



# IT-sikkerhedspolitik Rebild Kommune



|   |    |
|---|----|
| Indledning  | 3  |
| Baggrund og formål  | 3  |
| Indholdet i IT-sikkerhedspolitikken   | 5  |
| Bilag A: Lovkrav, organisering og ansvar.   | 6  |
| Bilag B: Beskrivelse af interessenter, roller og ansvar.  | 7  |
| Bilag C: Risikostyring (risikovurdering, og -forebyggelse)                                      | 8  |
| Bilag D: Beredskabsstyring: Procedure for håndtering af sikkerhedshændelser og<br>nødberedskab. | 9  |
| Bilag E: Anskaffelse, vedligeholdelse og udskiftning af hardware & software.                    | 10 |
| <i>Adgang.</i>  | 11 |
| <i>Overvågning.</i>   | 11 |
| <i>Lager af hardware og rekvireret udstyr</i>   | 11 |
| Bilag G: Ansvarlig for håndtering af adgangskontrol.  | 12 |
| Bilag H: Ansvarlig for håndtering af data.  | 13 |
| Bilag I: Anvendelse af intranet og Internet i Rebild Kommune.                                   | 14 |
| Intranet  | 14 |
| Anvendelse af Internet  | 14 |
| Privat brug af Internet   | 14 |
| Download  | 14 |
| Bilag J: Retningslinier for brug af e-post i Rebild Kommune                                     | 15 |
| Modtagelse af krypteret/sikker post/digital signatur  | 15 |
| Afsendelse af krypteret/sikker post/digital signatur  | 15 |
| Virus   | 15 |
| Distribution til egen privat postkasse  | 16 |
| Anvendelse af arbejdsmail til private mails   | 16 |
| Personfølsomt og fortroligt data  | 16 |
| Download af patches, updates og div. Microsoftværktøjer   | 16 |
| Bilag K: Mobile arbejdspladser (Internt og eksternt)  | 17 |
| Bilag L: Hjemmearbejdspladser (Citrix / webmail).   | 18 |



## Indledning

Det overordnede mål med IT-sikkerhedspolitikken er at have ét fælles dokument for, hvordan IT-sikkerheden er defineret, og hvordan IT-sikkerheden reguleres i forbindelse med styring af sikkerhedshændelser.

### ***Dokumentets målgruppe og læsevejledning***

IT-sikkerhedspolitikken er et dokument, der kan læses på intranettet i sin helhed. Nye medarbejdere vil få udleveret en "*pixiudgave*", specielt rettet mod bruger relaterede forhold. IT-sikkerhedspolitikken er sat sammen af en række bilag, der som enkeltstående dokumenter adresserer hvert sit emne. Alle på afdelings- og institutionslederniveau bedes dog gennemlæse den samlede IT-sikkerhedspolitik.

## Baggrund og formål

IT-sikkerhedspolitikken for Rebild Kommune definerer, hvordan IT-sikkerheden varetages i Rebild Kommune. IT-sikkerhedspolitikken og de opsamlede sikkerhedshændelser evalueres løbende ud fra en IT-sikkerhedslog, som minimum tages op hver 6. måned.

Derfor tager dokumentet udgangspunkt i en overordnet risikovurdering af sikkerheden i forbindelse med Rebild Kommunes IT-anvendelse. Ud fra en tankegang om "at en kæde ikke er stærkere end det svageste led", skal dette dokument således medvirke til at;

- ❖ Identificere svaghederne, og
- ❖ Beskrive løbende tiltag til at minimere effekten af disse svagheder.

Dette gøres bl.a. ved at beskrive en række af nødberedskaber, der kan tages i brug ved allerede identificerede hændelser.

Formålet med IT-sikkerhedspolitikken er at skabe et fælles grundlag for anvendelse af IT-sikkerhed ud fra Rebild Kommunes almindelige værdisæt. Derfor er der i mindre grad lagt vægt på restriktiv regelstyring og i større grad regulering af adfærd ud fra den betragtning, at medarbejderne kan bruge sund fornuft og er ansvarlige.

