CIR nr 10242 af 04/11/2007 (Historisk)

Cirkulære om sikkerhedsforanstaltninger i Kirkenettet

Ministerium: By-, Land- og Kirkeministeriet

Journalnummer: Kirkemin., dokid. 346100

Cirkulære om sikkerhedsforanstaltninger i Kirkenettet

Cirkulæret omhandler organisatoriske forhold og fysisk sikring, herunder sikkerhedsorganisation, administration af adgangskontrolordninger og autorisationsordninger samt kontrol med autorisationer for brug af edb-udstyr og programmer med adgang til Kirkenettet.

Desuden omhandler cirkulæret Kirkeministeriets godkendelse af øvrige it-systemer.
Cirkulærets bilag findes alene på Kirkenettets Intranet under punktet IT-sikkerhed.

Cirkulærets anvendelsesområde

§ 1. Cirkulæret omfatter alle edb-arbejdspladser der har adgang til Kirkenettet. Hjemmearbejdspladser og arbejdspladser i Rigsrevisionen, samt hos Kirkeministeriets IT-leverandører med adgang til Kirkenettet, er også omfattet af bestemmelserne i cirkulæret.

Stk. 2. Alle brugere af Kirkenettet er omfattet af bestemmelserne i nærværende cirkulære.

Stk. 3. Alle hjemmearbejdspladser er desuden omfattet af de i Bilag 6 nævnte bestemmelser.

Stk. 4. I cirkulærets bilag 8 er der fastsat bestemmelser vedrørende de it-systemer Kirkeministeriet godkender.

Definitioner

§ 2. Ved Kirkenettet forstås det edb-netværk med tilhørende edb-arbejdspladser, der er etableret i og mellem myndigheder, institutioner og ansatte. Desuden omfatter Kirkenettet arbejdspladser i Rigsrevisionen og hos Kirkeministeriets IT-leverandører.
Ved en bruger forstås en person, som er tildelt et brugernavn og en adgangskode til Kirkenettet.
Ved autorisation forstås kombinationen af et brugernavn og en adgangskode, som giver adgang til Kirkenettet eller et program tilknyttet Kirkenettet.
Ved sikkerhedsansvarlig forstås en person, der har et sikkerhedsmæssigt ansvar for en eller flere brugere og for et eller flere installationssteder.

Organisatoriske forhold

§ 3. Afdelingschefen for Kirkeministeriets Personale- og IT-Afdeling er øverste sikkerhedsansvarlige for Kirkenettet og tilhørende systemer og herunder for, at der fastsættes retningslinier for tilsyn med overholdelsen af de sikkerhedsforanstaltninger, der er fastsat.

§ 4. Kirkeministeriets IT-Kontor forestår den daglige drift af Kirkenettet og træffer herunder de fornødne tekniske foranstaltninger til opretholdelse og kontrol af sikkerheden i Kirkenettet.

§ 5. Til varetagelse af de sikkerhedsmæssige opgaver i Kirkenettets enkelte dele er udpeget lokale sikkerhedsansvarlige.

Stk. 2. De lokale sikkerhedsansvarlige tildeler, ændrer og fratager brugerne autorisation. De skal desuden sikre, at:

- oplysninger ikke misbruges eller kommer til uvedkommendes kendskab
- lokalerne, hvori der sker behandling af data, er indrettet med henblik på at forhindre uvedkommende adgang til oplysningerne.

Stk. 3. De lokale sikkerhedsansvarlige skal sikre, at brugerne får udleveret dette cirkulære og overholder de heri indeholdte regler og sikkerhedsforskrifter, der gælder for Kirkenettet, og skal påtale, hvis regler og forskrifter ikke overholdes. Hvis en bruger herefter fortsat tilsidesætter de gældende sikkerhedsforanstaltninger, foranlediger den lokale sikkerhedsansvarlige at Kirkeministeriets IT-Kontor straks spærrer den pågældende brugers autorisation.

Stk. 4. En fortegnelse over de lokale sikkerhedsansvarlige fremgår af Bilag 1 til cirkulæret.

Autorisation af brugere

§ 6. Autorisation af nye brugere, ændring af og fratagelse af autorisation for eksisterende brugere iværksættes af IT-Kontoret på grundlag af skriftlig anmodning fra den lokale sikkerhedsansvarlige. Anmodninger skal af de lokale sikkerhedsansvarlige fremsendes på de blanketter, som er optrykt i Bilag 2.

Stk. 2. Såfremt IT-Kontoret:

- ikke kan verificere den sikkerhedsansvarliges underskrift, skal anmodningens autenticitet kontrolleres ved opringning til den sikkerhedsansvarlige
- ikke kan kontrollere en ny brugers identitet i Kirkeministeriets informationssystem (KIS), skal identiteten verificeres ved opringning til den sikkerhedsansvarlige eller eventuelt ved opringning til den relevante stiftsøvrighed
- er i tvivl om anmodningens ægthed, skal anmodningen forelægges chefen for IT-Kontoret.

