E-postpolicy för företag och organisationer

Sammanställt av Azenna Advox AB

Författare: Stefan Sjödin
Datum: 2002-05-12

Granskare: Jan Blomqvist
Granskningsdatum: 2002-05-14

Adress: Azenna Advox AB
Esplanaden 3e
172 67 Sundbyberg
Telefonnummer: +46 544 90 900
Faxnummer: +46 732 49 72

---

1 Företagets e-postpolicy

E-post har blivit en av de vanligaste kommunikationsformerna mellan företag och dess omvärld. E-post innebär en rad positiva möjligheter men är även förenad med hel del problem. För att hantera ev problem bör varje företag sammanställa en e-postpolicy som klargör hur företagets e-postsystem får användas och ges tillträde till. Företaget ska även tala om för de anställda vilken denna policy är.

Azenna Advox AB har nedan samman ställt ett antal förslag på regler och klausuler som kan användas vid sammaställningen av företagets e-postpolicy.

Den sorts policy som är lättast att upprätthålla och som ger det mest produktiva resultatet är den som respekterar de anställdas privatliv, och som även innehåller ansvarsfulla och genomtänkta procedurer när juridiska eller affärsmässiga skäl leder till att privatlivets helgd måste brytas. Faktum är att blotta existensen av en policy med en tillämpningsprocedur som tar hänsyn till allas intressen i sig självt kan vara det mest värdefulla verktyg man kan skaffa sig mot angrepp mot företagets praxis i olika sammanhang.

Det är bra att inkludera de anställda (liksom tekniska experter, advokater och ledningen) i processen att formulera en företagspolicy i den här frågan. De anställda användarna av systemet kan hjälpa till att identifiera frågeställningarna. Deras engagemang hjälper till att utveckla en sund policy som kan nå allmän acceptans och respekt. Anta inte en policy som det skulle vara svårt att presentera fullt ut för de anställda.

Samtidigt som företagspolicyn formuleras bör man samla in nyckelinformation om företagets e-postsystem: typ och omfattning, vem som har tillgång till vilken sorts data, vilka åtgärder som gjorts för backup och säkerhet, vem som har ansvaret för begäran om tillträde för tredje part och vem som har gjort vad för att bedöma och minimera alla förutsebara risker. Vid införandet av en e-postpolicy bör även säkerställas att antagen policy kan verifieras och kontrolleras att den efterföljs.

Se till att policyn harmonierar med och är inlemmad i de processer som används vid etablerandet och förmedlandet av all annan företagspolicy.

Företagets anställda bör informeras om de regler, risker och etikett som generellt används för e-postkommunikation. De bör påminnas om att e-post är ett skrivet media och bör hanteras med den varsamhet som detta innebär. En speciell varning gäller runt e-post som innehåller negativa, kritiserande eller nedsättande meddelanden. Förslag på förhållningsätt finns hos Internet Society, http://www.isoc.org/ och en skriven specifikation finns hos Internet Engineering Task Force (IETF), RFC1855, Netiquette Guidelines: http://www.ietf.org/rfc/rfc1855.txt

2 Grundläggande regler

2.1 Företagets e-post får inte användas i olagliga eller bedrägliga syften.

De anställda får inte använda företagets e-postsystem i syfte att göra intrång på copyright eller andra rättigheter hos tredje part, att sprida nedsättande, kränkande eller trakasserande meddelanden eller på annat sätt ägna sig åt olagligt eller bedrägligt uppträdande.

2.2 Syften för vilka företagets e-postsystem får användas

Alternativa klausuler för användandet av företagets e-postsystem för personligt bruk.

2.2.1 E-post får endast användas för företagsändamål

Det är aldrig tillåtet att använda företagets e-postsystem för personligt bruk.

2.2.2 E-post får användas för tillfälligt personligt bruk

Det är tillåtet att använda företagets e-postsystem för tillfälligt personligt bruk. Det är inte tillåtet att ägna någon längre tid till det, att använda det för personlig vinning eller på sätt som på annat vis går emot företagets policy när det gäller den anställdes arbetstid och utnyttjande av företagets utrustning.

2.2.2.1 Personlig e-post måste märkas

De anställda måste märka all personlig e-post så att det framgår att e-posten är personlig, eller sända alla personliga meddelanden på ett sätt som tydligt anger att det är ett personligt meddelande. Alla meddelanden som skickas utan någon sådan märkning kommer företaget att betrakta som post skickad å företagets vägnar.
Anställda måste i meddelanden skickade till tredje part använda signaturfiler som tydligt klargör om meddelandet skickats å företagets vägnar eller inte.

2.2.3 E-post får användas för personligt bruk utan begränsningar

Det är tillåtet att använda företagets e-postsystem för personligt bruk.

2.2.3.1 Personlig e-post måste märkas

De anställda måste märka all personlig e-post så att det framgår att e-posten är personlig, eller sända alla personliga meddelanden på ett sätt som tydligt anger att det är ett personligt meddelande. Alla meddelanden som skickas utan någon sådan märkning kommer företaget att betrakta som post skickad å företagets vägnar.
Anställda måste i meddelanden skickade till tredje part använda signaturfiler som tydligt klargör om meddelandet skickats å företagets vägnar eller inte.

3 E-postsäkerhet

3.1 Kommunikation över Internet eller annat publikt nät

Alternativa klausuler för skydd av e-post och internetkommunikation

3.1.1 Skyddad Internet kommunikation

All kommunikation med Internet skall alltid ske indirekt, via brandvägg, via skyddade servrar, eller på annat skyddat sätt. Företagets interna datastruktur skall alltid vara skyddat från insyn och möjlighet till extern kartläggning.