I umiddelbar tilknytning til IT-sikkerhedspolitikken udarbejdes der en kort, generel og vejledende beskrivelse til medarbejdere samt retningslinier for

1. Eksterne samarbejdspartnere og leverandører
2. Håndtering af borgerrelaterede data på Rebild Kommunes hjemmeside
3. IT-medarbejders anvendelse af systemer
4. Brugerautorisation
5. Logning



6. Anvendelse af E-mail.
7. Skærmlås. (Risiko hvis den undlades)
8. *Trådløs hacking*

IT-sikkerhedspolitikken skal sammen med vejledning og retningslinier være med til at danne et grundlag for at der kan foretages revision.



## Indholdet i IT-sikkerhedspolitikken

Indholdet i IT-sikkerhedspolitikken baserer sig på nedenstående emner:

- A.** Lovkrav, organisering og ansvar
- B.** Interessenter og roller
- C.** Risikostyring
- D.** Beredskabsstyring
- E.** Fysisk sikkerhed
- F.** Anskaffelse, vedligeholdelse samt udskiftning af hardware og software
- G.** Håndtering af adgangskontrol og datasikkerhed i Rebild Kommunes IT-miljø
- H.** Anvendelse af Internet og Intranet
- I.** E-mailpolitik
- J.** Mobile arbejdspladser
- K.** Hjemmearbejdspladser



## Bilag A: Lovkrav, organisering og ansvar.

Rebild Kommune overholder gældende lovgivninger og tilstræber at effektuere væsentlige anbefalinger fra KL og regering vedr. IT-sikkerhed.

Der vil i 2008 blive taget stilling til, hvordan arbejdet med indførelse af DS484 (*Dansk standard om IT-sikkerhed*) efterfølgende skal foregå.

Kommunaldirektør Erik Odder er officielt øverste sikkerhedsansvarlige. Erik Odder har uddelegeret ansvaret til stabschef Lars Peter Schou, der har ansvar for opfølgning og kontrol. IT-chef Per Bo Christensen har det daglige driftsansvar.

Den enkelte afdelings- og institutionsleder har ansvaret for at læse og forstå Rebild Kommunes IT-sikkerhedspolitik.

Den enkelte medarbejder har sammen med nærmeste leder, ansvaret for at overholde de retningslinier og de regler der angives i IT-sikkerhedspolitikken.

Dette gælder i forbindelse med anvendelse af systemer og data der skabes i forbindelse med anvendelse af systemer. Oversigt over systemer findes i "Mål for service fra IT-afdelingen til Rebild Kommunes organisation" (SLA) bilag 15.

Væsentlige ændringer til IT-sikkerhedspolitikken skal godkendes politisk efter forudgående drøftelse i chefgruppen.



## Bilag B: Beskrivelse af interessenter, roller og ansvar.

I forbindelse med håndtering af sikkerhedspraksis i Rebild Kommune har hver enkelt et ansvar, der dagligt skal varetages.

Nedenstående er en skematisk beskrivelse af, hvem der i det daglige arbejde, har ansvaret for de enkelte sikkerhedsområder.

|  | <i>Sikkerhed ansvarlig</i> | <i>IT-<br/>chef</i> | <i>IT-<br/>afd.</i> | <i>Afd./<br/>Inst-<br/>leder</i> | <i>Fagsystem-<br/>ejer</i> | <i>Medar-<br/>bejder</i> | <i>Super<br/>bruger</i> | <i>revision</i> |
|--|----------------------------|---------------------|---------------------|----------------------------------|----------------------------|--------------------------|-------------------------|-----------------|
| <i>IT sikkerhedspolitik</i>                | ✓                          |                     |                     |                                  |                            |                          |                         | ✓               |
| <i>Opdater IT<br/>sikkerhedslog</i>        |                            | ✓                   | (✓)                 |                                  |                            |                          |                         |                 |
| <i>Backup</i>                              |                            | ✓                   | (✓)                 |                                  |                            |                          |                         |                 |
| <i>Serverrum</i>                           |                            | ✓                   | (✓)                 |                                  |                            |                          |                         |                 |
| <i>Identifikation af<br/>fagsystemejer</i> |                            | ✓                   |                     | ✓                                |                            |                          |                         |                 |
| <i>Adgang til fagsystem</i>                |                            |                     |                     | ✓                                | (✓)                        |                          |                         |                 |
| <i>Adgang til andre<br/>systemer</i>       |                            | ✓                   | (✓)                 |                                  |                            |                          |                         |                 |
| <i>Adgang til netværk</i>                  |                            | ✓                   | (✓)                 |                                  |                            |                          | (✓) *                   |                 |
| <i>Passwordbeskyttelse</i>                 |                            |                     |                     |                                  |                            | ✓                        | vejledning              |                 |
| <i>Låsning af skærm</i>                    |                            |                     |                     |                                  |                            | ✓                        | vejledning              |                 |
| <i>Opbevaring af data</i>                  |                            |                     |                     |                                  |                            | ✓                        | vejledning              |                 |
| <i>Adgang data</i>                         |                            |                     |                     | ✓                                | (✓)                        |                          |                         |                 |

