



2006 UPPHOVSRÄTTS- OCH SÄKERHETSGUIDE FÖR FÖRETAG[®]



representing the
recording industry
worldwide

De ansvariga på ett företag tar stora risker om det finns musik, film eller annat upphovsskyddat material på företagets servrar eller datorer utan korrekta tillstånd.

Den här guiden förklarar vad ni kan göra för att skydda er organisation mot rättsliga påföljder för intrång i upphovsrätten och mot säkerhetsrisker.

INNEHÅLL[©]

- 03 **VILKA ÄR RISKERNA?**
- 04 **HAR ERT FÖRETAG PROBLEM?**
- 05 **VAD KAN ERT FÖRETAG GÖRA?**
- 06 **EXEMPEL PÅ PM**
- 07 **EXEMPEL PÅ POLICY**





VILKA ÄR RISKERNA? ©

JURIDISKA OCH SÄKERHETSRISKER

Det är olagligt att tillgängliggöra upphovsrättsskyddad musik, film och annat material via Internet utan tillstånd från rättighetshavarna. Upphovsrätten skyddar upphovsmän m.fl. mot olovlig kopiering och spridning av deras verk och produktioner. Brott mot upphovsrätten kan likställas med stöld från upphovsmannen.

Utan tillfredsställande försiktighetsåtgärder kan dator- och serversystem på ett företag användas för illegal spridning av upphovsrättsskyddat material. Av den anledningen är det viktigt att förstå vilka juridiska och säkerhetsmässiga risker som ert företag, de ansvariga och era anställda kan utsättas för.

CIVILRÄTTSLIGA ELLER STRAFFRÄTTSLIGA ÅTGÄRDER

Det är olagligt att kopiera, distribuera eller att tillgängliggöra någon annans material via Internet utan tillstånd. Rättighetshavare är särskilt oroade för stöld av upphovsrättsskyddat material via Internet både av privatpersoner och via företag.

Därför vidtar rättighetshavarna regelbundet rättsliga åtgärder mot företag och privatpersoner som begår brott mot upphovsrätten via tex fildelning eller andra nätverk.

Ett exempel är när musikindustrin vidtog rättsliga åtgärder mot en läkarmottagning i Tyskland som på sina datorer lagrade och tillgängliggjorde stora mängder musik via fildelning på Internet.

SÄKERHETSLUCKOR

Om det finns illegala kopior av upphovsrättsskyddat material lagrade på ert företags servrar eller datorer finns det en risk för att ert företags data och IT-säkerhet är utsatt för en säkerhetsrisk. Illegala webbsidor och fildelningsklienter – som många gånger är källan till stora mängder illegal musik, film, programvara, spel mm – är kända källor för:



Virus. Virus kan orsaka stor skada som tex att förstöra individuella datorer eller spridas vidare inom nätverket. En undersökning genomförd av säkerhetsföretaget TruSecure visade att 45% av de filer som laddades ned från de mest kända och populära fildelningstjänsterna innehöll datorvirus, maskar eller elak kod.



Spyware. Fildelningsklienter innehåller ofta odokumenterad "spyware" som återrapporterar användandet av datorn dvs vilka webbplatser som besöks mm samt visar reklam och andra oönskade filer på skärmen. Spyware är mycket svårt ta bort och det krävs stor datorkunskap samt mycket tid för att radera spyware, dessutom orsakas ibland skador på datorn vid radering.¹



Brandvägssluckor.

Fildelningsprogram kräver oftast att det finns en direktkommunikation, en öppen port i brandväggen, mellan användarens dator och Internet. Detta är samma sak som att lämna ett gapande hål i brandväggen. Samma brandvägg som ert företag använder för att skydda företagets interna nätverk och servrar är då öppen för miljontals okända användare.



Förlorade resurser.

Olaglig musik och annat upphovsrättsskyddat material kan uppta mycket stora utrymmen (gigabyte) på företagets servrar och datorer. Fildelning medför även att både personer på företaget och externa personer nyttjar ert företags dator- och Internetkapacitet för att ladda ner eller distribuera olagliga filer. Detta kan medföra att stora lagringsutrymmen upptas samt att stora delar av er Internetkapacitet utnyttjas till olaglig verksamhet.

Nedan har vi listat ett antal situationer som kan innebära att ert företags utrustning används för brott mot upphovsrätten och att ert företags datorsystem är utsatt för säkerhetsrisk.

HAR ERT FÖRETAG PROBLEM?®

Nedan har vi listat ett antal situationer som kan innebära att ert företags utrustning används för brott mot upphovsrätten och att ert företags datorsystem är utsatt för säkerhetsrisk.

