

Verksamhetssystem Today Consulting

IT-POLICY

Den 2018-05-23, har följande policy upprättats för Today Consulting AB nedan kallat "företaget".

Bakgrund

Med IT (Informationsteknik) menas både system, hårdvara och mjukvara som används för att ta fram, bearbeta, lagra, söka och sprida information samt utrustning som används till kommunikation mellan interna och externa enheter d.v.s. datorer (både stationära och bärbara), servrar och andra lagringsmedia, telefoner, handterminaler osv.

Alla medarbetare har skyldighet att i alla avseenden följa de lagar, förordningar och myndighetskrav som finns kring användning och utveckling av IT.

Syfte

Denna policy gäller för anställda inom företaget och syftar till att skapa en tydlig struktur över hur IT ska hanteras och användas i företaget. Den ska öka kunskapen kring IT, effektivisera informationsflödet och användandet samt öka säkerheten i verksamheten. Den skall också säkra och skydda de personuppgifter som lagras i systemen.

Riktlinjer

Information och utrustning

Den IT-utrustning och information som företaget tillhandahåller ska användas i arbetet och under arbetstid. Privat användning av information och utrustning som ägs av företaget bör ske med sparsamhet och gott omdöme och får inte ske på arbetstid, lunchen undantagen.

Det är inte tillåtet att använda bolagets IT-resurser för privat kommersiell verksamhet t.ex. försäljning, reklam, publicitet och liknande i något avseende.

Alla program ska installeras av IT-ansvarig och vara godkända av närmste chef. Varje dator skall ha godkända programlicenser för de program som är installerade.



Verksamhetssystem Today Consulting

Internet

Tillgång till Internet på arbetsplatsen ska ses som ett arbetsredskap. När du använder Internet på din arbetsplats representerar du vårt företag och organisation. Vid all kommunikation på Internet lämnar du spår efter dig på de webbplatser du besöker. Det är därför inte tillåtet att besöka anstötliga eller på annat sätt olämpliga platser eller att utnyttja Internet för olagliga, kränkande eller oetiska ändamål.

Spridning av information med stöd av Internet eller publicering av information på nätet gällande förtal, kränkning, mobbning, diskriminering, hets mot folkgrupp eller intrång på annans konto eller server, gäller svensk lag och är därmed straffbart. Det är inte heller tillåtet att sprida politisk, ideologisk eller religiös propaganda från den IT-utrustning som ägs av företaget.

Användningen av företagets IT-resurser får inte strida mot företagets verksamhetsmål och skapa badwill. I vår organisation utgår vi ifrån att all kommunikation på Internet följer god sed. Det är viktigt att ha säkerhetsaspekterna i åtanke vid användningen av Internet. Det är inte tillåtet att ladda hem filer, programvaror eller för den delen kopiera skyddat digitalt material om det strider mot lagen.

E-post

Alla medarbetare som har en personlig e-postadress ansvarar själva för att sortera e-post så inte lagringskapaciteten blir överfull.

Vid längre frånvaro eller ledighet ska det finnas ett system för hantering av inkommande e-post. Den anställda ska se till att ett automatisk meddelande svarar på inkommande post och hänvisar till en kollega som finns på plats.

IT-säkerhet

Informationssäkerheten ska ha en fastställd struktur med klara rutiner där säkerhetsnivån avvägts mot tillgänglighet och effektivitet. Följande riktlinjer gäller:

- Nätverket ska vara väl skyddat mot intrång
- All programinstallation och uppdatering ska utföras IT-ansvarig
- Information ska skyddas mot skada och förlust genom ett säkert backup-system
- Ett antivirusprogram skall vara installerat på varje dator där programmet uppdateras automatiskt
- E-postmeddelanden där innehållet är okänt eller där filer finns bifogade ska hanteras med försiktighet då det kan vara virus. Misstänkta meddelande får inte öppnas
- IT-ansvarige skall ansvara för underhåll och drift och regelbundet kontrollera säkerhetssystemet

Verksamhetssystem Today Consulting

Användarnamn och lösenord

- För att kunna identifiera medarbetare samt minimera risken för dataintrång har varje medarbetare ett eget användarnamn och lösenord. Den anställda som får användarnamn och lösenord tilldelat, uppmanas byta lösenord, samt måste själv välja ett lösenord. Riktlinjer är framtagna som gäller för hur lösenordet skall konstrueras för att de ska vara så säkra som möjligt.
- Företagets chefer ansvarar för att alla anställda inom bolaget är förtrogna med riktlinjerna för att konstruera lösenord, men det ligger på individens ansvar att följa den.
- Följande riktlinjer gäller för att konstruera lösenord
 - Lösenordet ska vara personligt och får inte avslöjas för andra
 - Lösenordet i berörda system ska bestå av:
 - Minst sex tecken.
 - Minst tre av de sex tecknen skall vara versaler, gemener, siffror
 - Lösenordet får inte vara knutet till personlig information, som till exempel telefon- eller personnummer.
 - Lösenordet ska bytas en gång om året
 - Lösenordet skall inte skrivas ned och sparas tillsammans med IT-klienten
 - Lösenordet ska hanteras som en värdehandling.
 - Vissa system kan kräva ytterligare säkerhet, som exempelvis låsning av system vid tre misslyckade inloggningsförsök.
 - Vid borttappat lösenord skall följande kontaktas i ordningen,
 1. IT-ansvarig

Missbruk

Vid missbruk eller misstanke om missbruk kan kontroller av användningen av datorer, nätverk och Internet genomföras. I förlängningen kan anställningen komma att ifrågasättas vid brott mot denna policy. Om det av kontrollerna framgår att riktlinjerna överträtts kan ärendet komma att utredas av personalchef. Arbetsgivaren kommer i första hand försöka åstadkomma rättelse genom påpekanden eller liknande förfaranden. Vid allvarigare missbruk kan disciplinära åtgärder komma att vidtas.

Hantering av personuppgifter i IT-system

Behandling av personuppgifter

Företaget värnar om din personliga integritet. Du ska kunna känna dig trygg när du anförtror oss dina personuppgifter. Vi har tydliga policyer och rutiner som beskriver hur vi behandlar personuppgifter inom organisationen. Den utgår från gällande dataskyddslagstiftning och beskriver bland annat hur vi samlar in personuppgifter, för vilka ändamål, hur länge uppgifterna sparas, vilka som har tillgång till uppgifterna, hur vi hanterar personuppgiftsincidenter etc. Policyerna beskriver även hur vi tillvaratar och tillmötesgår dina rättigheter och din integritet.



Verksamhetssystem Today Consulting

Today Consulting AB är personuppgiftsansvarig, vilket innebär att vi är ansvariga för hur dina personuppgifter behandlas och att dina rättigheter tas tillvara.

Kontaktuppgifter

Du kan kontakta oss på gdpr@todayconsulting.se eller 010 207 19 10 samt via vanligt brev till Today Consulting AB, Nygatan 35 A, 311 31 Falkenberg

Ansvar

Som ytterst ansvarig för företagets IT-strategi och denna IT-policy står företagets VD. Ansvarig för drift och säkerhet är IT-ansvarig.