Datasäkerhetspolicy Konsulter AB

Alexander Nilsson

Datorteknik 1a
Hermods gymnasium, Västerås

16 mars 2020

Innehåll

1 Inledning **1**
1.1 Datasäkerhet 1
1.2 Omfattning 1

2 Integritet **2**
2.1 Användare 2

3 Arbetsstationer **3**
3.1 Programvara med tillgång till Internet 3

4 Administratörskonton **4**

5 Datasäkerhetsskydd **5**
5.1 Anti-virusprogram 5

6 Granskning **6**
6.1 Administratörer 6
6.2 Användare 6
6.3 Intrångsskydd 6

7 Dataskyddsförordningen **7**
7.1 Personuppgifter 7
7.2 Dataskyddsombud 7

1 Inledning

1.1 Datasäkerhet

Syftet med datasäkerhet är att säkerställa och skydda sekretessen och integriteten av datan och dess användare, samt att säkerställa tillgängligheten av datan och driften av datasystemen. Målet med denna policy är att skapa och upprätthålla trygga system utan att försvåra för användaren onödigt mycket; om en användare anser att säkerheten är för otymplig och komplicerad uppstår risken att han/hon kringgår säkerhetsåtgärderna på ett sätt som skapar risk för dataintrång, med mera.

Användarna i företagsnätverket och -systemet har tillgång till potentiellt känslig information (personuppgifter, säkerhetsnycklar till olika tjänster, hemlighetsstämplad företagsinformation).

1.2 Omfattning

Datasäkerhetspolicyn omfattar hela systemet och alla dess användare oavsett företagsroll. Samtliga användare ska tillkännagiva riktlinjerna enligt datasäkerhetspolicyn innan tillgång till systemet beviljas utav IT-säkerhetsansvarig.

2 Integritet

2.1 Användare

2.1.1 Användare i organisationen ska tilldelas rättigheter och tillgång till delade resurser och programvara som krävs för att kunna utföra sina arbetsuppgifter.

2.1.2 Användarnas primära konton på arbetsstationer ska inte ha administratörsrättigheter. Om användaren kräver administratörsrättigheter ska ett sekundärt konto, med lösenordsskydd, skapas åt användaren på arbetsstationen i fråga.

2.1.3 Enheter som hanterar företagsdata lokalt ska ha diskkryptering påslaget (systemadministratör ansvarar för tillämpliga teknologier för respektive operativsystem).

3 Arbetsstationer

3.1 Programvara med tillgång till Internet

Användare måste känna till riskerna, och hur man skyddar sig mot dom, med att använda Internet med företagets utrustning via företagsnätverket.

Se även § 5.1.1 och 5.1.2.

3.1.1 Bilagor som bifogas med inkommande e-postmeddelanden ska alltid beaktas med försiktighet då filerna kan maskeras som ofarliga filformat, men i verkliga fallet vara en programfil som kan köra skadlig kod på enheten. Inkommande e-postmeddelanden och bilagor ska genomsöks av företaget.

3.1.2 Användare ska uppvisa försiktighet vid filnedladdningar från webbplatser, e-postmeddelanden, internetkonversationer och dylikt.

3.1.3 Programvara får endast installeras om IT-säkerhetsavdelningen har granskat och godkänt programvaran.

4 Administratörskonton

4.0.1 Alla personer med administratörsrättigheter till delar av eller hela systemet ska ha ett eget konto med unik inloggningsinformation. Flera personer får aldrig dela på ett och samma konto.

4.0.2 Nya administratörskonton med tillgång till delar av eller hela systemet måste granskas och beviljas av IT-säkerhetsavdelningen. IT-säkerhetsavdelningen avgör om personen i fråga har behov av administratörsrättigheter.

5 Datasäkerhetsskydd

5.1 Anti-virusprogram

5.1.1 Systemtjänster med uppkoppling mot Internet och som hanterar eller agerar som mellanhand med filer från okända källor ska vara skyddade med anti-virusprogram.

5.1.2 Arbetsstationer som är anslutna till företagsnätverket och med tillgång till Internet ska vara skyddade med anti-virusprogram som regelbundet uppdaterar virusdefinitioner.

6 Granskning

6.1 Administratörer

6.1.1 Administratörskonton på samtliga system ska regelbundet granskas och inaktuella eller oanvända konton ska inaktiveras för att begränsa attackvektorer.

6.1.2 Samtliga modifieringar (inom rimliga nivåer) av systemfiler och -konfigurationer ska loggas till en central server.

6.2 Användare

6.2.1 Regelbundna granskningar av samtliga systemanvändare och deras tillgång till data och systemet.

6.2.2 Installationer, ändringar och avinstallationer av programvara på arbetsstationer ska loggas till en central server.

6.2.3 Modifieringar av systemfiler och -tjänster på arbetsstationer och serverdatorer ska loggas till en central server.

6.3 Intrångsskydd

System- och nätverksadministratörer ska ta ansvar för att regelbundet se över nätverks- och systemsäkerheten för att begränsa risken för intrång av systemen och företagsdata [1].

[1] Intrångsskyddsgranskningar enligt denna policy gäller inte endast digitala system, men ansvaret för analog datasekretess faller på andra enhetschefer.

7 Dataskyddsförordningen

7.1 Personuppgifter

7.1.1 Personuppgifter om privatpersoner får endast behandlas av användare som har tillkännagivit alla riktlinjer i dataskyddsförordningen (GDPR). Personuppgifter innefattar:

- Namn
- Adress
- Personnummer
- Porträtt eller annan avbildning av privatperson
- Ljudinspelningar av samtal

7.1.2 Känsliga personuppgifter ska inte lagras eller behandlas på eller med systemet eller företagsutrustning. Känsliga personuppgifter innefattar:

- Etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i en fackförening
- Hälsa
- Sexualliv eller sexuella läggning
- Genetiska uppgifter
- Biometriska uppgifter som används för att entydigt identifiera en person

7.1.3 Företaget ska utse ett dataskyddsombud om något av följande stämmer:

- Bolaget är ett offentligt organ
- Bolaget utför regelbundet, systematiskt och i stor omfattning övervakning av enskilda personer
- Bolaget har som kärnverksamhet att behandla känsliga personuppgifter eller uppgifter om brott i stor omfattning

7.2 Dataskyddsombud

7.2.1 Dataskyddsombudet ska ha kunskaper om dataskyddsförordningen, förstå företagets kärnverksamheten, ha fullständig inblick i hur personuppgifter behandlas, ha inblick i och förståelse för företagets informationstekniska säkerhet samt ha förmågan att etablera en dataskyddskultur.

7.2.2 Dataskyddsombudet ska ha en oberoende ställning i företaget, får ej låta påverkas av andra inom företaget, får ej ha arbetsuppgifter som kan skapa intressekonflikter och bör lämpligen inte ingå i företagets ledning eller styrelse.