- Ni vet inte vilka program och filer som finns lagrade på företags datorer och servrar.** Ni bör göra en inventering av alla program, musikfiler, filmer, spel och annat upphovsrättskyddat material som finns lagrade på företags datorer och servrar. Kontrollera datorer och servrar och se om det finns mappar som innehåller stora mängder musik eller annat material som inte har relevans för ert företag. Kontrollera även om anställda har installerat fildelningsprogram på sina datorer.
- Ert företag saknar brandvägg och ni har obehörig trafik via er Internetförbindelse** För att stoppa inkräktare och obehörig trafik måste alla företag som är uppkopplade mot Internet ha en brandvägg. Inkommande och utgående trafik måste regleras så att oönskad trafik och icke godkända kommunikationsprotokoll stoppas.
- Er Internetuppkoppling och ert interna nätverk är väldigt långsamt.** Långa svarstider kan vara en indikation på att någon "stjälar" kapacitet i ert nätverk eller att det finns oönskad trafik via tex fildelningstjänster. Det kan också innebära att det finns virus, spyware eller annan elak kod inom ert nätverk.
- Ni har regelbundna problem med datorvirus.** Om ert datorsystem upprepade gånger drabbats av virus eller om kunder och externa kontakter får virus via datafiler från ert företag kan det bero på att någon eller några på ert företag använder fildelning eller olagligt laddar ner upphovsrättskyddat material via Internet och samtidigt får med sig virus.
- Ni saknar en policy för hur era anställda får nyttja företags datorsystem.** Fri användning av företags datorsystem drabbar ofta produktiviteten i företaget och kan även leda till illegal fildelning och nedladdning.

Det finns flera praktiska åtgärder som ni kan ta för att undvika att brott mot upphovsrätten begås via ert företags datornätverk och på det sättet undvika de säkerhets och juridiska risker som det medför.

VAD KAN ERT FÖRETAG GÖRA? ©

UPPRÄTTA EN FÖRETAGSPOLICY.

Det är viktigt att användare, chefer och IT-personal förstår att obehörig kopiering och spridning av någon annans musik eller annat material som skyddas av upphovsrätten är ett brott mot upphovsrättslagen och något som företaget inte kan tolerera. Det bästa är att inkludera en policy för hantering av upphovsrättskyddat material i företagets policyhandbok och anställningsvillkor. Ett exempel på hur en policy kan se ut finner ni längre bak i den här guiden.

INVENTERA UPPHOVSRÄTTSSKYDDAT DIGITALT MATERIAL.

Många företag inventerar sina datorsystem och kartlägger viss typ av upphovsrättskyddat material som till exempel programvaror, men man bör även inventera annat material som skyddas av upphovsrätten som tex musik och film. Musik lagras vanligtvis i formaten .mp3 och .vma, varje musikfil är ca 3-5 Mbyte och musik hittas ofta i mapparna \min musik eller \delade filer.

RADERA OLAGLIGT MATERIAL.

Kommersiella inspelningar av musik och film är i princip aldrig licensierade för företag att distribuera via Internet, undantag är via lagliga tjänster. Om ni sprider musik eller annat upphovsrättskyddat material via Internet måste ni kunna visa att ni har tillstånd att göra det.

KONTROLLERA FILDDELNING.

Många företag förbjuder olaglig kopiering av programvaror och användning av fildelning i företagets datornätverk men kontrollerar inte att förbudet efterföljs. Det finns gratis program som till exempel Digital File Check (som finns att ladda ner på www.ifpi.se) som kan söka igenom ert företags datorer och sammanställa information om vilka fildelningsprogram och mediefiler som finns installerade och lagrade. Du får sedan välja om du vill radera, blockera eller spara de fildelningsprogram och de mediefiler som hittades.

KONFIGURERA DIN BRANDVÄGG.

En brandvägg kan konfigureras så att den tittar på all in- och utgående trafik och upptäcker otillåtna filer och program. Ni kan även konfigurera er brandvägg så att den blockerar de Internetadresser och kommunikationsprotokoll som oftast används av fildelningsprogram. Det finns även programvaror som på ett intelligent sätt kan filtrera bort upphovsrättskyddat material.

SÄKRA TRÅDLÖSA ANSLUTNINGAR.

Det är viktigt att säkerställa att företagets eventuella trådlösa nätverksanslutningar är krypterade och säkra så att dessa anslutningar inte nyttjas av okända personer för illegala ändamål.

BEVAKA TRAFIKNIVÅERNA I ERT NÄTVERK.

Det finns programvaror som kan övervaka trafiken i ert nätverk. Möjligtvis fick ni tillgång till ett när ert nätverk installerades, och som ger er möjlighet att se om vissa användare eller någon utrustning "stjäl" stora mängder bandbredd. Kontrollera "hot spots" för att se om det finns något systemfel eller om någon illegal aktivitet pågår.

HA BRA VIRUSSKYDD.

Antivirusprogram kan säkerställa att ert datorsystem inte drabbas av virus, spyware eller andra filer som kan skada era datorer och bör därför finnas installerat på alla datorer inom företaget. Leverantörerna av antivirusprogram uppdaterar regelbundet programmen för att det ska skydda mot de senaste typerna av virus. Det är därför viktigt att alltid ha den senaste versionen av antivirusprogrammet installerat.

