af kolleger, så de kan se *hvornår du indenfor dine normale arbejdstider er tilgængelig* for fx telefonisk kontakt og for evt. planlægning af møder. Åbne kalendere er desuden en forudsætning for at vores receptionister kan yde den bedst mulige service, bl.a. ved indkommende opkald og viderestilling.
- Du skal anvende kalendersystemet til at booke interne og eksterne arbejdsrelaterede mødeaftaler. *Du behøver ikke at gøre detaljer i din kalender synlig for andre, blot de kan se hvornår du er tilgængelig for fx telefonisk kontakt og mødeplanlægning.*
- Du kan give en kollega adgangsrettigheder til at tilgå din postkasse/kalender i tilfælde af længerevarende fravær. Pågældende medarbejder/kollega er underlagt fortrolighed og tavshedspligt overfor din mail og kalender.
- Lederen kan, hvis det findes nødvendigt i forbindelse med en opgaves udførelse, beslutte at du skal give en kollega adgangsrettigheder til at tilgå din postkasse/kalender. Pågældende medarbejder/kollega er underlagt fortrolighed og tavshedspligt overfor din mail og kalender.
- Personfølsomme og fortrolige data og informationer må ikke sendes via University College Lillebælts WebMail (mail.ucl.dk) – de skal sendes via Outlook2007-klienten i Office-pakken.
- Det er ikke tilladt at have automatisk viderestilling fra egen mailadresse/mailboks til mailsystemer udenfor University College Lillebælts Exchange/Outlook-system.
- Du skal være opmærksom på, at forskellige typer bilag (vedhæftede filer) kan indeholde virus. Åbn derfor ikke bilag hvor du er usikker på indholdet. Kontakt eventuelt IT-ServiceDesk, hvis du er i tvivl.
- Hvis du modtager post, der er adresseret forkert, skal du sende svar til afsenderen om at posten er adresseret forkert.
- Svar **ALDRIG!** på spam-mails.

Besvarelse af e-mails:

!	Retningslinier for besvarelse af e-mail fra studerende fastlægges lokalt. Svartider for interne og eksterne henvendelser kan være yderligere fastlagt af lokale servicemål for ekspedition af henvendelser.
----------	---

Hovedprincippet er at du skal sørge for at de e-mails du modtager bliver besvaret i løbet af få arbejdsdage – af dig, en kollega eller en anden medarbejder i University College Lillebælt.

IT-Politik

ucl_it-politik_ver15_cw091207.doc



Besvarelsen kan alene være en bekræftelse af modtagelsen og, hvis henvendelsen fx kræver igangsættelse af en egentlig sagsbehandling, en angivelse af forventet ekspeditionstid.

I øvrigt:

- Check din mailboks for modtagne e-mails hver arbejdsdag, så vidt det er muligt.
- Besvar e-mails senest 3 arbejdsdage efter modtagelsen – evt. med en meddelelse der angiver hvornår der vil blive svaret på henvendelsen, og hvis det ikke er dig selv der besvarer den, hvem der så vil besvare henvendelsen.
- Hvis du ikke kan efterse indbakken i din mailboks i en periode, så sørg for at en kollega passer den i denne periode, eller indstil din mailboks til at sende et autosvar til afsenderen med besked om:
 - hvornår du besvarer e-mails igen, **og**
 - hvem der kan kontaktes i stedet, eller at e-mailen automatisk bliver videresendt til en kollega som vil besvare henvendelsen.