SKEMA1; Roller/Ansvar

(✓) uddelegeret ansvar \* løbet af 2008

Med "*fagsystemer*" menes, eksempelvis Acadra og KMD systemer. Med "*andre systemer*" menes eksempelvis Mail og intranet.

I forbindelse med at kunne spore sikkerhedshændelser skal datatransaktioner kunne spores – lige fra systemarbejde på servere og netværk til adgang til fagsystemer og anvendelse af disse, jf. beskrivelse af brugerautorisation og logning.

Sikkerhedshændelser registreres i en sikkerhedslog. Denne log drøftes halvårligt mellem stabschef og IT-afdeling, således regulering af risikostyring og beredskabsstyring kan tilpasses.



## Bilag C: Risikostyring (risikovurdering, og -forebyggelse)

For at vurdere hvilke hændelser der kan forekomme, arbejdes der i IT-sikkerhedspolitikken generelt med risikostyring. Her tænkes der på, at få vurderet og prioriteret relevante risici, således forebyggelse kan igangsættes inden en konkret sikkerhedstrussel opstår.

Nedenstående tabel er en oversigt over nogle af de risici, der kan true IT-sikkerheden i Rebild Kommune. Hver hændelse har en **risikoprofil**, der er dannet ud fra en samlet vurdering af

- ❖ Risiko for at indtræffe (angivet i skema som risiko)
- ❖ Konsekvens for IT-drift (server og netværk) samt sikkerhed kompromitteres – (angives i skema som K IT-dr)
- ❖ Konsekvens for IT-anvendelse generelt (brugeranvendelse) – (angives i skema som K IT-an)

*Risiko* og *konsekvens* angives med værdierne 1 – 10. Risikoprofilen for hver hændelse er en multiplikation af de 3 tal. Den samlede vurdering angiver dermed, hvilke forhold der umiddelbart skal have størst prioritet. Alle sikkerhedshændelser vurderes dog som "kritisk" jf. "Mål for service fra IT-afdelingen til Rebild Kommunes organisation", kap. 6.

| Hændelse  | Risiko | K IT-dr | K IT-an | Samlet | Forbyggelsesindsats                      | Prioritering |
|---|--------|---------|---------|--------|--|--------------|
| 1 Servernedbrud                                 | 8      | 10      | 10      | 800    | Overvåg, vedligehold, redundance, backup |              |
| 2 Større virus/hackerangreb                     | 5      | 5       | 10      | 250    | Firewall, Virusskjold, sikkerhedstjek    |              |
| 3 Brand i serverrum                             | 2      | 10      | 10      | 200    | Check alarm, brandslukningsudstyr        |              |
| 4 IT- medarbejder. PW misbruges                 | 2      | 10      | 6       | 120    | Uddannelse, PW regler                    |              |
| 5 Vandskade                                     | 2      | 7       | 8       | 112    | Dykpumpe installeret, rør afskærmet      |              |
| 6 Langt strømsvigt                              | 2      | 5       | 10      | 100    | Check generator                          |              |
| 7 Brugers password (PW) misbruges               | 4      | 8       | 2       | 64     | Uddannelse, PW regler                    |              |
| 8 Kort strømsvigt                               | 3      | 2       | 10      | 60     | Check UPS                                |              |
| 9 Print med følsomme oplysninger bortkommer     | 8      | 3       | 2       | 48     | Placering af printer, "sund fornuft"     |              |
| 10 Mindre virus/hackerangreb                    | 2      | 6       | 3       | 36     | Firewall, Virusskjold                    |              |
| 11 Tyveri                                       | 5      | 2       | 2       | 20     | Mærkning, alarm, bygning aflåses         |              |
| 12 Bærbart datamedie inficeres eller bortkommer | 8      | 1       | 1       | 8      | Virusskjold, "sund fornuft"              |              |