Stk. 3. Når en anmodning er ekspederet og kontrolleret af IT-Kontoret, sendes det i Bilag 3 indeholdte stamkort i 3 eksemplarer til den sikkerhedsansvarlige i udfyldt stand.

- et eksemplar er den sikkerhedsansvarliges kvittering
- et eksemplar er til brugeren med oplysning om, hvilke autorisationer han er tildelt
- et eksemplar, der skal underskrives af brugeren, returneres til IT-Kontoret som kvittering for modtagelsen.

Stk. 4. Samtidig sendes til brugerens privatadresse en pinkodekuvert med brugerens hemmelige og strengt personlige adgangskode sammen med dette cirkulære.
Desuden vedlægges en instruks til brugeren om at gennemlæse cirkulæret og derefter henvende sig til den lokale sikkerhedsansvarlige for at få udleveret brugernavn(e).
Ved udlevering af brugernavn(e) skal brugeren underskrive det i stk. 3 nævnte stamkort og kvitterer hermed for at have modtaget og læst bestemmelserne i cirkulæret.

Stk. 5. For autorisation af vikarer i stifterne gælder særlige retningslinjer, jf. Bilag 7.

§ 7. Ved tildeling af autorisation(er) er det den sikkerhedsansvarliges ansvar, at brugere ikke autoriseres til anvendelser, som de ikke har behov for.

Stk. 2. Den lokale sikkerhedsansvarlige skal, som angivet i § 6 stk. 1, give besked om fratagelse af en autorisation ved ændret arbejdsfordeling, fravær længere end 6 måneder og ved fratræden.

Adgang til og adgangskontrol i Kirkenettet

§ 8. Autorisationen giver brugeren adgang til Kirkenettets postsystem og til intra- og internettet. I postsystemet er brugeren tildelt en personlig postadresse og tilhørende postkasse. I den udstrækning brugeren er tildelt flere autorisationer, er der også adgang til disse andre systemer.

§ 9. Den enkelte bruger skal overholde følgende regler vedrørende adgangskoden:

1) adgangskoden skal udskiftes efter højst 90 dages brug,
2) længden af adgangskoden skal være mindst 8 tegn, heraf
   - mindst 1 stort bogstav
   - mindst 1 lille bogstav
   - mindst 1 ciffer (tal),
3) brugerens egne navne må ikke indgå i adgangskoden,
4) adgangskoden kan ikke genbruges ved de næste tre skift, og

5) adgangskoden skal ændres, hvis den kan være blevet kendt af andre.

Stk. 2. Den enkelte bruger har sin egen autorisation. To eller flere medarbejdere må ikke dele autorisation.

Stk. 3. Autorisationen vil blive spærret efter et antal mislykkede forsøg på at indtaste den rigtige adgangskode. Koder, der er blevet spærret eller glemt, vil først kunne benyttes efter henvendelse til IT-Kontorets Brugerservice. Hvis Brugerservice ikke ved tilbageringning eller på anden måde kan skabe vished for, at det er den rigtige person, der anmoder om at få genåbnet en autorisationskode, kan genåbning kun ske efter skriftlig henvendelse.

§ 10. Ved arbejdet med systemerne må brugeren ved søgninger og opslag alene skaffe sig adgang til oplysninger, som er nødvendige for at kunne udføre pålagte funktioner og opgaver, dvs. oplysninger, som naturligt indgår i sagsbehandlingen/opgaveløsningen.
Adgang til og anvendelse af Internettet er dog ikke underlagt denne begrænsning.

Stk. 2. Det er tilladt at anvende e-post og Internet til private, ikke-kommercielle formål.

Stk. 3. Såfremt en bruger bliver opmærksom på, at han/hun eller andre har adgang til systemer og/ eller oplysninger, som er mere vidtgående, end vedkommende er autoriseret til, skal han/hun straks underrette den lokale sikkerhedsansvarlige eller IT-Kontoret.

§ 11. Enhver anvendelse af Personregistrering (Den elektroniske Kirkebog) og/ eller CPR-systemet til privat brug er strengt forbudt.

Stk. 2. Alle forespørgsler og databehandlinger i Personregistrering (Den elektroniske Kirkebog) og/ eller CPR-systemerne registreres på den enkelte persons autorisation. Denne registrering danner grundlag for udskrift i tilfælde, hvor der er mistanke om misbrug.

De sikkerhedsansvarliges kontrol af brugen af udstyr og programmer

§ 12. For den daglige brug af udstyr og programmer, herunder hvilket udstyr, der må tilsluttes Kirkenettet, gælder bilag 4: »Vejledning og retningslinjer for brug af programmer og udstyr i Kirkenettet«.

