God brug af e-post

- en vejledning

Ministeriet for Videnskab
Teknologi og Udvikling

>

God brug af e-post
- en vejledning

Udgivet af:
Videnskabsministeriet

Ministeriet for Videnskab,
Teknologi og Udvikling
Bredgade 43
1260 København K

Telefon: 3392 9700
Fax: 3332 3501

Publikationen udleveres gratis
så længe lager haves, ved
henvendelse til:

IT- og Telestyrelsen.
danmark.dk
Telefon: 1881
sp@itst.dk
www.netboghandel.dk

Publikationen kan også hentes
på Videnskabsministeriets
hjemmeside: http://www.vtu.dk
ISBN (internet): 87-91469-93-7

Tryk:
Grefta Tryk A/S
Oplag: 3.000
ISBN: 87-91469-92-9

>

God brug af e-post
- en vejledning

Ministeriet for Videnskab, Teknologi og Udvikling
Juni 2005

Indhold >

1	**Indledning**	**5**
2	**God brug af e-post**	**7**
	2.1 E-post - fordele og særlige kendetegn	7
	2.2 God opførsel / ”netikette” for brug af e-post	7
	2.3 Hvad sendes til hvem?	10
	2.4 Anvendelse af modtaget e-post	12
	2.5 Her skal e-post ikke bruges	15
	2.6 E-post og den daglige arbejdssituation	17
3	**E-post og formel sagsbehandling.**	**20**
	3.1 Henvendelser på e-post	20
	3.2 Udvekslingsformater	21
	3.3 Forskellige e-post-kasser	22
	3.4 Sagsdannelse	23
	3.5 Ministerpost	24
	3.6 E-post og juridisk bindende afgørelser	24
4	**Sikker e-post**	**26**
	4.1 Autenticitet og ægthed af e-post-meddelelser	26
	4.2 Integritet af en e-post-meddelelse	27
	4.3 Uafviselighed – e-post er afsendt og modtaget	27
	4.4 Fortrolighed i e-post-meddelelser – kryptering	28
	4.5 Særlige forhold vedr. digital signatur	29
5	**Andre forhold omkring sikkerhed**	**32**
	5.1 Beskyttelse mod hacker- og virusangreb	32
6	**Personlig e-post**	**33**
	6.1 Privat e-post	33
	6.2 Beskyttelse af privat e-post	34
	6.3 Adgang til medarbejders e-post-kasse	35
	6.4 Misbrug af den personlige e-post-kasse	36
7	**Andre forhold**	**37**
	7.1 E-post og bindende aftaler	37
	7.2 Kopiering og logning	38
	7.3 Ophør af ansættelse	39
8	**Teknik**	**41**
	8.1 E-post-adresser	41
	8.2 Nationale tegn – æ, ø og å	42
9	**Bilag**	**43**

1 Indledning

>

E-post har gennem de seneste 10 år udviklet sig til at blive et kommunikationsværktøj, som anvendes overalt i samfundet. E-post har i stort omfang erstattet traditionel brevpost mellem private, ligesom henvendelser både til virksomheder og offentlige myndigheder sker ved anvendelse af e-post.

Internt i den offentlige sektor og i de fleste virksomheder har e-post effektiviseret og forbedret den interne kommunikation. Også eksternt understøtter e-post effektivitet og samarbejde gennem hurtig kommunikation uafhængig af tid og sted såvel nationalt som internationalt.

Senest har eDag og eDag2 initiativerne understøttet udbredelsen af elektronisk kommunikation både internt i den offentlige sektor og i forhold til borgere og virksomheder.

Udviklingen i anvendelsen af e-post betyder, at e-post er blevet en vigtig faktor i den enkelte medarbejders daglige arbejdssituation og arbejdsbelastning. En udvikling, der kræver, at enhver organisation fastlægger hensigtsmæssige rammer for organisationens brug af e-post.

Denne vejledning, "God brug af e-post", er en opdatering af tidligere vejledninger fra Forskningsministeriet og fra IT-Sikkerhedsrådet. Vejledningen er udarbejdet af en arbejdsgruppe under Statens it-råd med deltagelse fra en række ministerier og bygger således på de erfaringer, staten hidtil har gjort sig med brug af e-post.

Vejledningen fokuserer primært på "traditionel" e-post og beskriver ikke nye kommunikationsteknologier som SMS, Instant Messaging, videokonference mellem arbejdspladser og samarbejde via nettet.

Målgruppen for vejledningen er sekretariatschefer eller andre, som i den enkelte offentlige organisation har ansvaret for håndtering af e-post i organisationen, herunder opgaven med at formulere en politik for organisationens brug af e-post.

>

Det er forventningen, at vejledningen også kan inspirere private organisationer ved udarbejdelse af interne retningsliner for organisationens anvendelse af e-post.

2 God brug af e-post

>

2.1 E-post - fordele og særlige kendetegn

Meddelelser

E-post giver mulighed for hurtig og effektiv skriftlig elektronisk kommunikation med stor fleksibilitet og høj kvalitet. E-post er velegnet til udveksling af meddelelser (noter) og opleves som mindre formel end egentlig brevkommunikation.

E-post er også effektiv til ”én til mange” kommunikation, hvor den samme meddelelse let kan sendes til mange modtagere.

Dokumenter og datafiler

Dokumenter og datafiler (data, grafik, billeder eller lyd) kan vedhæftes en e-post-meddelelse. Hos modtageren kan tekst eller data gemmes, redigeres og anvendes i andre sammenhænge.

> **E-post er velegnet både til uformel kommunikation med udveksling af korte meddelelser og til mere formel kommunikation med udveksling af dokumenter og data.**

Internationalt

Internationalt samarbejde smidiggøres gennem hurtig udveksling af e-post uafhængig af tid og sted. Forskellen i tidszoner muliggør, at det samme materiale kan gennemgå en række arbejdsprocesser i løbet af et døgns 24 timer

2.2 God opførsel / ”netikette” for brug af e-post

E-post er et supplement til men også en blanding af andre kommunikationsformer: brev, fax og telefon. Overholdelse af nogle få spilleregler vil bidrage til en "god kommunikation”.

Emnefelt

Emnefeltet anvendes til at give en "overskrift" på e-posten. Teksten bør være kort og beskrive indholdet, således at modtageren let kan orientere sig og sortere sin post. Emnefeltet må ikke indeholde personrelateret information, da indholdet ikke kan krypteres.

Meddelelsesfeltet

Traditionelt bruges meddelelsesfeltet til at skrive korte ikke-formaterede meddelelser. Ofte skrives disse meddelelser ud fra holdningen ”hurtigt skrevet - hurtigt læst”.

En række organisationer har udviklet interne procedurer, hvor man bruger meddelelsesfeltet også til mere formelle dokumenter. Det kan være notater fra møder, indberetninger om sagsforløb eller tilsvarende materiale. Fordelen er, at man sparer arbejdsgange i forhold til at skrive og sende teksten som vedhæftet dokument.

Fra e-post til sagsakt

Den videre udvikling på dette område vil blive tæt integration mellem sagsbehandlingssystemerne og e-post-systemet. Som led i sagsbehandlingen skabes de nødvendige e-post-meddelelser med adresse, information i emnefeltet og med det egentlige indhold i meddelelsesfeltet.

Format

De forskellige typer af indhold i meddelelsesfeltet stiller forskellige krav til, hvorledes indholdet kan formateres og præsenteres. For at bevare e-postens fleksibilitet er det vigtigt, at indholdet uanset forudgående behandling præsenteres i et format, der kan læses af modtageren.

> **Teksten i meddelelsesfeltet skal fremsendes i et format, der umiddelbart kan læses i de fleste e-post-systemer.**

Almindelig tekst er et åbent format, som understøttes af alle e-post-systemer. Dets begrænsninger ligger i de manglende muligheder for at formatere indholdet.

HTML-mail er et relevant format, hvis man ønsker at formatere tekst og data i meddelelsesfeltet. E-post-systemer kan ofte specificeres til automatisk at medsende ren tekst som alternativ, da ikke alle e-post-systemer understøtter HTML-mail.