SKEMA2: Risiko/forebyggelse

Det er hensigten, at tabellen løbende skal udvikles og tilføjes oplysninger, efterhånden som der identificeres flere risici.



## Bilag D: Beredskabsstyring: Procedure for håndtering af sikkerhedshændelser og nødberedskab.

I forbindelse med at sikkerhedshændelser indtræffer, vil der efterfølgende blive iværksat nødberedskab, således IT-sikkerheden kan blive genoprettet. Endnu ikke definerede risikoelementer vil blive opsamlet i IT-sikkerhedsloggen. Efter at sikkerhedshændelsen er afdækket, udbedret og analyseret revurderes risikostyringen i Rebild Kommunes IT-sikkerhedspolitik.

I forbindelse med håndtering af sikkerhedshændelser skal der udarbejdes konkrete procesbeskrivelser for hvert enkelt nødberedskab. Procesbeskrivelserne vil kunne kombineres, hvor der måtte være behov for dette.

| Hændelse  | Samlet | Nødberedskab  | Nødberedskab efterfølgende  |
|---|--------|---|---|
| 1 Servernedbrud                                 | 800    | Afhjælp fejl, flyt services til ny server               | Vurder skader, vurder årsag, opdater IT-sikkerhedslog, afreporter         |
| 2 Større virus/hackerangreb                     | 250    | Monitorer, opdater IT- sikkerhedslog rapporter          | Overvej lukning af netforbindelse, forbedre sikkerhed, afreporter         |
| 3 Brand i serverrum                             | 200    | Check automatisk slukning                               | Vurder skader, vurder årsag, opdater IT- sikkerhedslog, afreporter        |
| 4 IT- medarbejder PW misbruges                  | 120    | Luk konto, ændre password                               | Efterforsk brud, opdater IT-sikkerhedslog, Informer leder                 |
| 5 Vandskade                                     | 112    | 1.. Luk for vand. 2. Tjek at pumpe kører. 3. Nedlukning | Udbedre skaden, forebyg gentagelse, opdater IT- sikkerhedslog, afreporter |
| 6 Langt strømsvigt                              | 100    | Check generator   | Efterforsk, opdater IT- sikkerhedslog, rapporter,                         |
| 7 Brugers password (PW) misbruges               | 64     | Luk konto, ændre password                               | Efterforsk brud, opdater IT-sikkerhedslog, Informer leder                 |
| 8 Kort strømsvigt                               | 60     | Check generator   | Efterforsk, afreporter  |
| 9 Print med følsomme oplysninger bortkommer     | 48     | opdater IT- sikkerhedslog                               | afreporter  |
| 10 Mindre virus/hackerangreb                    | 36     | Monitorer, opdater IT- sikkerhedslog                    | afreporter  |
| 11 Tyveri                                       | 20     | Spær enheden, anmeld tyveri, opdater IT- sikkerhedslog  | afreporter  |
| 12 Bærbart datamedie inficeres eller bortkommer | 8      | Rens medie, opdater IT sikkerhedslog                    | afreporter  |

SKEMA3; håndtering af sikkerhedshændelser og nødberedskab



## Bilag E: Anskaffelse, vedligeholdelse og udskiftning af hardware & software.

Ønskes der anskaffet software et givet sted i organisationen, skal dette drøftes med IT-afdelingen forud for anskaffelse. IT-afdelingen fastlægger overordnede regler for håndtering af hardware og software i Rebild Kommunes IT-miljø. Disse regler sigter mod, at give den størst mulige driftssikkerhed.

