

Anvisningar beträffande informationssäkerheten (modell)

Genom att gå igenom följande frågor och ta reda på svaren kan du bygga upp en bra stomme för företagets informationssäkerhetsanvisningar.

1. In- och utgångar till lokaliteterna

- Fastställ normala rutter och undantagsrutter till företagets lokaliteter.
- Vilka rutter används i en nödsituation?
- Vem svarar för passersedlar?

2. Allmänna anvisningar om verksamhet i företagets lokaliteter

- På vilket sätt har det beaktats i fråga om informationssäkerheten, om det arbetar flera företag i byggnaden eller i samma lokaliteter?
- Finns det gemensamma lokaliteter som används av flera företag? Inverkar detta t.ex. på diskussioner om frågor som hänför sig till kundprojekt. Vilka instruktioner har personalen fått om detta?

3. Lösenord till nätet

- Hur länge är ett lösenord i kraft?
- Finns det anvisningar om innehållet i lösenord?
- Vad skall man göra om man glömmer sitt lösenord?
- Hur snabbt föråldras ett lösenord?

4. Virusbekämpning

- Vilket antivirusprogram är i användning och hur uppdateras det?

4.1 E-post

- Vilka anvisningar om kryptering av e-postmeddelandet har getts?
- Finns det anvisningar om öppnande av bilagor i e-postmeddelanden.

4.2 Installering av program som laddats ned från nätet

- Vilka program är det tillåtet att ladda ned i arbetsdatorerna från nätet?

5. Säkerhetskopior

- Vem svarar för säkerhetskopiering?
- Hur sköts säkerhetskopiering av servrarna?
Obs. Säkerhetskopiering ersätter inte arkivering av filer!

6. Utskrifter

- Finns det anvisningar om användning av skrivarna?

7. Konfidentiellt material

- Material som innehåller konfidentiell information får inte slängas i en vanlig skräpkorg, det skall i stället läggas i ett låst kärl från vilket det förstörs på ett tryggt sätt.

8. Användning av arbetsstation och bärbar dator

- Datorn skall alltid låsas då du går bort från din arbetsstation (t.ex. genom att trycka *ctrl-alt-del* en gång). På det här sättet kan förbipasserande inte se vad som finns på skärmen. Om du delar ut filer från din egen arbetsstation till andra, bör du alltid kontrollera vem som får tillgång till filerna. Dela aldrig ut hela skivenheten från "roten" eftersom det ger tillgång till all information på ifrågavarande enhet.
- Lämna inte datorn liggande framme i bilen eller på något annat ställe, då du är borta från kontoret.
- Om du hanterar filer från arbetet på din hemdator, måste du försäkra dig om att datorn är utrustad med en aktuell och fungerande brandvägg och ett antivirusprogram.

9. Demonstrationstillfällen

- Lagra filer som du behöver vid ett demonstrationstillfälle på maskinen eller försäkra dig om att du kommer åt dem över nätet innan demonstrationen börjar. Om du söker filer från företagets intranät under mötet, skall du göra det via maskinens egen skärm och inte över videokanonen skärm. Städa bort alla anteckningar från bord, tavlor och andra ställen efter mötet.

10. Användning av internet

- Vilka anvisningar har getts om användning av internet i arbetet och under arbetstid? Har de anställda fri tillgång till nätet? Har "suspekta" webbplatser definierats.

11. Gäster

- På vilket sätt tas gäster emot? På vilket sätt har informationssäkerheten tagits i beaktande i fråga om placeringen av konferensrummet. Kommer gästerna in i produktionslokalerna?

12. Underleverantörer och frilansare

- Ingå sekretessavtal med underleverantörer och frilansare som används i projekt innan arbetet inleds.