Mere information i OIO-kataloget: www.oio.dk

Form

Normalt læses e-post direkte på skærmen. Teksten bør derfor skrives i en kort og præcis form. Man bør være opmærksom på, at en e-post-meddelelse skriftligt fastholder et udsagn mere entydigt end for eksempel et referat af en telefonsamtale. Man bør ligeledes være opmærksom på, at e-post let kan sendes videre til andre end den oprindelige kreds af modtagere.

>

Grafik eller videosekvenser i meddelelsesfeltet bør undgås, da e-post af den karakter ofte vil være vanskelig at håndtere for modtageren og optage megen plads i indbakken.

> **Officiel e-post bør anvende den samme sprogstil, som gælder for papirpost, men brug korte direkte sætninger.**

Vedhæftede filer

E-post kan være brevbærer for vedhæftede dokumenter eller datafiler.

Man bør sikre sig, at dokumenter eller data vedhæftes i et format, som modtageren kan læse. (Jf. afsnit 3.2).

> **Afsender af e-post med vedhæftede dokumenter eller data skal sikre sig, at der anvendes et format, der kan læses af modtageren.**

Det anbefales generelt at afsender og modtager bliver enige om, hvilket udvekslingsformat, man vil anvende.

Et relevant alternativ til udveksling af dokumenter er dokumentformatet PDF (Portable Document Format). PDF er udviklet af firmaet Adobe, og er et ophavsretligt beskyttet (men royalty frit) format, som er meget udbredt og understøttet.

PDF kan anvendes til publicering af dokumenter - tekst, såvel som regneark - når der er tale om dokumenter, der alene skal kunne læses, men ikke redigeres.

Det er afsenderen, der har ansvar for kvalitetssikring af dokumentet, hvilket gør PDF-formatet attraktivt, da det kan bruges til at "lukke" versionen af dokumentet.

Mere information: Om eDag på www.e.gov.dk

Afsender

E-post systemer har normalt faciliteter til automatisk at indsætte en afsenderidentifikation, for eksempel i slutningen af en meddelelse. Sender man e-post til udlandet bør disse informationer skrives på for eksempel engelsk.

>

Afsenderidentifikation i en e-post meddelelse bør begrænses til nogle få linier med følgende information:
<Navn> - <Titel>
<Organisationens navn> - <Fysisk postadresse> - <CVR nr.>
<Telefonnummer> - <Evt. direkte lokalnr.>
<E-post-adresse> - <Evt. adresse på hjemmeside>

> **En e-post skal altid indeholde identifikation af afsenderen.**

Som en konsekvens af den øgede anvendelse af e-post også til formel sagsbehandling vælger mange organisationer automatisk at påføre enhver afsendt e-post-meddelelse afsenderidentifikation.

Anvendelse af grafisk logo, videoklip og tilsvarende bør undgås, da denne type data både er pladskrævende og kan give problemer i de elektroniske arkivsystemer.

Skjult information

En række tekstbehandlingssystemer gemmer rettelser og eventuelt information om, hvem der har foretaget disse rettelser. Desuden gemmes andre informationer, for eksempel hvem der har oprettet et dokument. For at sikre at sådanne informationer ikke spredes utilsigtet, bør teksten fra den endelige udgave af et dokument med følsomme informationer kopieres over i et nyt dokument. Alternativt kan dokumentet distribueres i et neutralt format, for eksempel PDF.

> **Ved ekstern udsendelse bør et dokument være renset for "historik" i form af skjult information.**

2.3 Hvad sendes til hvem?

Når en meddelelse foreligger i elektronisk form, kan den hurtigt og let sendes som e-post til en eller flere modtagere.

Muligheden for at benytte adresselister med et stort antal modtagere kan indbyde til at sende den samme e-post til mange

modtagere. Denne mulighed bør dog bruges med omtanke, da det for de fleste modtagere er irriterende at modtage e-post med ikke-relevant indhold. Samtidig øges risikoen for, at modtageren ikke kan nå at læse og besvare de relevante henvendelser.

> **Det er afsenders pligt, at en e-post kun sendes til relevante modtagere og ikke til flere end nødvendigt.**

Cc:

E-post til flere modtagere kan sendes til en eller flere hoved-modtagere. Desuden kan e-post sendes som kopi til orientering for andre modtagere (Cc:-modtagere). Der kan på denne måde skelnes mellem personer, der forventes at tage aktivt del for eksempel i et videre sagsforløb, og personer, der blot skal holdes orienteret.

> **Det bør normalt fremgå af en e-post, hvem der er modtagere enten i adressefeltet eller i selve meddelelsen.**

Med mindre det er aftalt, kan man ikke forvente, at man opfylder en forpligtigelse til at informere for eksempel chef eller kolleger blot ved at sende e-post Cc: til disse personer.

Bcc:

Mange e-post-systemer giver mulighed for at sende en ”skjult kopi” til modtagere (Bcc:-modtagere), uden at dette kan ses hos de øvrige modtagere. Det kan være relevant at benytte dette felt i særlige tilfælde, for eksempel hvor persondataloven forbyder, at de enkelte modtagere får kendskab til hinanden.

Formidling af information

Erfaringen viser, at det er vigtigt, at en organisation formulerer en relativ restriktiv politik for brug af e-post til generel information i organisationen. Således bør e-post ”til alle” begrænses til helt specifikke formål.

> **Der bør fastlægges en politik for formidling af information internt og eksternt.**

Interne og eksterne hjemmesider er relevante alternativer til formidling af generel information via e-post, eventuelt suppleret med en kort e-post til den relevante kreds af interessenter med oplysning om tilstedeværelsen af den pågældende information.

E-post og markedsføring

Anvendes e-post til ekstern formidling af information, der kan have karakter af markedsføring, skal man være opmærksom på, at der med udgangspunkt i et EU-direktiv gælder særlige regler på dette område.

Grundregler for lovlig markedsføring via e-post:

> Markedsføring via e-post er kun tilladt med modtagernes forudgående samtykke. En begrænset undtagelse gælder for e-post, der sendes til eksisterende kunder og vedrører samme produkter eller tilsvarende tjenesteydelser.
> Det er ulovligt at sløre eller skjule identiteten af den afsender, på hvis vegne meddelelsen sendes.
> Al e-post skal indeholde en returadresse, som modtageren kan henvende sig til for at få standset sådanne henvendelser.

(EU-direktiv om databeskyttelse inden for elektronisk kommunikation)

Mere information: www.forbrug.dk

Ved ekstern formidling af information skal man være opmærksom på, at man ikke ved en fejl kommer til at sende informationen til en større kreds af modtagere end planlagt. Der er eksempler på, at svigt i teknik eller manglende styring af adresselister har medført masseudsendelse af e-post, der var i strid med reglerne for lovlig markedsføring via e-post.

2.4 Anvendelse af modtaget e-post

Læse e-post

De fleste organisationer vil udover personlige e-post-kasser til medarbejderne etablere en officiel e-post-kasse og eventuelt kontor-/funktionspostkasser.

Organisationen skal fastlægge arbejdsgange for tømning af den officielle e-post-kasse og af kontor-/funktionspostkasser.

> **Der bør fastlægges procedurer for behandling af e-post modtaget i den officielle postkasse eller i en funktionspostkasse.**

Identifikation af afsender

Det vil ofte være vanskeligt at identificere en person alene udfra en kort e-post-adresse. I tvivlstilfælde bør man derfor sende en forespørgsel og bede om yderligere identifikation af afsenderen.

> **Før man behandler en e-post, bør man sikre sig fuld information om afsenderens identitet.**

Kvittering

Sagsbehandlingstiden ved henvendelser via e-post bør ikke være anderledes end for tilsvarende henvendelser via papirbaseret post. Alligevel bør der etableres rutiner, som udnytter e-postens mulighed for at give et hurtigt tilbagesvar med en kvittering for den modtagne post. Hvis muligt bør kvitteringen kort relatere sig til henvendelsens indhold og videre behandling i organisationen.