Hardware og software vil kunne blive forlangt udskiftet, hvis det vurderes, at der er risiko for sikkerhedsbrud, og at sikkerhedsbruddet har dybe konsekvenser for Rebild Kommunes IT-miljø og daglige drift.

IT-afdelingen har ansvaret for at installere software på medarbejdernes IT-arbejdspladser. Det er ikke tilladt for medarbejderne at downloade og installere free-ware eller shareware-programmer på Rebild Kommunes IT-arbejdspladser. Hvis der ønskes adgang til software kontaktes IT-afdelingen gennem Rebild Kommunes superbrugerorganisation eller via [itsupport@rebild.dk](mailto:itsupport@rebild.dk).



## Bilag F: Fysisk sikkerhed

### ***Adgang.***

Adgang til serverrum er begrænset til IT-afdelingens personale og enkelte interne servicemedarbejdere, der har ansvar for alarmsystem.

Eksterne servicemedarbejdere eller leverandører kan få adgang efter specifik aftale om tidsrum, arbejdets omfang og indflydelse på andre systemer. Dissets besøg noteres i en besøgslog. Som hovedregel skal der være en IT-konsulent fra Rebild Kommune til stede, når der er eksterne servicemedarbejdere eller leverandører til stede i serverrum.

Eksterne servere og netværksudstyr opbevares i aflåste rum eller skabe.

PC'er, PDA'er og printere tyverimærkes.

### ***Overvågning.***

Serverrummet overvåges af alarm (Brand/indbrud/oversvømmelse). Alarm overvåges af rådhusbetjent. Alarmernes funktionsduelighed checkes efter fastlagt interval. Ved alarm kontaktes såvel rådhusbetjent som afdelingsleder for IT-afdelingen.

Brandslukning er installeret. Brandslukning checkes efter fastlagt interval.

Servere og netværksudstyr dækkes helt eller delvist af UPS og generatoranlæg. UPS og generatoranlæg checkes efter fastlagt interval.

Gnaverbekæmpelse aftales. (Gift kasser udendørs og fælder indendørs)

IT-afdelingen er omfattet af det generelle alarmsystem og er desuden udstyret med røgkanon. Uautoriseret adgang uden for åbningstid udløser røgkanonen, hvorved muligheden for tyveri minimeres inden vagtselskab har kontaktet personale i Rebild Kommune. Hvis alarmerne udløses aktiveres overvågningsudstyret hvorved hændelsen optages på video.

### ***Lager af hardware og rekvireret udstyr***

Hardware indkøbt til udskiftning – f.eks. af pc, tastatur, mus, skærm, lagringsmedier m.v. opbevares forsvarligt aflåst i tilknytning til serverrum.

Rekvireret udstyr af afdelinger eller institutioner i Rebild Kommune klargøres og placeres i IT-afdelingen til afhentning eller levering efter nærmere aftale.



## Bilag G: Ansvarlig for håndtering af adgangskontrol.

Adgangskontrol betyder fysisk eller elektronisk styring af adgang til lokaler, systemer, filer og hardware.

Fysisk adgangskontrol er aflåsning af rum og sikring af at IT-udstyr opbevares forsvarligt i og uden for Rebild Kommunes bygninger.

Elektronisk adgangskontrol er sikring vha. oprettelse af brugerlogin/password eller brug af kode på PDA.

| <b>ADGANGSKONTROL</b>    | <b>IT-afd.</b> | <b>Systemejer</b> | <b>Ejer</b> |
|--------------------------|----------------|-------------------|-------------|
| <b>Serverrum</b>         | ✓              |                   |             |
| <b>Netværk</b>           | ✓              |                   |             |
| <b>PC, Citrix og PDA</b> | ✓              |                   | ✓           |
| <b>Systemer</b>          | ✓              | ✓                 |             |
| <b>Filer</b>             | ✓              | ✓                 | ✓           |

SKEMA4; Ansvar for adgangskontrol



## Bilag H: Ansvarlig for håndtering af data.

Ansvar for håndtering af data henviser til, hvordan omgang med data skal foregå, samt hvem der har ansvaret herfor.

Omgang med data betyder alt omgang med information – hvad enten det er elektronisk på harddisk, CD, USB nøgler, mail eller udskrift i papirformat.