HA BRA SKYDD MOT SPYWARE.

Det är även viktigt att skydda företagets datorer mot spyware, adware och liknande program. Precis som för antivirusprogram måste det finnas skydd mot spyware, adware m.m. installerat på alla datorer inom företaget och det är viktigt att alltid att ha den senaste versionen.

TILLSÄTT EN ANSVARIG.

Varje företag bör utse en person, om en sådan inte redan finns, som är ansvarig för att säkerställa att företagets policy kring hantering av upphovsrättskyddat material efterföljs. Det är viktigt att den ansvarige personen kan tydliggöra vikten av att företagets policy efterföljs. Den ansvarige personen måste även säkerställa att olagligt material raderas och att personer som inte efterföljer policyn blir informerade om att företaget inte accepterar brott mot upphovsrätten samt vilka konsekvenser det kan få för både företaget och den individuella personen.

PM

TILL: (DISTRIBUTIONSLISTA)
FRÅN: (FÖRETAGETS LEDNING)
ÄRENDE: FÖRETAGETS POLICY KRING UPPHOVSSKYDDAT MATERIAL
DATUM: (DATUM)

Syftet med detta PM är att påminna dig om (företagets namn) förhållningssätt till användandet av upphovsrättsskyddat material på (företagets namn) datorer, nätverk och liknande media.

Kopiering och nyttjande av upphovsrättsskyddat material utan tillstånd från dess rättighetshavare är olagligt och kan leda till att du utsätter både dig själv och företaget för civilrättsligt och straffrättsligt ansvar i enlighet med upphovsrättslagen. Detta gäller all typ av upphovsrättsligt skyddat material inklusive musik, film och programvaror.

Anställda får ej hantera olagliga kopior av upphovsrättsskyddat material från sin dator, nätverk eller annan form av media som ägs av (företagets namn). Anställda får ej heller tillgängliggöra kopior av upphovsrättsskyddat material via Internet eller ägna sig åt verksamhet såsom att koppla upp sig via fildelningsnätverk i avsikt att främja eller medverka till upphovsrättsligt intrång.

(Företagets namn) policy kring användandet av upphovsrättsskyddat material finns bifogad. (Namn på den person som är ansvarig för dessa frågor på företaget) kommer regelbundet att genomföra kontroller för att säkerställa att det inte finns olagligt material lagrat på (företagets namn) datorer och servrar och att inte företagets utrustning används för olaglig spridning av upphovsrättsskyddat material.

Om du har frågor ber vi dig kontakta (namn på ansvariga för dessa frågor).

POLICYREGLER BETRÄFFANDE ANVÄNDADET AV UPPHOVSRÄTTSSKYDDAT MATERIAL

(Företagets namn) respekterar den upphovsrätt som tillhör den som skapar och äger rättigheterna till upphovsrättsskyddat material inklusive musik, film och programvaror skapade av andra.

(Företagets namn) anställda skall icke kopiera, förvara, överföra eller tillgängliggöra olagliga kopior av upphovsrättsligt skyddat material på företagets datorer, servers eller nätverk.

(Företagets namn) anställda får inte ladda ner, sprida (ladda upp), förvara eller tillgängliggöra olagliga kopior av upphovsrättsskyddat material via Internet genom att nyttja företagets nätverk, utrustning eller lagringsmedia.

(Företagets namn) anställda får inte installera och använda fildelningsprogram eller driva en fildelnings hub eller server inom företagets datorsystem utan godkännande från (Namn på den person som är ansvarig för dessa frågor på företaget).

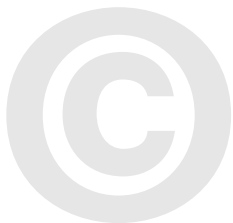
(Namn på den person som är ansvarig för dessa frågor på företaget) är ansvarig för att säkerställa så att de här policyreglerna efterföljs. Vid tveksamheter om en anställd kopierar eller hanterar upphovsrättsskyddat material på ett sätt som kan strida mot dessa policyregler skall ärendet tas upp med (Namn på den person som är ansvarig för dessa frågor på företaget) innan andra åtgärder vidtas.

Alla aktiviteter eller material som bryter mot dessa policyregler kommer omedelbart att åtgärdas.

(Företagets namn) anställda som bryter mot dessa policyregler är föremål för disciplinära åtgärder i enlighet med företagets interna regler i denna typ av ärende. Sådana disciplinära åtgärder kan komma att innebära uppsägning.

Underskrift





representing the
recording industry
worldwide

IFPI Svenska Gruppen
Box 1429
111 84 Stockholm

Tel: +46 (8) 735 97 50
Fax: +46 (8) 27 37 45
www.ifpi.se
www.legalmusik.se