> **Der bør etableres procedurer til kvittering for modtaget e-post.**

Autosvar

E-post-systemerne giver mulighed for, at modtaget e-post umiddelbart kan besvares ved modtagelsen med en automatisk genereret meddelelse, et såkaldt "autosvar".

Det bør altid fremgå af autosvar-meddelelser, at der er tale om automatisk genererede meddelelser, så man ikke får opfattelsen af, at henvendelsen er besvaret af en person.

Autosvar-faciliteten kan være nyttig i visse sammenhænge for eksempel ved ferielukning, adresseskift eller nedlæggelse af e-post-kasser. Et autosvar bør ikke indeholde information om personlige forhold, for eksempel langtidssygemelding, men blot angive information om alternativ mulighed for kontakt.

Anvendelse af autosvar som kvittering for modtagelse af e-post vil normalt ikke være hensigtsmæssig, da det blot er en kvittering for den tekniske modtagelse.

Man bør også være opmærksom på, at autosvar kan føre til misforståelser og unødig trafik, for eksempel hvis autosvar igen genererer et retur-autosvar og så videre.

> **Brugen af autosvar-faciliteten bør begrænses til særlige tilfælde, hvor autosvar er relevant.**

Sende videre

Det er nemt at videresende modtaget e-post. Dette kan bruges til at effektivisere den direkte sagsgang, ligesom det kan være en effektiv måde til at inddrage andre i en vurdering/dialog eller til at holde andre orienteret.

Hvis der er rettet i en meddelelse, der sendes videre, bør det fremgå hvad og hvem, der har foretaget rettelsen.

> **Når en meddelelse videresendes med tilføjelse af egen tekst, skal det ske på en sådan måde, at modtageren kan se, hvem der har forfattet tekstens dele.**

Svarpost

Svarfunktionen i e-post gør det let at sende et svar til den korrekte adresse. Hvis en e-post har mange kopi-modtagere, bør man overveje meget nøje, om det er relevant, at alle modtager kopi af svaret.

I forbindelse med funktionspostkasser skal man være opmærksom på, at den oprindelige afsender-adresse kan gå tabt i forbindelse med videresendelse af e-posten internt i organisationen. Dette kan eventuelt løses ved, at den oprindelige e-post fremsendes som bilag i en ny e-post.

Original-meddelelse i svar

E-post-systemerne kan normalt indstilles til at medtage den oprindelige meddelelse i et retursvar. Man får derved muligheden for at genbruge hele eller dele af den oprindelige tekst og for at føje svar ind direkte på relevante steder i den

modtagne tekst. Hvis der er behov for det, giver gentagelserne mulighed for at følge og dokumentere et sagsforløb. For at undgå udveksling af unødvendigt store datamængder vil man ofte slette den modtagne tekst i svaret.

> **Overvej om det er nødvendigt at bibeholde hele den modtagne tekst, når en e-post besvares.**

2.5 Her skal e-post ikke bruges

Uanset at e-post er et effektivt værktøj til intern og ekstern kommunikation, så er der en række situationer, hvor brug af e-post vil være uhensigtsmæssig.

Tidskritisk information

E-post er uegnet til formidling af tidskritisk information, med mindre man har haft forudgående kontakt. Man bør således ikke indkalde til møde med kort varsel via e-post eller fremsende mødemateriale umiddelbart forud for et møde.

Omvendt kan e-post også være et effektivt værktøj i tidskritiske situationer, hvis de involverede parter er enige herom. Risikoen for teknisk systemsvigt bør dog altid inddrages, når håndteringen af opgaver, der er tidskritiske, planlægges.

> **Tidskritisk information bør kun formidles via e-post efter forudgående aftale.**

Store datafiler

Den tekniske udvikling betyder, at de fleste e-post-systemer råder over stadig større kapacitet til at håndtere store datamængder. Alligevel kan den enkelte bruger opleve begrænsninger både i plads til lagring af store datafiler og i kapacitet til dataoverførsel i kommunikationssystemerne. Fremsendelse af store dokumenter, grafik eller billeder bør derfor kun ske efter aftale, således at man undgår, at modtagerens e-post-system bliver blokeret.

> **Store datafiler bør kun sendes med e-post efter aftale med modtageren.**

Hvis man ofte har behov for at udveksle store datafiler, kan man overveje at anskaffe et særligt program, der kan "pakke" en datafil, således at den fylder mindre. Det kræver dog, at modtageren har et tilsvarende program til "udpakning" af filen.

Fortrolig/følsom information

Fortrolig eller følsom information herunder følsomme personoplysninger må kun sendes via e-post, hvis man kan kryptere meddelelsen eller eventuelt anvende særligt sikrede net. Kryptering kan ske ved brug af digital signatur (jf. afsnit 4).

> **Fortrolig og følsom information skal krypteres, hvis den sendes via e-post.**

Datatilsynet fører tilsyn med enhver behandling, der er omfattet af lov om behandling af personoplysninger.

Datatilsynets hjemmeside indeholder under afsnittet "Værd at vide" en række afgørelser og praktiske anvisninger om korrekt behandling af følsomme personoplysninger.

Mere information: www.datatilsynet.dk

Ubehagelig information

Information, som modtageren vil opfatte som ubehagelig, for eksempel en meddelelse til en medarbejder om opsigelse, bør ikke kommunikeres via e-post. Her er den direkte dialog nødvendig.

Ligeledes bør kommunikation, der kan involvere stærke følelser, for eksempel vrede, ikke formidles via e-post. Dels er der risiko for, at de skriftlige udtryk misforstås. Dels medfører e-postens hurtige kommunikation en øget risiko for, at der "siges" ting, der senere fortrydes.

> **Ubehagelig information bør ikke formidles via e-post.**

Spam

Spam er en væsentlig kilde til forurening på internettet. Den enkelte e-post-bruger bør derfor aldrig reagere på en spam-meddelelse, men slette den direkte uden at åbne den.

Spam vil ofte være karakteriseret af en mangelfuld eller for modtageren helt ukendt afsenderadresse, samt af irrelevant eller mangelfuld information i emnefeltet.

> **Undlad at læse og besvare spam.**

Bekæmpelse af spam er en international sag, da de fleste spam meddelelser har sin oprindelse udenfor Danmark. De fleste professionelle e-post-systemer beskyttes af spam-filtre, som fjerner kendte spam-meddelelser.

I Danmark er det forbudt at sende e-post-meddelelser, der har karakter af spam.

E-post uden reelt indhold

Den lette og billige adgang til at sende e-post betyder, at e-post bruges til mange for modtageren irrelevante formål, for eksempel reklamer, meddelelser med generelle budskaber, meddelelser uden reelt indhold eller meddelelser, der alene tjener til "chikane" af modtageren. Organisationen bør fastlægge retningslinier for behandlingen af denne type af e-post.

> **Der bør opstilles retningslinier for behandlingen af modtagen e-post uden reelt indhold.**

2.6 E-post og den daglige arbejdssituation

Organisering og adgang

Den øgede anvendelse af e-post gør det nødvendigt, at brugen af e-post organiseres som led i den daglige arbejdsplanlægning.

Hvis man ikke anvender funktionspostkasser (jf. afsnit 3.3), kan det i en række arbejdssituationer være hensigtsmæssigt at give en kollega læseadgang til e-post-kassens indbakke. Herved kan man opnå en fleksibilitet, hvis flere arbejder indenfor samme opgaveportefølje, eller hvis den enkelte er fraværende på grund af sygdom eller ferie.

Et alternativ, som ofte bruges af chefer, er, at sekretæren modtager kopi af chefens indgående e-post. Denne løsning kan suppleres med opsætning af regler for videresendelse af kopi. For eksempel at post ikke sendes videre, hvis der står ”privat” i emnefeltet.

Sluk for lyd

Brug af markante lydsignaler ved ny post bør undgås, da det kan virke forstyrrende i arbejdssituationen.