Som hovedregel befinder data sig i Rebild Kommunes datalagringsmedier - og heraf tages der løbende backup med et fastlagt interval. Data gemmes i 6 versioner. Der foretages test af genindlæsning af data efter fastlagte intervaller. Data kan flyttes eller kopieres til eksterne medier – bærbare PC, PDA, USB nøgler, CD/DVD eller via. mail.

Data der skabes, opbevares eller redigeres udenfor de interne datalagrings medier, er alene ejerens ansvar. Hermed forstået, at disse data skal håndteres sikkerhedsmæssigt korrekt, således at de ikke beskadiges, slettes, bortkommer eller overdrages til uautoriseret anvendelse, hvorved der sker overtrædelse af datatilsynets bestemmelser.

| <b>DATAOPBEVARING</b>      | <b>IT-afd.</b> | <b>Systemejer</b> | <b>Ejer</b> |
|----------------------------|----------------|-------------------|-------------|
| <i>Filservere</i>          | ✓              |                   |             |
| <i>PC</i>                  |                |                   | ✓           |
| <i>PDA</i>                 |                |                   | ✓           |
| <i>Systemer</i>            | ✓              | ✓                 |             |
| <i>CD, USB nøgler etc.</i> |                |                   | ✓           |

SKEMA5: Ansvar for håndtering af data.

For at undgå at løbe en unødvendig risiko henvises der til Rebild Kommunes Citrix løsning, der giver mulighed for, at arbejde med data på de interne datalagrings medier fra en vilkårlig PC. Løsningen forudsætter;

- ❖ At PC'en har adgang til internettet.
- ❖ At brugeren er oprettet på Rebild Kommunes netværk
- ❖ At brugere har en elektronisk kodenøgle

Anvendes denne løsning er alt data sikret, på lige fod med data der behandles internt på Rebild Kommunes netværk.



## Bilag I: Anvendelse af intranet og Internet i Rebild Kommune.

### **Intranet**

Medarbejdere i Rebild Kommune, der er oprettet som brugere på kommunens IT-netværk, bør dagligt gøre sig bekendt med nyheder og meddelelser, der publiceres via kommunens intranet.

Information om nedbrud på mail- eller IP telefoniplatform vil fremgå på intranettet.

### **Anvendelse af Internet**

Rebild Kommunes internetforbindelse er oprettet med henblik på arbejdsrelateret brug og for at sikre, at kommunens ansatte har adgang til informationer, som kan understøtte deres arbejdsfunktioner. Alt brug af Internet forventes at ske ud fra brug af "sund fornuft"

Det vil blandt andet sige, at:

- Ved brug af Internet tages der højde for risikoen for virus-angreb og spam.
- Den enkelte medarbejder må ikke downloade og installere programmer. IT-afdelingen har ansvaret for, at de nødvendige anti-virusprogrammer og sikkerhedsindstillinger er på plads.

### **Privat brug af Internet**

Det er tilladt for medarbejdere, at anvende Internet til privat brug under forudsætning af, at det er foreneligt med varetagelse af medarbejderens arbejde i kommunen. Kun medarbejderen selv må tilgå Internettet via Rebild kommunes Netværk.

Uanset hvor man bevæger sig på Internettet, vil man efterlade et visitkort, som viser, at man kommer fra Rebild Kommune.

Det er derfor ikke tilladt at besøge hjemmesider med pornografisk, racistisk, voldeligt eller ulovligt indhold. Skulle en medarbejder uforvarende alligevel besøge en sådan hjemmeside, skal webbrowseren straks lukkes.

### **Download**

Det er ikke tilladt for den enkelte medarbejder at hente programmer med henblik på anvendelse på udstyr tilkøbt Rebild Kommunes netværk. Hvis der til arbejdsmæssigt brug er behov for et bestemt program kan installation kun ske efter godkendelse af IT-afdelingen.

Dokumenter kan downloades såfremt det ikke er i strid med gældende lovgivning.



## Bilag J: Retningslinier for brug af e-post i Rebild Kommune

Rebild Kommunes e-post-system er oprettet med henblik på arbejdsrelateret brug. Enhver e-post sendt eller modtaget via kommunens system opfattes derfor som tilhørende Rebild kommune.