Stk. 2. Det indskærpes særligt, at de sikkerhedsansvarlige skal føre tilsyn med, at der:

- ikke sker uautoriseret indgreb i det installerede udstyr
- kun tilkobles udstyr, der er godkendt til brug i Kirkenettet
- ikke tilkobles ekstraudstyr, der kræver fysisk indgriben i installeret udstyr
- kun installeres programmer, hvortil der er erhvervet licens.

Stk. 3. De sikkerhedsansvarlige skal sikre, at de rutiner, der er fastsat for sikkerhedskopiering, bliver fulgt, herunder at eksterne lagringsmedier (tapes/bånd, cd-rom m.m.) opbevares under lås.

Stk. 4. Ved mistanke om misbrug kan de sikkerhedsansvarlige hos IT-Kontoret rekvirere en benyttelsesstatistik fra DNK systemet, der for et brugernavn angiver, hvilke transaktionstyper der har været anvendt, og antallet af gange den enkelte type har været anvendt.

Stk. 5. For edb-installationerne i Kirkeministeriet, stiftsøvrighederne og i IT-Kontoret gælder særlige regler for edb-installationernes udførelse og sikring samt for sikkerhedskopieringen, der er nævnt i Bilag 5.

Stk. 6 Det på kirkenettet godkendt udstyr må ikke tilkobles andre net end kirkenettet.

Opgaver og regler for IT-Kontoret og dets medarbejdere

§ 13. IT-kontoret, der er driftsansvarlig for Kirkenettet, skal have etableret faste arbejdsrutiner til sikring af, at de fornødne sikkerhedsforanstaltninger er implementeret og er virksomme.

Stk. 2. Det skal sikres, at ingen pc kan tilkobles Kirkenettet uden aktivering af programmer, der overvåger og eventuelt installerer nødvendige opdateringer til virusbeskyttelse og andre komponenter, der har betydning for datasikkerheden og som sikkerhed imod uvedkommendes misbrug af oplysninger.

Stk. 3. Efter nærmere fastsatte intervaller opsamles tekniske informationer, der bruges til:

– kontrol af uautoriserede indlogningsforsøg
– deaktivering af autorisationskoder, der ikke har været brugt i 6 måneder
– overvågning af, at der ikke installeres modems
– kontrol af, at pc'er og servere er installeret med de rigtige programversioner.

§ 14. Medarbejderne i IT-Kontoret og hos leverandører til Kirkeministeriet har tavshedspligt med hensyn til oplysninger de i den forbindelse kommer i besiddelse af. Det gælder både i deres opfyldelse af nærværende kontrol- og sikkerhedsforanstaltninger og i deres hjælp til brugerne igennem Brugerservice.

Stk. 2. Der er forbudt at skaffe sig adgang til brugeres arkivområder, dokumenter, postkasser og lignende. Undtaget er dog tilfælde, hvor dette sker efter udtrykkelig aftale med den pågældende bruger, og da alene med det formål at bistå brugeren i tekniske spørgsmål.

Stk. 3. Der er forbudt at registrere brugernes adfærd på Internettet, herunder forsøge at skaffe sig oplysning om hvilke adresser en bruger benytter. Dette gælder også vedrørende en brugers e-post trafik.

Stk. 4. Såfremt afhjælpning af et teknisk problem afhænger af, at IT-Kontoret eller en leverandør får adgang til informationer om hvilke Internet og/eller e-postadresser en bruger korresponderer med, skal IT-Kontorets chef først give tilladelse hertil. De adresseinformationer, der derved opnås adgang til, skal behandles fortroligt.

§ 15. Der skal regelmæssigt gennemføres kontrol af, at de implementerede sikkerhedsforanstaltninger virker.

Stk. 2. Beredskabsøvelserne skal gennemføres under realistiske forhold. Mindst én gang årligt skal det uvarslet:

– af en uvildig instans efterprøves om Kirkenettet har den fornødne sikkerhed mod uautoriseret indtrængen
– konstateres om data og systemer kan genskabes på grundlag af foretagne sikkerhedskopieringer.

§ 16. Mindst én gang årligt skal der foretages en gennemgang af sikkerhedsbestemmelserne med henblik på at sikre, at de er fyldestgørende og afspejler de faktiske forhold i og omkring Kirkenettet.

§ 17. Cirkulæret træder i kraft straks.

Stk. 2. Samtidig ophæves Kirkeministeriets cirkulære af 8. december 2006 om sikkerhedsforanstaltninger i Kirkenettet.

Kirkeministeriet, den 4. november 2007

STEFFEN BRUNÉS
AFDELINGSCHEF

/ Torben Stærgaard
IT-chef