Ryd op i din e-post

Erfaringen viser, at mange e-post-brugere anvender indbakker og udbakker som et personligt arkiv. For materiale, der ikke skal arkiveres som led i sagsbehandlingen, og som kun skal gemmes i en begrænset periode, kan det være hensigtsmæssigt. Skal materiale gemmes i længere tid, bør man anvende andre former for elektronisk arkiv.

Generelt anbefales det, at man systematisk sletter e-post fra indbakke og udbakke, når e-posten er læst, sendt og arkiveret.

> **Ryd op i din e-post og slet ”gamle” meddelelser.**

Man kan desuden overveje at indføre en fast og kendt procedure, hvor den nødvendige sletning foretages automatisk.

Det følger af persondataloven, at e-post, der indeholder personoplysninger skal slettes, når de har opfyldt deres formål. Dette skal ske senest efter 30 dage.

I det omfang, der er behov for at gemme e-post med fortrolige/ følsomme personoplysninger, skal de overføres til et system, der opfylder særlige krav til adgangskontrol og logning.

Papirkurv

De fleste e-post-systemer anvender en papirkurv, hvor slettet post lagres i en periode. Det betyder, at e-post, der er slettet ved en fejltagelse, ikke går tabt, men kan genfindes så længe e-posten ligger i papirkurven.

Som bruger bør man sikre sig, at systemet indstilles til at tømme papirkurven for eksempel hver dag eller en gang om ugen.

> **Papirkurven i e-post-systemet bør tømmes jævnligt.**

Nogle e-post-systemer gemmer slettet e-post i en periode efter, at posten er slettet fra papirkurven, således at slettet post kan gendannes ved brug af særlige funktioner.

Man skal også være opmærksom på, at der hver nat tages sikkerhedskopier af alle data i e-post-systemet. En e-post vil derfor, uanset at den er slettet fra indbakke eller udbakke, findes i sikkerhedskopien i en lang periode fremover.

Det betyder, at man skal tage særlige forholdsregler, hvis man vil være sikker på, at en e-post bliver endeligt slettet her og nu. I praksis vil det være vanskeligt at få slettet en e-post-meddelelse, der er registreret på en sikkerhedskopi.

Systemadministrator for e-post-systemet vil ofte begrænse den lagerplads, som den enkelte bruger har til rådighed. Det sker dels for at undgå, at de enkelte e-post-kasser ”svulmer op”, og dels for at sikre at sikkerhedskopiering kan afvikles indenfor de givne tidsrammer.

Lås arbejds-pladsen

En administrativ arbejdsplads skal være beskyttet af brugernavn og adgangskode. Det er nødvendigt for at skabe større sikkerhed omkring arbejdspladsen og for at beskytte organisationens data.

Den personlige adgangskode må ikke kendes af andre, og arbejdspladsen skal låses, når den forlades. Herved vanskeliggør man, at andre for eksempel kan sende e-post fra arbejdspladsen.

> **Den personlige adgangskode skal beskyttes, og arbejdspladsen skal låses, når den forlades.**

3 E-post og formel sagsbehandling.

>

3.1 Henvendelser på e-post

E-post-henvendelser

Borgere og virksomheder anvender i stigende omfang e-post ved henvendelse til offentlige myndigheder. Tilsvarende anvendes e-post i den interne kommunikation mellem myndigheder.

eDag giver offentlige myndigheder en generel ret til at kommunikere via e-post eller internettet med andre myndigheder, og der lægges op til, at man herefter kun i undtagelsestilfælde bruger almindelig post.

Efter eDag2 har alle borgere og virksomheder mulighed for via sikker e-post at sende dokumenter med fortrolige og følsomme oplysninger elektronisk til det offentlige. Alle offentlige myndigheder får ret til via sikker e-post at sende fortrolige og følsomme oplysninger, når de kommunikerer med andre myndigheder.

Mere information: Om eDag på www.e.gov.dk

I mange sammenhænge lægger e-post op til hurtig uformel kommunikation, og der vil ofte være en forventning om hurtigt at modtage svar på en henvendelse til en offentlig organisation.

Principielt er der ikke noget, der taler for, at en henvendelse via e-post skal have prioritet over en henvendelse modtaget på anden måde. Henvendelser, hvor et svar ikke kræver nærmere undersøgelser, bør dog besvares hurtigt, ligesom muligheden for let og hurtigt at sende en kvittering med supplerende information om forventet sagsbehandlingstid bør udnyttes.

> **Behandlingen af modtaget e-post skal i princippet ikke adskille sig fra behandlingen af papirbaseret post.**

3.2 Udvekslingsformater

Borgere og virksomheder

En borger eller en virksomhed kan ikke forpligtes til at anskaffe særligt teknisk udstyr eller programmel for at kommunikere elektronisk med en offentlig myndighed. Den offentlige myndighed bør råde over udstyr, der kan modtage og læse de mest almindelige dokument- og dataformater på markedet.

En række initiativer arbejder på at få fastlagt åbne dataformater til elektronisk udveksling af for eksempel dokumenter.

> **Henvendelser via e-post bør normalt besvares i et format, der umiddelbart kan læses af modtageren.**

eDag2 anbefalinger om valg af filformater, der skal bruges til kommunikation med andre myndigheder:
Som led i aftalen om eDag2 anbefales følgende retningslinjer for digital udveksling af dokumenter:

> Følsomme dokumenter: Giver afsenders anvendte formater problemer for modtagere, anbefales formatet PDF som fælles udvekslingsformat. Dokumenter kan eventuelt beskyttes yderligere mod redigering efter dekryptering, for eksempel gennem skrivebeskyttelse med kode.

> Færdige officielle dokumenter: Giver afsenders anvendte formater problemer for modtagere, anbefales formatet PDF som fælles udvekslingsformat.

> Arbejdsdokumenter anbefales udsendt i redigerbart format, som begge samarbejdspartnere kan læse. Giver afsenders anvendte formater problemer for modtagere, anbefales formatet PDF som fælles udvekslingsformat

Mere information: eDag2 anbefalinger på www.e.gov.dk

> **PDF** .pdf: Udbredt format til udveksling af dokumenter, der ikke skal redigeres. PDF læseprogram er gratis.

> **MS Word** .doc: En de facto standard, som via sin store udbredelse umiddelbart kan bruges til udveksling af redigerbare dokumenter mellem brugere af MS Word. Vær opmærksom på at ældre udgaver af MS Word ikke kan læse dokumenter skrevet i de nyeste udgaver af MS Word.

> **Rich Text Format** .rtf: Et udbredt format, som kan anvendes i mange systemer. Anbefales til udveksling af redigerbare dokumenter på tværs af forskellige it-systemer

> **OpenOffice.org 1.0 file format** .sxw: Åbent XML-format til OpenOffice.org dokumenter. Formatet anvendes i flere kontorprogrammer.

> **OASIS Open Office XML Format** Open Document: Åbent XML-format til kontorprogrammer.

> **Word Document Markup Language, WDML**: WordML. Åbent XML format for MS Word dokumenter. Alternativt format i MS Word 2003.

En række initiativer arbejder på at skabe et åbent XML baseret udvekslingsformat blandt flest mulige typer af kontorprogrammer.

Mere information i OIO-kataloget: www.oio.dk

3.3 Forskellige e-post-kasser

Officiel/personlig e-post-kasse

Enhver organisation må afhængig af opgaver og typer af sagsbehandling afklare i hvilket omfang, e-post skal kommunikeres gennem organisationens officielle e-post-kasse, gennem funktions-e-post-kasser eller direkte til den enkelte medarbejder.

I situationer, hvor flere medarbejdere skal have mulighed for at have adgang til de samme e-post-meddelelser, kan det være hensigtsmæssigt at anvende en funktionspostkasse.

Organisationens hjemmeside bør gengive organisationens politik på dette område. Desuden bør hjemmeside og brevpapir gengive de relevante e-post-adresser. Hvis hjemmesiden omfatter en oversigt over medarbejderne bør denne oversigt også vise lokalnr. og e-post-adresse.