Rebild Kommune tillader dog privat brug - se vejledning på intranettet.

### **Modtagelse af krypteret/sikker post/digital signatur**

I Rebild Kommune kan man sende og modtage sikker e-mail vha. sikkerpost@rebild.dk. Den sikre e-post vil automatisk blive videresendt til den almindelige e-postkasse. Den fremsendte e-post vil ikke være signeret og krypteret. E-posten vil som minimum indeholde signaturbeviset og indholdet af den modtagne sikre e-post, herunder vedhæftede filer. E-posten kan videresendes, journaliseres mv. på samme måde som en almindelig e-post.

Hvis signaturkontrollen afslører, at det anvendte certifikat ikke er gyldigt, vil den sikre e-post ikke blive videresendt til den almindelige e-postkasse.

### **Afsendelse af krypteret/sikker post/digital signatur**

Når der anvendes sikker e-mail er det tilladt at sende følsomme eller fortrolige oplysninger ved hjælp af e-mail. Når man anvender sikker e-mail vil mail blive krypteret og der vedhæftes en digital signatur.

I Rebild kommune benyttes der virksomhedssignaturer. Signaturen er således en "underskrift" fra Rebild Kommune og ikke fra en bestemt medarbejder. Den digitale signatur svarer til, at man anvender kommunens officielle brevpapir.

### **Virus**

Det er IT-afdelingens ansvar at tilse, at e-post kommunikation er sikret i samarbejde med den enkelte. Følgende retningslinjer skal iagttages af alle medarbejdere:

1. E-post uden afsender må ikke åbnes, men skal slettes umiddelbart
2. E-post, der kan karakteriseres som spam, må ikke besvares. Ved spam forstås e-post, som modtageren ikke har bedt om at få, som ikke er relevant for modtageren, og hvor modtageren ikke er direkte relateret til indhold eller afsender
3. Vedhæftede filer må kun åbnes, når afsenderen er kendt, og der ikke synes at være tvivl om ægtheden af filerne.

I tvivlstilfælde skal IT-afdelingen kontaktes inden åbning af e-post og/eller filer. Hvis man som bruger har mistanke om, at en pc har fået virus, skal alle operationer på pc'en straks stoppes, og IT-afdelingen skal kontaktes omgående.

Advarsler og orientering om virusangreb må alene udsendes af IT-afdelingen.



## **Distribution til egen privat postkasse**

E-post må af sikkerhedsmæssige grunde ikke videresendes automatisk til eksterne mailsystemer.

## **Anvendelse af arbejdsmail til private mails**

Efter en medarbejders fratreden har Rebild Kommune ret til, at åbne, læse, gemme og slette E-post, som er sendt til den fratrådte medarbejder. Dette gælder også eventuel privat post, som således ikke vil blive videresendt. Det anbefales derfor, at medarbejderen flytter privat kommunikation til en mappe mærket "Privat e-post" eller lignende.

Medarbejderen må kun anvende og videregive sin personlige e-post-adresse til nyhedsbreve, debatfora, chat mv. i arbejdsrelaterede sammenhænge.

Det er ikke tilladt at benytte officielle e-postkasser til privat brug.

## **Personfølsomt og fortroligt data**

Medarbejderen har pligt til at slette e-post med følsomme eller fortrolige oplysninger efter 30 dage jf. Persondatalovens bestemmelser. Journalisering skal således være foretaget forinden 30 dage fra modtagelse og afsendelse.

## **Download af patches, updates og div. Microsoftværktøjer**

Det er ikke tilladt at downloade og eksekvere filer til Outlook, der vil kunne give ekstra funktionalitet.

IT-afdelingen sørger for, at den fornødne funktionalitet i Outlook er på plads ved hjælp af central opdatering.



## Bilag K: Mobile arbejdspladser (Internt og eksternt)

Rebild Kommune bruger mobile arbejdspladser i form af bærbare pc'er og PDA'er

Bærbare pc'er kan bruges med netværksforbindelse på alle Kommunens lokationer. Hvis der arbejdes på bærbare pc'er udenfor disse lokationer vil det udelukkende kunne ske, ved at arbejde med data lokalt på maskinen, ud fra de angivne krav omkring håndtering af data (se bilag H), eller ved at der arbejdes via Rebild Kommunes Citrix platform (se bilag L).