3.1.2 Skyddad Internet kommunikation med endast utgående datatrafik

All kommunikation med Internet skall alltid ske indirekt, via brandvägg, via skyddade servrar, eller på annat skyddat sätt. Företagets brandvägg skall endast tillåta utgående datatrafik, ingen ingående datakommunikation från extern plats är tillåten. Företagets interna datastruktur skall alltid vara skyddat från insyn och möjlighet till extern kartläggning.

3.2 Skydd mot datavirus

All e-post som passerar genom företagets e-postsystem skall viruskontolleras, exekverbara filtyper får ej mottagas utan att de först verifierats hos avsändaren att de ej innehåller datavirus. De anställda får inte använda företagets e-postsystem för att ladda ner programvara om de inte uppfyller etablerade procedurer för kontroll av datorvirus.

3.3 Skydd mot oönskad e-post och ej auktoriserade e-postavsändare.

Företaget kan från tid till annan blockera ej önskvärd e-postkommunikation, från avsändare som sprider oönskad reklam, nedsättande, kränkande eller trakasserande meddelanden eller på annat sätt ägna sig åt olagligt eller bedrägligt uppträdande.

3.4 E-postkryptering

Alternativa klausuler runt e-postkryptering

3.4.1 All e-post som skickas mellan företagens kontor skall krypteras

All e-post som skickas över Internet eller över annat publikt nät mellan företagets olika kontor skall alltid krypteras.
All kommunikation och e-post som skickas mellan företaget och externt beläget anställda skall alltid krypteras.

3.4.2 All e-post som skickas mellan företaget och företagtes affärspartners skall krypteras

All e-post som skickas över Internet eller över annat publikt nät mellan företaget och företagtes viktiga affärspartners skall alltid krypteras.

3.4.3 Personlig kryptering

Har anställda rätt att använda personlig kryptering?

3.4.3.1 All form av personlig e-postkryptering är tillåten

De anställda får kryptera sin e-post och sina filer med valfritt krypteringsprogram.

3.4.3.1 Bara specificerad e-postkryptering är tillåten

De anställda får endast kryptera sin e-post och sina filer med den programvara som företaget har godkänt. Programvaran måste tillåta att företaget behåller en nyckel så att alla krypterade meddelanden kan öppnas. Den skyddsnivå som ges av krypteringen måste kunna begränsas.

3.5 Informationsrättsförbehåll

Anställda måste i meddelanden som skickade till tredje part använda signaturfiler som tydligt klargör att meddelandet som skickats endast avser adresserad mottagare och innehåller konfidentiell information.

4 E-postövervakning, arkivering och e-posttillträde

4.1 Elektronisk övervakning är förbjuden.

All icke-auktoriserat övervakning av företagets meddelandesystem är ej tillåten och betraktas som ett allvarligt brott mot företagets sekretessregler

4.2 Övervakning av företagets e-postkommunikation och e-postsystem

Alternativa klausuler för övervakning av företagets e-postsystm

4.2.1 Ingen systematisk övervakning

Företaget kommer inte att ägna sig åt systematisk övervakning av e-postmeddelanden, de elektroniska arkiv som e-postsystemet skapar eller av andra elektroniska filer som skapats av de anställda.

4.2.2 Övervakning och e-post arkivering är tillåten av företagsskäl

Företaget får av giltiga affärsskäl ägna sig åt övervakning och arkivering av e-postmeddelanden eller andra elektroniska filer som skapats av de anställda, inklusive övervakning av den anställde. Alla anställda måste informeras om all sådan övervakning och måste som anställningsvillkor godkänna all sådan övervakning.

4.2.3 Övervakning och arkivering bara av goda skäl eller av juridisk nödvändighet

Företaget får bara övervaka och arkivera e-postmeddelanden eller andra elektroniska filer skapade av de anställda om det föreligger specifika skäl till detta, eller om det föreligger en juridisk nödvändighet. I sådana fall ska företaget i god ordning klargöra vilka dessa skäl är, samt begränsa övervakningen till sådana handlingar som är rimliga under omständigheterna.

4.3 Tillträde och offentliggörande av e-postmeddelanden

Alternativa klausuler runt tillträde till e-postmeddelanden

4.3.1 Tillträde utan tillstånd kan inte ges utan lagliga skäl

Företaget kommer inte att skaffa sig tillträde till en anställds privata e-postmeddelanden eller filer utan den anställdes tillstånd, såvida det inte finns lagliga skäl eller plikt mot tredje part.

4.3.2 Tillträde eller offentliggörande av goda skäl och under bestämda former

Företaget får tillträde till och kan offentliggöra privata e-postmeddelanden eller filer om det finns goda skäl till detta, förutsatt att det följer bestämda former som är i enlighet med företagets policy. Goda skäl kan vara att skydda systemsäkerheten, uppfylla företagets åligganden, upptäcka olagligheter från de anställdas sida, rätta sig efter juridiska processer eller skydda företagets rättigheter eller egendom. Lämpliga procedurer måste inkludera granskning från företagsledningen för att se till att de anställdas privatliv inte kränks utan goda skäl.

4.3.3 Tillträde eller offentliggörande av affärsskäl av person med ledningsansvar

Personer med ledningsansvar kan ges tillträde till eller kan offentliggöra en anställds privata e-postmeddelanden eller filer av giltiga affärsskäl. De anställda måste informeras om detta och ge sitt tillstånd till det som anställningsvillkor.

Meddelande efter tillträde eller offentliggörande utan den anställdes tillstånd
I de fall då företagets personal ges tillträde till eller offentliggör en anställds privata e-postmeddelanden utan den anställdes tillstånd ska företaget meddela den anställde detta. Meddelandet kan fördröjas för att skydda de intressen för vilka tillträdet företogs.