Ved angivelse af e-post-adressen anbefales det at skrive adressen på en form, der ikke umiddelbart kan identificeres af "robot-søgemaskiner".

> **Organisationen bør fastlægge og offentliggøre en politik for modtagelse af officiel e-post.**

Svar

Den enkelte organisation bør fastlægge, hvorledes sagsgangen skal være for afsendelse af e-post, som er svar på formelle henvendelser. Sendes svaret fra den officielle postkasse eller fra en funktionspostkasse, vil eventuelt tilbagesvar fra modtageren blive sendt hertil.

3.4 Sagsdannelse

Sagsid. i e-post

På samme måde som breve og andre dokumenter i en sag skal påføres sagsnr. eller anden identifikation, skal materiale, der formidles via e-post, også indeholde sagsidentifikation. Kun herved kan der sikres den nødvendige entydighed og sammenhæng i sagsbehandlingen.

> **E-post, der indgår i sagsbehandling, skal indeholde sagsidentifikation.**

Journalisering

Når e-post indgår som led i en sagsbehandling, skal modtaget og afsendt e-post journaliseres, således at e-post-meddelelsen indgår på sagen og i givet fald kan gøres til genstand for aktindsigt i overensstemmelse med offentlighedslov og forvaltningslov.

En organisation bør fastlægge interne forretningsgange, der sikrer, at al sagsrelevant e-post journaliseres i overensstemmelse med reglerne, uanset om e-posten modtages i organisationens officielle e-post-kasse, i en funktionspostkasse eller i medarbejdernes personlige e-post-kasser.

Arkivering af e-post

E-post skal arkiveres på sagen sammen med andet sagsmateriale. Hvis sagsdannelsen er baseret på papirdokumenter udskrives og arkiveres e-post på papir.

E-post, der er krypteret og signeret med digital signatur, gemmes sammen med signaturbeviset (jf. afsnit 4.). Dette gælder, uanset om man har papirarkiv eller anvender elektronisk arkivering.

> **I forbindelse med modtagelse af e-post i en organisations officielle postkasse skal der fastlægges rutiner for journalisering og arkivering.**

3.5 Ministerpost

Ministerpost

Den lette adgang til at sende e-post betyder, at ministeren modtager mange flere henvendelser fra borgere og virksomheder. Der bør fastlægges en intern procedure, der sikrer, at ministeren bliver bekendt med den modtagne e-post, og at der udarbejdes svar i overensstemmelse med henvendelsens karakter.

3.6 E-post og juridisk bindende afgørelser

I forbindelse med eDag2 initiativet er det fastsat, at en offentlig myndighed kan kommunikere elektronisk med borgere og virksomheder.

Det indebærer blandt andet, at en myndighed, der træffer bindende afgørelser i forhold til borgere og virksomheder, kan anvende e-post til at fremsende afgørelserne. Dette kræver blot borgernes/virksomhedernes samtykke hertil.

>

Det antages, at en borger har givet samtykke til digital kommunikation, såfremt borgeren selv har henvendt sig til myndigheden digitalt. I forhold til virksomheder er det tilstrækkeligt, at virksomheden har angivet en e-post-adresse på sit brevpapir, hjemmeside eller lignende.

4 Sikker e-post

>

Sikker elektronisk kommunikation kræver blandt andet følgende forhold opfyldt:

> **Autenticitet**: Det skal være muligt at dokumentere identiteten på de kommunikerende parter.

> **Integritet**: Det må ikke være muligt at ændre meddelelsens indhold under kommunikationen.

> **Uafviselighed**: Parterne må ikke efterfølgende kunne benægte at kommunikationen har fundet sted.

> **Fortrolighed**: Det må ikke under kommunikationen være muligt for andre at få kendskab til meddelelsens indhold.

Indførelsen af den offentlige digitale signatur efter OCES-standarden og eDag2 har skabt grundlaget for standardiserede løsninger og metoder til håndtering af sikker e-post.

I Danmark har Videnskabsministeriet i 2003 efter EU-udbud indgået aftale med TDC som certifikatcenter til udstedelse af OCES-certifikater (Offentlige Certifikater til Elektronisk Service).

Det betyder, at TDC kan udstede de certifikater, der er grundlag for en digital signatur. Og det betyder, at TDC har etableret og driver den infrastruktur, der er en nødvendig forudsætning for, at den digitale signatur kan anvendes i praksis.

Mere information: www.digitalsignatur.dk

4.1 Autenticitet og ægthed af e-post-meddelelser

Falsk afsender

Ligesom med telefonopringninger, telefax'er og almindelig brevpost, er det muligt at forfalske afsender-information i e-post-meddelelser. Medarbejderne i en organisation bør instrueres om, i mistænkelige tilfælde, at verificere ægtheden af en meddelelse.

Signaturbevis

I forbindelse med eDag2 har alle centrale myndigheder indført sikker e-post-løsninger med henblik på at kunne signere

henholdsvis kontrollere signaturen på officiel e-post. Ved kontrollen genereres et signaturbevis, som den enkelte medarbejder skal informeres om og forholde sig til. Det anbefales tillige, at der udarbejdes procedurer for, hvorledes undtagelser, for eksempel e-post med ikke valide signaturer, skal håndteres.

4.2 Integritet af en e-post-meddelelse

Uændret indhold

Både ved udveksling af uformelle informationer og ved udveksling af kritiske dokumenter er det vigtigt, at både afsender og modtager kan have tillid til, at indholdet af det, der modtages, er lig med indholdet af det, der blev afsendt.

De sikre e-post-løsninger, der er implementeret i forbindelse med eDag2, håndterer denne problematik. Ved afsendelse forsynes e-posten med en digital signatur, der blandt andet låser e-postens indhold. Ved modtagelsen af en signeret e-post kan det kontrolleres, om e-posten er blevet ændret undervejs. Desuden genereres et signaturbevis, der er organisationens bevis for, at afsenders identitet er blevet kontrolleret, og at dokumentet ikke er ændret siden, det blev afsendt.

4.3 Uafviselighed – e-post er afsendt og modtaget

Ved brug af e-post kan man indstille systemerne til at kræve/sende kvittering for modtagelse fra modtagerens system. En sådan kvittering er imidlertid en ”teknisk” kvittering, der ikke dokumenterer, om e-posten er modtaget og læst af modtageren. Tekniske forhold i modtagerens system kan principielt betyde, at en given e-post går tabt.

Modtager-uafviselighed

Det vurderes at være tilstrækkeligt, at en myndighed genererer et signaturbevis ved modtagelsen af signerede og/eller krypterede e-post-meddelelser. Herved kan modtageren dokumentere, hvem der har afsendt e-posten, og at indholdet ikke er ændret.

Afsender-uafviselighed

Afsenders dokumentation for, at e-posten er afsendt og modtaget, kan etableres ved, at modtager returnerer en signeret e-post med kvittering for modtagelse. Også for denne kvitterings-e-post skal der genereres et signaturbevis.

Dokumentation

Supplerende skal det anbefales, at de generelle procedurer for håndtering af e-post er forsvarlige og dokumenterede. Således bør man for al officiel e-post logge tidspunkt for afsendelse og modtagelse.

3. part

Uafviselighed kan styrkes ved at kommunikere via en uafhængig 3. part, der tidsstempler e-posten og gemmer en kopi.

4.4 Fortrolighed i e-post-meddelelser – kryptering

Ligesom med almindelig brevpost kan der i brugen af e-post være behov for at opnå en høj grad af sikkerhed for, at ingen uvedkommende læser indholdet af e-post-meddelelser.

Kryptering

Offentlige myndigheder er forpligtede til at beskytte udvekslingen af fortrolige eller personfølsomme oplysninger over internettet eller andre åbne net. Denne beskyttelse opnås ved at kryptere indholdet af e-posten.

Data, der er sikkerhedsklassificeret til for eksempel ”Tjenstlig brug” eller højere klassificering, kræver også særlig beskyttelse.