Kodeks for indhold i e-mails

- Skriv altid et emne i emnerubrikken, og skriv høfligt, kort, præcist, enkelt og overskueligt.
- Husk at anvende en signatur der tydeligt angiver dine kontaktinformationer for modtageren. Brug evt. en kort signatur til kolleger (fx navn, stilling/funktion, afdeling/enhed, telefonnumre), og en lang signatur til eksterne kontaktpersoner (fx navn, stilling, afdeling/enhed, adresse, hovedadresse, telefonnumre, mailadresse, website).
- Brug Cc (kopi til – modtagere angivet hér kan ses af de andre modtagere) med omtanke. Pas på med at svare alle oprindelige modtagere – det er ofte ikke nødvendigt.
- Brug kun Bcc (blind kopi til – modtagere angivet hér kan ikke ses af de andre modtagere) i særlige tilfælde.
- Brug ikke e-mail til følelsesladede budskaber.
- Husk at e-mails skal kunne tåle at blive læst af andre. Nogle medarbejdere har brug for (evt. i perioder) at give en sekretær eller en anden kollega adgang til sin mailboks.
- Husk at dine e-mails i tilfælde af mistanke om (evt. andres) it-misbrug kan blive åbnet af ledelsen ved undersøgelser af mistanken.

Adgang til brugernes mailkonti

Hvis det af driftsmæssige årsager er nødvendigt, kan IT-medarbejdere uden forudgående varsel åbne en medarbejders mailkonto for at udbedre problemet. Mailkontoens ejer skal hurtigst muligt orienteres herom og have anvisning på korrekt anvendelse af systemet.

IT-medarbejdere er pålagt fortrolighed og tavshedspligt i forbindelse med tilgang til mailkonti.

Adgang til brugernes personlige data og dokumenter

Ved driftsarbejde kan IT-medarbejdere have behov for at tilgå data og filer i forbindelse med vedligeholdelse eller undersøgelse. **IT-medarbejdere er pålagt fortrolighed og tavshedspligt i forbindelse med tilgang til disse personlige data og filer.**

Overvågning og logning af vores IT-systemer sker alene af hensyn til drift, fejlretning, sikkerhed, genetablering og dokumentation. Det kan fx være i forbindelse med undersøgelse af it-faciliteters logfiler for fejl og/eller driftsforstyrrelser, netværksovervågning, undersøgelse af e-post der ikke er blevet leveret til en postkasse, håndtering af virus- og spamfiltre, brug af internet, afklaring af ressourcebegrænsninger o.lign.

Adgang til logning og overvågning er begrænset til personale hvis opgave det er at sikre it-driften. **IT-medarbejdere (og evt. eksterne IT-konsulenter) skal respektere fortrolighed og tavshedspligt brugernes personlige og evt. private data og filer, og skal behandle disse i overensstemmelse med bestemmelserne i persondataloven.**

Håndtering af brugerdata og brugerrettigheder

IT-afdelingen henter de basale brugerdata i University College Lillebælts personaleenhed og i studieadministrationen. Brugernavne/bruger-ID og mail-adresser dannes automatisk ud fra disse stamdata.

Brugeres adgang til It-faciliteterne styres via tildeling af brugerrettigheder. Disse rettigheder skal løbende revideres i overensstemmelse med brugerens behov.

En brugers adgang til it-faciliteter skal lukkes hvis brugeren ikke længere er ansat, er sygemeldt på ubestemt tid, har længerevarende orlov eller andre begrundede forhold, hvor ledelsen vurderer at adgangen bør lukkes.

!	Personaleenheden og studieadministrationen udarbejder procedurer, herunder tidsfrister, for ændring af medarbejders og studerendes adgang til it-faciliteter og it-systemer ved tilgang, afgang og flytning.
---	--

Retningslinier for studerende, kursister og gæster

Du kan bruge University College Lillebælts It-faciliteter ved at koble din egen PC til vores netværk, eller ved at bruge en af vores studie/kursus-PC-arbejdspladser.

