ANTONUTBILDNING

Policy för användning av digitala verktyg

Denna policy omfattar medarbetare och konsulter inom Anton Utbildning under arbetstid och användning av företagets utrustning och datakommunikation.

Vi hanterar dagligen allt större mängder digital information, och det blir samtidigt allt vanligare med digitala brott. Det finns därmed en ökad risk att du förlorar utfört arbete eller att känslig information hamnar i orätta händer.

Den största risken är många gånger vårt eget beteende. Att stanna upp och tänka till innan man klickar på en länk eller e-postbilaga hindrar du de allra flesta virusattacker.

När du ska hantera personuppgifter, tänk först efter om det verkligen är nödvändigt. Om det är det, är nästa steg att tänka på vilken typ av personuppgift det handlar om och vilket skydd som krävs för att du ska hålla dig till förordningen. Till exempel är det viktigt att inte samla in fler personuppgifter än nödvändigt, att inte spara dessa längre än nödvändigt och att känsliga uppgifter lagras i säkra system.

1. **Privat användning** är tillåten i minsta mån men ska inte inkräkta på arbetstid och ska göras med gott omdöme. Det är till exempel inte tillåtet att besöka webbplatser som förknippas med pornografi, rasism, nynazism eller liknande om det inte är professionellt motiverat. För att undvika oklarhet ska privata mejl inte skickas med företagsadressen som avsändare. Privata ljudfiler eller filmer ska inte lagras på företagets datorer eller lagringsytor lagring av fler än enstaka privata bilder.

2. **Upphovsrättsskyddat material** - Lagar och regler om upphovsrätt gäller även material som finns på internet. Det är inte tillåtet att använda information från internet på ett sätt som kränker upphovsrätten (t.ex. genom felaktig användning av bilder eller upp-/nedladdning av piratkopierat material).

3. **Hantering av konton och lösenord** - Lösenord är en allt viktigare del av vår digitala säkerhet och ska aldrig lämnas ut till annan person. Lösenord som används till Anton Utbildningssystem får inte användas i något annat system eller tjänst då det kraftigt ökar risken för intrång. Om vi lämnar dator/platta/telefon utan övervakning ska den låsas eller stängas av så att obehörig åtkomst förhindras.

4. **Känslig information** - Känsliga personliga uppgifter eller annan känslig information ska alltid hanteras med försiktighet och endast lyftas ut ur, för dem avsedda, informationssystem om vi vet att hanteringen är säker. I dessa fall ska epost användas minimalt och inte utanför koncernen. Känsliga dokument som skickas i mail måste lösenordsskyddas.

5. **Installation av programvara** Om du installerar programvara som du varken fått via ramavtal eller enligt instruktion från Antonkolan måste du vara helt säker på att den är licensierad och inte innehåller skadlig kod. Om du är osäker ska du ta kontakt med IT-supporten. All lagrad information eller trafik kan under vissa förutsättningar komma att kontrolleras, exempelvis för att spåra hackerangrepp eller undersöka eventuella oegentligheter. Detta gäller även privat information eller användningshistorik som lagras på utrustning och system.

Rev 2018-05-28