Sikker e-post-løsningerne i forbindelse med eDag2 giver mulighed for at opfylde behovet for kryptering. Med digital signatur kan man lægge sin e-post i en ”digital kuvert”. Det sker ved hjælp af kryptering baseret på modtagerens offentlige nøgle knyttet til den digitale signatur. Det betyder, at det kun er modtageren, der ved brug af sin private nøgle kan åbne og læse den krypterede meddelelse.

4.5 Særlige forhold vedr. digital signatur

Der kan udstedes tre forskellige digitale signaturer: Personsignatur, medarbejdersignatur og virksomhedssignatur. Særligt i forbindelse med sikker e-post er det væsentligt at skelne mellem disse tre typer.

Personsignatur

Personcertifikatet udstedes til privatpersoner og kan anvendes som identifikation af borgeren som privatperson. Et "PID" nummer skaber entydig identitet og sammenhæng til data i CPR-registret. I daglig tale bruges betegnelsen personsignatur.

Personsignaturen kan bruges dels til at signere og kryptere e-post, dokumenter og blanketter, dels som log-on-identifikation til web-baserede selvbetjeningsservices på nettet, hvor entydig identifikation af brugeren er nødvendig

Personsignaturen er privat og må ikke anvendes ved løsning af arbejdsrelaterede opgaver.

Medarbejderens personlige e-post-adresse på arbejdspladsen må derfor ikke angives, når medarbejderen som privat person opretter sin personsignatur.

Installation af personsignatur.
Personsignaturen installeres normalt på privat it-udstyr til brug ved signering af privat e-post og som brugeridentifikation ved web-baserede services.

Personsignaturen kan installeres på medarbejderens arbejdsplads-udstyr og på eventuel hjemmearbejdsplads. Signaturen må i denne sammenhæng kun anvendes til private formål men kan ikke anvendes til signering af privat e-post, der sendes gennem medarbejderens arbejdsrelaterede e-post-kasse.

Medarbejder-signatur

Et medarbejdercertifikat identificerer medarbejderen som tilknyttet en given organisation. Et såkaldt "RID" nummer og virksomhedens CVR-nr. skaber entydig sammenhæng mellem medarbejdercertifikat og organisation.

I daglig tale bruges betegnelsen medarbejdersignatur. Når en medarbejder signerer en e-post med sin medarbejdersignatur, kan modtageren verificere, at medarbejderen er knyttet til den pågældende organisation.

Medarbejdersignaturen anvendes til brugeridentifikation ved arbejdsrelaterede web-baserede services og eventuelt til signering af web-blanketter.

Medarbejdersignaturen kan også anvendes til signering og kryptering af e-post. Denne mulighed bør dog kun bruges, hvis særlige forhold gør sig gældende, da krypteret e-post sendt direkte til medarbejderen vil kræve særlig håndtering i organisationens e-post-system.

Blandt andet vil krypteret e-post til den enkelte medarbejder ikke blive checket i den centrale virus-scanning. Der sker ikke en central generering af signaturbevis. Og ved medarbejderens fravær kan modtagen officiel e-post ikke læses af andre i organisationen.

Indtil der findes standardiserede løsninger på disse områder, anbefales det, at afsendelse og modtagelse af signeret og krypteret e-post sker gennem organisationens officielle e-post-kasse.

Det anbefales, at organisationen frasorterer krypteret e-post, der er sendt direkte til en medarbejder, og sender et autosvar til afsenderen, hvor der henvises til organisationens officielle e-post-kasse og den tilknyttede virksomhedssignatur.

Splitcertificat

Der arbejdes p.t. på at muliggøre anvendelsen af såkaldte splitcertifikater, dvs. certifikater, der giver mulighed for signering hos den enkelte medarbejder, men hvor kryptering og dekrypteringen af meddelelsen foregår centralt. Det anbefales at afvente denne løsning, hvis man ønsker at anvende medarbejdersignaturer til signering af e-post.

>

Installation af medarbejdersignatur.
Medarbejdersignatur installeres på medarbejderens it-arbejdsplads. Medarbejdersignaturen kan anvendes som brugeridentifikation ved web-baserede services. Er der behov for at anvende medarbejdersignaturer i forbindelse med e-post, bør der udarbejdes retningslinier for håndtering af e-post krypteret direkte til medarbejderen.
Personsignatur og medarbejdersignatur installeres uafhængigt af hinanden på den samme it-arbejdsplads.

Virksomheds-signatur

Et virksomhedscertifikat identificerer en organisation. Certifikatet indeholder organisationens CVR-nummer og skaber derved sammenhæng til organisationens officielle registrering i det centrale virksomhedsregister.

I daglig tale bruges betegnelsen virksomhedssignatur. Alle organisationer skal have et CVR-nummer og kan få udstedt et virksomhedscertifikat.

Virksomhedssignaturen tilknyttes en organisations officielle e-post-adresse. Officiel e-post til og fra organisationen, der anvender virksomhedssignaturen, skal derfor modtages i og sendes fra den officielle e-post-kasse. De officielle e-post-adresser tilknyttet virksomhedssignaturer er fundamentet for eDag2

Installation af virksomhedssignatur.
Virksomhedssignaturen installeres i tilknytning til organisationens hovedpostkasse og knyttes til organisationens e-post-system.
Gennem supplerende funktioner i e-post-systemet kan alle brugere vælge, om en udgående e-post skal signeres og/eller krypteres før afsendelse.
Virksomhedssignaturen gør det muligt at sende en e-post i en ”officiel, lukket” kuvert.

Signering og kryptering af intern post

Interne netværk i en organisation anses for sikre. Det anbefales derfor, at der ikke anvendes signering og kryptering i forbindelse med intern e-post. Har myndigheden specifikke behov herfor, bør der fastlægges retningslinier for, hvorledes dette skal håndteres.

5 Andre forhold omkring sikkerhed

>

5.1 Beskyttelse mod hacker- og virusangreb

Hacker-angreb

Selve e-post-forbindelsen til omverdenen indebærer en potentiel risiko for hacker-angreb.

> **Definition af sikkerhedsniveau og -løsning samt opsætning og løbende administration af sikkerheden skal varetages af den enkelte organisation.**

Virusrisiko

Der er ingen virusrisiko forbundet med almindelige tekst-meddelelser uden vedhæftede filer/dokumenter. Tekstmeddelelser i HTML-format kan dog indeholde referencer, som, hvis de aktiveres, kan give risiko for virus. Tilsvarende kan HTML-formatet indeholde egentlig kode (oftest JavaScript), der kan forvolde skade.

Vedhæftede filer/dokumenter med eksekverbare funktioner, som modtageren importerer og/eller udfører, giver ligeledes risiko for virus.

> **E-post med eksekverbare funktioner modtaget fra ukendte afsendere bør normalt slettes.**

Sikkerheds-foranstaltninger

De fleste e-post-systemer omfatter i dag faciliteter til automatisk virusscanning af indkommende e-post-meddelelser. Modtages komprimerede (for eksempel zip'ede) eller krypterede filer bør virus-check foretages umiddelbart efter udpakning/ dekryptering. Ofte vil dette ske automatisk gennem et antivirusprogram på arbejdspladsen.

Alle brugere bør orienteres om risikoen for at modtage virusbefængte programmer, og den enkelte medarbejder bør normalt ikke kunne installere "egne" programmer.

> **Der bør fastlægge en politik for anvendelse af programmer modtaget som e-post eller på anden måde via net.**

6 Personlig e-post

>

En it-arbejdsplads i en organisation er en professionel arbejdsplads, som stilles til rådighed for medarbejderne. E-post sendt til en medarbejders postkasse i en organisation må derfor normalt betragtes som e-post til organisationen.

6.1 Privat e-post

Privat e-post

De fleste organisationer accepterer, at medarbejdere i begrænset omfang kan anvende arbejdspladsens faciliteter til private opgaver i tilknytning til arbejdstiden. Medarbejderne vil derfor ofte have en forventning om, at privat brug af e-post og internet i begrænset omfang kan foretages på arbejdspladsen. Etableringen af hjemmearbejdspladser vil naturligt understøtte denne forventning.