Som bruger af University College Lillebælts It-faciliteter har du følgende forpligtigelser:

- Såfremt du er i besiddelse af eget personligt brugernavn og adgangskode, skal du altid koble dig på University College Lillebælts netværk med det. Brugernavn og adgangskode må ikke gives eller udlånes til andre.
- Du skal altid logge af PC'en, når du forlader den.
- Du må ikke foretage ulovlige handlinger ved brug af University College Lillebælts It-faciliteter og internettet.
F.eks. er download af musikfiler, video og andet beskyttet materiale forbudt, ligesom kopiering og distribution af piratkopier ikke må finde sted.
- Du må ikke foretage handlinger ved brug af University College Lillebælts It-faciliteter, der er til skade for University College Lillebælts omdømme.
- Du må ikke ændre computerens opsætning og/eller installere programmer på computeren, medmindre det sker som led i undervisningen eller efter aftale med den IT-ansvarlige.
- Du må ikke anvende University College Lillebælts computere i kommercielt øjemed.
- Ved overtrædelse udsætter du dig for følgende:
- Du kan få din ret til at anvende University College Lillebælts computere inddraget.
- Du kan i særlig grove tilfælde blive bortvist fra University College Lillebælt og/eller politianmeldt.
*Du risikerer at få bøde eller i særlig grove tilfælde fængselsstraf som følge af ulovlige handlinger foretaget ved brug af University College Lillebælts computere.
Erstatningsansvaret påhviler alene den enkelte bruger, der har foretaget den ulovlige handling. University College Lillebælt er ikke ansvarlig for ikke-ansattes (dvs studerendes og kursister) handlinger.*

Adgang til brugernes data, filer og mails

Ved driftsmæssige forstyrrelser og ved begrundet mistanke om alvorligt misbrug af University College Lillebælts computere, kan IT-afdelingen efter forudgående godkendelse hos ledelsen, foretage gennemgang af en brugers data og filer, herunder evt. mail, og iværksætte undersøgelser. Den enkelte bruger skal i givet tilfælde orienteres snarest muligt efterfølgende.

IT-medarbejdere er pålagt fortrolighed og tavshedspligt i forbindelse med tilgang til personlige data, filer og e-mails.

Hvad er uacceptabel brug af it-faciliteter?

Uacceptabel brug af University College Lillebælts it-faciliteter er brug der:

- er direkte ulovlig,
- kompromitterer it-sikkerheden, eller
- skaber it-driftforstyrrelser ved brud på retningslinier eller regler.

Eksempler

Nedenfor gives en række eksempler på aktiviteter, der må anses for uacceptable. Listen er ikke udtømmende.

Det er uacceptabelt for brugere, der ikke er autoriseret hertil, at:

- Forsøge at få adgang til personlige og/eller personfølsomme informationer.
- Anvende en anden brugers adgangskode(r).
- Søge informationer om password eller data som tilhører andre brugere.
- Udføre aktiviteter, som ikke overholder gældende love og regulativer, herunder uautoriseret kopiering af ophavsretsligt materiale, brug af retsbeskyttet software uden licens eller formidling af uautoriserede kopier af retsbeskyttet software til andre.
- Forsøge at omgå IT-sikkerhedsmetoder og operativsystemer eller undersøge sårbarheder i andre It-faciliteter eller på netværk.
- Anvende University College Lillebælts It-faciliteter til privat kommerciel brug.
- Opfange eller undersøge data uden de fornødne rettigheder eller autorisation.
- Forstyrre eller afbryde andre brugeres og It-faciliteters arbejde eller deltage i en aktivitet, som kan medføre tab af andre brugeres og It-faciliteters data.
- Publicere indhold på personlige arbejdsrelaterede hjemmesider der kan kompromittere University College Lillebælt eller er ulovlig.
- Udføre aktiviteter som kompromitterer University College Lillebælts IT-sikkerhedsregler og retningslinier eller andre lokale politikker, herunder forsøg på at omgå IT-sikkerhedsbestemmelser eller ressourcebegrænsninger ved at tilsløre eller forfalske sin identitet.

Brug af Internet

- Det er ikke tilladt at anvende internetadgangen til private kommercielle formål.
- Brug af internet fra University College Lillebælts netværk bør ske med omtanke da infektion med virus eller anden skadelig software kan få store negative konsekvenser for hele netværket.
- Hold dig fortrinsvis til internetsider fra kendte firmaer eller organisationer, og søg ikke efter "useriøse" sider. Der kan ikke gives en fast definition på hvad "useriøse" sider er, men et pejlemærke er e sund fornuft og undgåelse af sider med porno, spil, chat, hacker,

IT-Politik

ucl_it-politik_ver15_cw091207.doc



musik, video, fildeling og lignende. Udover at søgning på nogle af disse typer hjemmesider kan være ulovlig, er det ofte på denne type sider, at der gemmer sig virus, spyware og ødelæggende programmer.