PDA'er kan sættes til at synkronisere data med brugerens egen pc via USB stik eller bluetooth. Alternativt kan synkronisering foregå via Rebild Kommunes Secure Mobil GPRS zone via TDC. Alle PDA'er skal have installeret antivirusprogram for PDA.

Af sikkerheds- og økonomiske hensyn, er det ikke tilladt at anvende PDA'en til at surfe på Internettet. Derudover er det ikke tilladt, at hente og installere software til PDA'en.

Såfremt der er ønsker om installation af andet software på PDA, skal dette aftales med IT afd. Først når IT afd. har testet softwaren, kan installationen foretages.

Bortkommer udstyr meldes dette omgående til IT-afdelingen, således at nødvendige forhåndsregler kan tages i brug.



## Bilag L: Distancearbejdspladser (Citrix / webmail).

Rebild Kommune tilbyder flere muligheder for at arbejde udenfor Rebild Kommunes net.

Dette kan enten ske vha. brug af bærbar pc og PDA (se bilag K). Alternativt kan det ske ved at gøre brug af Citrix Metaframe eller Microsoft Exchange Webmail.

Adgang til Rebild Kommunes Citrix platform gives af IT-afdelingen efter aftale med medarbejderen og dennes leder. For at få adgang modtager medarbejderen en personlig elektronisk Citrix nøgle. Adgangen skal fortrinsvis ske fra medarbejderens egen pc, hvor medarbejderen har administrator rettigheder.

Adgang til Microsoft Exchange Webmail er givet til alle, der er oprettet som brugere på Rebild Kommunes domæne. Adgangen til denne service kan ske fra en vilkårlig pc hjemme hos en medarbejder, på biblioteket, internetcafe eller via egen PDA etc. Fælles for en sikkerhedsmæssig forsvarlig brug af denne service er, at der sættes korrekt flueben i felterne offentlig / privat pc, samt at der ikke gemmes data lokalt på maskinen. Dette være sig data om logningsaktivitet, anvendelse af password samt filer der er downloadet. Er det nødvendigt at downloade filer til en offentlig computer, skal filen(erne) efterfølgende slettes ved at markere filen(erne) og trykke samtidig på "Shift" og "Del".



## Ordforklaring

|                         |   |  |
|-------------------------|---|--|
| Antivirusprogram        | = | Software til beskyttelse mod virus                             |
| Backup                  | = | Sikkerhedskopiering  |
| Citrix                  | = | Software til distancearbejdsplads                              |
| Downloade               | = | Hente programmer eller data på Internettet.                    |
| Free-ware               | = | Gratis software  |
| Generatoranlæg          | = | Dieseldrevet dynamo  |
| GPRS                    | = | General Packet Radio System – Bredbånd via mobiltelefoninettet |
| Hacking                 | = | Udefrakommendes forsøg på at få adgang til netværket           |
| Hardware                | = | PC, printer, server  |
| Intranet                | = | Intern hjemmeside  |
| IP telefoni             | = | Telefoni baseret på datanetværk                                |
| Officielle e-postkasser | = | E-postkasser der bruges af afd. Eller funktioner               |
| Password                | = | Personlig kodeord  |
| PDA                     | = | Personlig digital assistent eller lommecomputer                |
| Secure Mobile GPRS      | = | Bredbånd via mobiltelefoninettet med ekstra sikkerhed          |
| Share-ware              | = | Gratis software med begrænset funktionalitet                   |
| SLA                     | = | Service Level agreement (Det aftalte serviceniveau)            |
| Software                | = | Programmer   |
| Superbruger             | = | Korps af medarbejdere med stærke IT kompetencer.               |
| UPS                     | = | Uninterruptible power Supply – Batteri backup                  |
| USB nøgle               | = | Digital lagringsmedie  |
| Webbrowser              | = | Software til visning af internetsider                          |
| Webmail                 | = | Mail der kan læses vha. webbrowser                             |
| Virus                   | = | Inficeret software   |