For at undgå misforståelser og ubehagelige situationer bør organisationen udarbejde regler for brug af e-post og internet på arbejdspladsen til private formål.

Den private anvendelse må ikke omfatte formål, der kan skade organisationens almindelige omdømme. Det kan for eksempel dreje sig om privat erhvervsmæssig kommunikation, udveksling af anstødeligt indhold, egentlig politisk aktivitet eller udsendelse af reklame eller propagandabudskaber.

I forbindelse med hjemmearbejdspladser skal det desuden klart angives, at for eksempel familiemedlemmer ikke må anvende medarbejderens personlige e-post-kasse.

> **En organisation skal afklare, om og i hvilket omfang organisationens e-post og internet må anvendes privat.**

Afgrænsningen af, hvad der er privat e-post, er ikke en simpel sag.

> E-post mellem læge og medarbejder om tid til konsultation er klart privat og fortrolig, men er det hensigtsmæssigt, at aftalen ikke må træffes fra arbejdspladsen?

> E-post til tillidsrepræsentanten med holdninger til løndrøftelser er helt klart privat fortrolige oplysninger, men er det privat e-post?

> "Small talk" via e-post med kolleger om et emne fra kontormødet. Indholdet er privat, men er det privat e-post?

Der findes i dag en række relevante muligheder for at etablere en e-post-adresse udelukkende til privat brug, for eksempel gennem en web-baseret e-post-service.

Uanset løsning så gælder det, at det er umuligt at undgå, at eksterne vil sende privat e-post til en medarbejders e-post-adresse.

6.2 Beskyttelse af privat e-post

Beskyttelse

Privat e-post bør mærkes "privat" i emnefeltet og medarbejderen bør oprette et bibliotek, som mærkes "privat e-post".

Medarbejdernes personlige e-post-kasse er normalt beskyttet af kombinationen af brugernavn og adgangskode. Det betyder, at den enkelte medarbejders e-post ikke umiddelbart kan læses af andre, med mindre man har givet dem særlig adgang hertil. Enhver medarbejder må dog være opmærksom på, at den systemansvarlige kan skaffe sig adgang til alle systemets e-post-kasser.

Lovgivning om brevhemmelighed (Straffelovens § 263) og afgørelser fra Datatilsynet fastlægger, at det ikke er lovligt at læse medarbejderes private e-post forudsat, at den kan identificeres som privat.

Lovgivningen forhindrer imidlertid ikke, at organisationen og medarbejderne aftaler, at organisationen må læse meddelelser i medarbejderens personlige e-post-kasse. En sådan aftale giver dog ikke ret til læsning af medarbejderens private e-post-meddelelser.

De arbejdsretlige regler peger på, at en eventuel kontrol ikke må være krænkende, diskriminerende eller påføre medarbejderen nævneværdige ulemper. Samtidig peges der på, at kontrollen skal være begrundet i organisationens driftsmæssige forhold.

Offentlige organisationer skal være opmærksom på, at kontrol af denne karakter skal anmeldes til Datatilsynet, jf. afsnit 7.2.

6.3 Adgang til medarbejders e-post-kasse

Adgang til medarbejders e-post-kasse

Ved en medarbejders fravær kan der opstå behov for at skaffe sig adgang til e-post-kassen. Der skal derfor være fastlagt regler for håndtering af denne situation. Reglerne kan for eksempel fastlægge, at den system- eller sikkerhedsansvarlige gennemgår e-post-kassen efter skriftlig anmodning fra medarbejderens nærmeste chef.

Nogle organisationer har fastlagt, at behovet for at åbne en medarbejders e-post-kasse skal forelægges et internt "udvalg", for eksempel sekretariatschefen og en intern juridisk medarbejder eventuelt suppleret med en tillidsrepræsentant.

Opstår der i en organisation mistanke om en medarbejders mulige misbrug af sin personlige e-post-kasse, kan det blive nødvendigt for organisationen at skaffe sig adgang til e-post-kassen.

Organisationens e-post-politik skal klart dokumentere disse forhold, og det skal sikres, at alle medarbejderne er bekendt hermed.

> **En organisation skal informere om i hvilke situationer, der kan være behov for at skaffe sig adgang til en medarbejders e-post-kasse.**

> **Der skal fastlægges procedurer for åbning af og gennemgang af en medarbejders e-post-kasse.**

6.4 Misbrug af den personlige e-post-kasse

Misbrug af e-post

Misbrug af den personlige e-post-kasse kan medføre en advarsel, og kan i alvorlige tilfælde føre til bortvisning af medarbejderen. Det er derfor vigtigt, at både ledelse og medarbejdere er opmærksom på situationer, der kan udvikle sig til misbrug, således at der kan gribes ind inden et eventuelt misbrug bliver kritisk.

> **Misbrug af den personlige e-post-kasse kan medføre advarsel eller bortvisning af medarbejderen.**

7 Andre forhold

>

Erfaringsmæssigt kan der opstå situationer omkring brug af e-post, der kræver både organisationens og medarbejdernes opmærksomhed. Det er også vigtigt, at man kender til blandt andet de juridiske forhold, der sætter rammer for håndteringen af disse situationer.

7.1 E-post og bindende aftaler

Bindende aftaler og e-post

Fordelene ved e-post-kommunikation betyder, at det er nærliggende også at bruge e-post til indgåelse af formelle aftaler. Dette sker i mange organisationer, hvor der dagligt indgås alt lige fra mindre aftaler med begrænset økonomisk betydning til større kontrakter, der kan have væsentlige økonomiske konsekvenser for organisationen.

Fordi e-post er et hurtigt og ofte uformelt værktøj, kan der være en risiko for, at en aftale mellem to parter udgøres af flere enkeltstående e-post-meddelelser, der er udvekslet mellem parterne. Det kan efterfølgende medføre, at der mellem aftaleparterne kan opstå uklarhed eller uenighed om indholdet aftalen, da den eventuelt skal sammenstykkes af flere brudstykker af information. Det indebærer også en risiko for, at der mellem to parter kan opstå uenighed om, hvorvidt der overhovedet er indgået en aftale.

Disse forhold skal holdes for øje ved indgåelse af aftaler via e-post. Man bør derfor som udgangspunkt følge en fremgangsmåde, hvor det samlede aftalegrundlag er samlet i den e-post, hvor aftalen indgås eller sørge for, at der præcist henvises til de tidligere sendte e-post-meddelelser indeholdende den relevante information, der udgør aftalegrundlaget.

Det kan generelt anbefales at benytte digital signatur ved indgåelse af aftaler via e-post, da dette giver en større sikkerhed i forhold til aftaleindgåelsen.

Ved indgåelse af væsentlige aftaler eller ved aftaler af et større økonomisk omfang bør organisationen bruge digital signatur til

både at signere og kryptere den e-post, der benyttes ved aftaleindgåelsen.

Dette sikrer, at aftalens ordlyd efterfølgende kan dokumenteres samt at uvedkommende ikke har mulighed for at opsnappe og læse aftalen.

> **Digital signatur bør anvendes til signering og eventuelt kryptering af e-post, der indebærer indgåelse af formelle aftaler.**

Den enkelte organisation skal være opmærksom på, at de normale forretningsmæssige procedurer knyttet til aftale-indgåelse, stadig følges, selv om aftaler indgås via e-post.

Udvikler en organisation en praksis med indgåelse af aftaler via e-post, skal man være opmærksom på, at det kræver særlig omhu for at undgå, at der opstår misforståelser. For eksempel bør man sikre, at en accept af en aftale ikke sendes til en personlig e-post-kasse, der ikke tømmes på grund af fravær.

7.2 Kopiering og logning

Sikkerhedskopi

For at skabe den nødvendige driftsikkerhed omkring et e-post-system bliver der jævnligt, som regel hver nat, taget en sikkerhedskopi af alle data. Sikkerhedskopien bliver gemt i en periode, hvorefter den bliver slettet.