- Download fra internettet må kun foretages, hvis det har et arbejdsmæssigt formål.
- Vær opmærksom på, at al færden på internettet efterlader elektroniske spor, der kan henføres til University College Lillebælt, på de servere der er besøgt. Når du færdes på internettet fra University College Lillebælts netværk bør du derfor aldrig besøge sider eller foretage handlinger, der på nogen måde kan virke kompromitterende for University College Lillebælt.
- Vær opmærksom på, at det ikke er lovligt at publicere fx fotos på nettet af personer der ikke forudgående har givet tilladelser hertil, ligesom loven om ophavsret naturligvis skal respekteres ved publicering og tilgængeliggørelse af andres værker via nettet.

Hvordan håndteres mistanke om uacceptabel brug af It-faciliteter?

I tilfælde hvor der kan konstateres en overtrædelse af University College Lillebælts IT-politik, eller hvor der er en begrundet mistanke om overtrædelse af University College Lillebælts IT-politik, skal IT-chefen kontaktes.

Henvendelser om overtrædelser af University College Lillebælts IT-politik skal altid undersøges og behandles seriøst, og henvendelsen skal besvares. Den mistænkte nærmeste leder og IT-chefen skal i alle tilfælde orienteres.

Enhver kendt overtrædelse af University College Lillebælts IT-politik skal analyseres for at udelukke eventuelle forsætlige fejl. Den mistænkte, dennes nærmeste leder og direktionen inddrages i undersøgelsen.

Det vil i mange tilfælde være tilstrækkeligt at afklare en hændelse ved en opklarende samtale med de implicerede parter. Det kan dreje sig om misforståelser, tekniske fejl eller brugerfejl og dermed være uforsætlige for brugeren af den pågældende IT-facilitet.

En anden kilde til undersøgelse af påstande om uacceptabel brug af University College Lillebælts it-faciliteter er:

- Logfiler, idet en del af it-brugen i University College Lillebælt logges, og dermed kan efterspores og henføres til en given bruger.
- IT-afdelingen kan om nødvendigt og ved tvivlsspørgsmål vælge at inddrage eksterne konsulenter eller andre myndigheder.

Alle personer involveret i opklarende virksomhed eller overvågning er undergivet tavshedspligt vedrørende de oplysninger af fortrolig karakter, de måtte få kendskab til.

Ledelsen behandler eventuelle sanktioner i forbindelse med overtrædelsen af University College Lillebælts IT-politik efter gældende regler i University College Lillebælt, herunder de personaleretslige regler.

Ulovlig brug af University College Lillebælts it-faciliteter (herunder internet), kan desuden medføre påtale, skriftlig advarsel og have disciplinære konsekvenser som fx afskedigelse i henhold til gældende regler.

I særligt grove tilfælde kan ledelsen foretage en politianmeldelse og inddrage politiet i efterforskningen.

Pressen vil i givet tilfælde blive håndteret af rektor.

Overtrædelser af University College Lillebælts IT-politik af ekstern part - herunder misbrug af it-faciliteter vil om nødvendigt blive anmeldt til CERT (Computer Emergency Response Team).

Vedrørende undersøgelse af påstande om uacceptabel brug af University College Lillebælts it-faciliteter henvises endvidere til Dansk IT's "Quick guide – Optimering af efterforskningsmulighederne ved datakriminalitet", der kan downloades her:

http://www.dansk-IT.dk/upload/quick_guide_endelig_lav.pdf

IT-Politik

ucl_it-politik_ver15_cw091207.doc



Ovennævnte IT-politik er vedtaget af XXX d. XXX og godkendt af XXX d. XXX

IT-politikken har været behandlet af XXX ... og træder i kraft d. XXX