Sikkerhedskopien bruges normalt kun til tekniske formål, men man bør være opmærksom på, at reglerne om beskyttelse af eventuelt private data overholdes, hvis materialet bruges i anden sammenhæng.

Sikkerhedslog

Organisationer, som har særlige sikkerhedskrav, vil have behov for at logge al e-post med henblik på at gennemføre en sikkerhedskontrol. Der må fastlægges en procedure for læsning af logfiler, idet der for eksempel udtages stikprøver efter varierende udvalgskriterier til gennemsyn af særligt udpegede

medarbejdere. Disse medarbejdere må behandle indholdet af logfilerne fortroligt og kun videregive indholdet efter fastlagte sikkerhedsforskrifter, hvis der er konstateret tilsyneladende uregelmæssigheder. Det kan overvejes, om man skal lade de enkelte brugere ved underskrift erklære sig indforstået med sådanne særlige sikkerhedsregler.

> **En organisation skal informere om formål med og indhold af eventuelle kontrolforanstaltninger.**

Hvis offentlige myndigheder foretager logning, sikkerhedskopiering og læsning af e-post for at føre kontrol med medarbejderne, skal det anmeldes til Datatilsynet. Et tilsvarende krav gælder ikke for private virksomheder.

7.3 Ophør af ansættelse

Ophør af ansættelse

Når en medarbejder forlader en organisation, er det vigtigt, at der findes en række fastlagte procedurer, som sikrer, at blandt andet spærring af adgang til organisationens it-systemer sker på en koordineret og hensigtsmæssig måde. Disse procedurer skal være kendt af medarbejderne.

Hovedreglen i disse procedurer er, at medarbejderens adgang til e-post-kassen spærres senest den dag, ansættelsesforholdet ophører. Ved ophør af arbejdsforholdet tidligere, for eksempel på grund af fritstilling, bør spærringen ske på dette tidspunkt.

I forbindelse med spærringen bør der i en periode svares med et autosvar, der oplyser, at medarbejderen er fratrådt, og at henvendelse bør ske til virksomhedens hovedpostkasse eller til en specifik medarbejder. Det anbefales, at man ikke oplyser medarbejderens fremtidige ansættelsesforhold eller e-post-adresse.

De interne regler bør også specificere, at e-post, der modtages i e-post-kassen, vil blive åbnet, og at eventuel privat e-post vil blive slettet.

>

Med mindre særlige forhold gør sig gældende, bør medarbejderen have mulighed for at få kopi af mapper med privat e-post.

> **Ved ophør af ansættelse skal medarbejderens adgang til e-post-kassen spærres, og e-post-kassen skal forsynes med autosvar om alternativ mulighed for henvendelse.**

8 Teknik

>

8.1 E-post-adresser

En internet e-post-adresse er opbygget som følger:

Brugernavn@organisationsnavn.landekode

E-post-adressen kan udformes i en kort version eller i en lang version:

pbj@vtu.dk

poul.bernt.jensen@videnskabsministeriet.dk

Den korte form er hurtig at skrive og let at kommunikere både på skrift og for eksempel over telefon.

Den lange form dokumenterer navn og organisation uden behov for supplerende information.

For brugernavnet er den korte udgave mest udbredt, idet man anvender det samme brugernavn som log-on-identifikation på it-arbejdspladsen. Brugernavnet registreres i organisationens e-post-system og skal være entydigt i organisationen.

For organisationsnavn vælger de fleste organisationer at registrere både en kort version og en lang version.

Organisationsnavnet skal registreres som domænenavn for at kunne anvendes på internettet.

Når navnet er registreret, kan det anvendes både i forbindelse med e-post og som organisationsnavn på en hjemmesideadresse:

www.organisationsnavn.dk

I Danmark varetager DK-hostmaster registreringen:

www.dk-hostmaster.dk

8.2 Nationale tegn – æ, ø og å

Internettet og de grundlæggende standarder for internettet blev udviklet og fastlagt i USA. Standarderne er derfor præget af blandt andet det engelske sprog og det engelske alfabet. Det har medført, at standarden oprindeligt ikke tog højde for nationale tegn som for eksempel æ, ø og å.

På samme måde gælder, at æ, ø og å normalt kun findes på tastaturer, der sælges i Danmark.

I dag er det muligt at anvende nationale tegn i navne på internettet. Man bør dog meget nøje overveje, om det er hensigtsmæssigt at anvende et navn med for eksempel æ, ø og å.

Skal man kommunikere e-post med udlandet eller bruge navnet på en hjemmeside fra en arbejdsplads i udlandet, bør man undgå nationale tegn i internet-navne. Primært fordi det udenfor Danmark er vanskeligt at finde disse tegn på tastaturet.

9 Bilag

>

(Kopi fra vejledningen "Brug af e-post og internet på arbejdspladsen", IT-Sikkerhedsrådet 2002).

Huskeliste til brug for udarbejdelse af politik for medarbejderes brug af e-post og internet (ikke udtømmende)

I. Privat brug af e-post og internet på arbejdspladsen

1. Må medarbejderne gøre privat brug af e-post og internet?

2. Hvis JA, i hvilket omfang?

3. Hvilke grænser for brugen skal gælde, herunder i forbindelse med hjemmearbejds-pladser?

4. Vurder virksomhedens behov for kontrol med medarbejdernes brug af e-post og internet.

5. Hvis det vurderes, at der er behov for at føre kontrol[1], skal kontrollen da omfatte brug, der fremstår som privat brug?

6. Informer medarbejderne om, at der foretages kontrol af medarbejderens brug af e-post og internet, herunder formål og omfang, og hvordan kontrollen gennemføres.

7. Indhent forhåndssamtykke, hvis kontrollen skal kunne omfatte læsning af privat e-post.

8. Andet

[1] Omfanget af kontrollen skal altid være sagligt begrundet og forfølge en berettiget interesse, for eksempel drifts- og eller sikkerhedsmæssige hensyn eller for at kontrollere, at retningslinjer for anvendelse af e-post og internet overholdes.

>

II. Håndtering af organisationens anvendelse af e-post og internet i øvrigt

1. I hvilket omfang skal fortrolige informationer kunne sendes via e-post?

2. Skal medarbejderen kunne indgå aftaler på vegne af organisationen via e-post og internet?

3. Hvornår bør identiteten af afsenderen af modtagne e-post-meddelelser sikres?

4. Fastsæt eventuelle retningslinjer for
   – sprog, tone og indhold af e-post-meddelelser,
   – hvem e-post bør sendes til,
   – hvornår e-post ikke bør anvendes,
   – signaturregler,
   – anvendelse af autosvar,
   – omgang med filer for at mindske risikoen for virus,
   – tidsfrist for besvarelse af modtaget e-post, herunder e-post til organisationens centrale e-post-adresse.

5. Udarbejd eventuel procedure for behandling af e-post, der sendes til fraværende medarbejdere med angivelse af, om e-posten må åbnes og læses af organisationen.

6. Udarbejd eventuel procedure for journalisering, arkivering og sletning af e-post-meddelelser.

7. Udarbejd procedure for behandling af e-post-meddelelser ved en medarbejders fratræden og død, herunder med retningslinjer for den fratrædende medarbejders ret til at slette og medtage e-post-meddelelser.

8. Beskriv organisationens syn på overtrædelse af e-post- og internetpolitikken og forventelige sanktioner.

9. Andet.

>

>

<

God brug af e-post
- en vejledning

E-post er i dag et vigtigt kommunikationsværktøj, som anvendes overalt i samfundet.

Både i den offentlige sektor og i de fleste private virksomheder bidrager e-post til effektiv og hurtig kommunikation både internt og eksternt.

Vejledningen præsenterer en bred vifte af gode råd og anbefalinger, som bør overvejes, når en organisation skal udarbejde en e-post politik.

Vejledningen, der er en opdatering af tidligere vejledninger på området, er udarbejdet af en arbejdsgruppe under Statens it-råd.