IT-Policy

Currentum är en installationskoncern som verkar inom ventilation, fastighetsautomation, VS, el, säkerhet och sprinkler över hela Sverige. Samtliga företag med anställda inom Currentum ska upprätthålla och följa riktlinjerna i denna policy.

Syftet med IT-policyn

IT-policyn beskriver hur företaget vill att den anställde skall agera i olika sammanhang gällande IT-relaterade frågor. Om alla följer den implementerade IT-policyn skapas bättre förutsättningar för att IT som funktion ska fungera på bästa tänkbara sätt och skydd från virus och cyber-attacker. Verksamheten är beroende av att IT-miljön fungerar. Företagets IT-resurser ägs av företaget och är avsedda att användas inom företagets verksamhetsområden. All annan användning får endast förekomma i begränsad omfattning.

Målgrupp

Samtliga anställda, inhyrd personal eller annan person som företräder företaget skall agera efter denna IT- policy och enligt svensk lagstiftning.

Internet

Privat surfande skall undvikas på arbetstid. Det är inte tillåtet att besöka webbplatser med rasistiskt, extrempolitiskt, pornografiskt eller annat lagöverträdande innehåll. Det är inte heller tillåtet att delta i chattsidor eller ladda upp/ned ej arbetsrelaterade filer från/till internet. För anmälan till mailinglistor gäller att anmälan endast får ske till listor där informationen behövs i tjänsten. Företaget har möjlighet att registrera all internetanvändning i en logg. Loggningen omfattar uppgifter om användarnamn och namnet på den webbplats som besökts. Kontroll av enskilda individers internetanvändande kan komma att utföras. Företagets IT-resurser får inte nyttjas för att på otillbörligt sätt sprida, förvara eller förmedla information som strider mot gällande lagstiftning.

Detta gäller exempelvis:

- hets mot folkgrupp
- hatbrott
- barnpornografibrott
- olaga våldsskildring
- förtal
- ofredande
- dataintrång
- upphovsrättsbrott

Vidare får inte företagets IT-resurser användas till aktivitet som:

- kan betraktas som politisk, ideologisk eller religiös propaganda

- strider mot PULs eller GDPRs stadgar om den personliga integriteten
- kan uppfattas som kränkande och stötande
- syftar till att marknadsföra produkter eller tjänster utan anknytning till företaget

Sociala medier

Sociala medier blir ett allt viktigare verktyg i företagets externa kommunikation. Dessa kan förenkla kommunikationen med nya och befintliga kunder men även göra företaget stor skada vid misstag eller felaktigt användande. Som anställd förväntas du företräda företaget professionellt, korrekt och för företagets bästa i företagets sociala medier. I de fall du som anställd publicerar inlägg i företagets externa kanaler ska inlägg handla om de områden som företaget agerar inom, t ex nyheter om vårt företag, våra tjänster, branschinformation, tips och idéer etc. som på ett sakligt sätt skapar en objektiv bild av oss och våra värdegrunder.
Följ företagets rutin för vem som ansvarar för publicering och kontohantering på sociala medier.

Nät/bandbredd

Det är viktigt att alltid undvika att utnyttja bandbredden och den delade internettrafiken för privata ändamål under arbetstid. Detta för att bandbredden har en belastningsgräns och företagets arbetsrelaterade tjänster, filhantering och surfhastighet prioriteras för att bibehålla prestanda.

Internet skall användas för informationsinsamling i tjänsten vilket innebär att användandet av Internet skall vara strikt yrkesmässig. Internet skall användas av samtliga anställda inom företaget med sunt förnuft och gott omdöme.

Internet får aldrig användas på följande sätt inom företaget:

- För illegal nedladdning av musik, filmer, mjukvara eller bilder till företagets datorer
- För att besöka sajter vars innehåll bryter mot företagets etiska regler. Detta kan till exempel vara sajter med rasistiskt, pornografiskt eller politiskt extremt innehåll. Det kan också vara sajter som innehåller någon form av olaglig information.
- För att ladda ner, installera och använda fildelning olagligt.
- För att spela någon form av spel på arbetstid.
- För att sprida information på exempelvis forum eller dylikt där det kan råda oklarhet i om man företräder företaget eller inte.

E-post

- All användning av e-post skall gälla arbetsrelaterad trafik. Privat trafik får förekomma i begränsad omfattning och under restriktioner som anges i denna policy.
- Företaget har möjlighet att registrera all mejlkommunikation i en logg. Loggningen omfattar uppgifter om användarnamn och namnet på mottagaren samt innehåll i mejlet. Kontroll av enskilda individers mejl kan komma att utföras om det råder misstanke om brott mot policy.
- Alla sända och mottagna mejl är företagets information, ej den enskilda anställdas.
- Filer från okända avsändare bör aldrig öppnas av säkerhetsskäl för att undvika virus och skadlig kod.

- Anställda får inte skicka mejl från en annan användares mejlkonto utan dennes godkännande.
- Det är förbjudet att läsa andra medarbetares e-post utan dennes medgivande.
- Känslig information såsom personlig information eller företagshemliga uppgifter skall krypteras innan dessa uppgifter sänds vidare när det möjligt. Överväg också om känslig information i stället bör skickas med vanlig postgång. Detta på grund av att risken för att en obehörig kan komma över informationen ökar när informationen har lämnat företaget.

Information

All information som finns på lagringsytor som på något sätt kontrolleras av företaget eller leverantör till företaget är företagets egendom. Anställd som har givits tillstånd att använda företagets eller annan parts material måste respektera copyrightskydd och kan därmed inte kopiera, modifiera eller vidarebefordra upphovsrättsskyddat material till annan part utan upphovsrättsmannens tillåtande. Det är inte heller tillåtet att förändra eller förmedla material skapat av annan utan dennes kännedom och/eller medgivande.

Mjukvara

Anställda eller inhyrd personal får ej på eget bevåg införskaffa eller installera/avinstallera program på server eller klient som inte först har godkänts av IT-ansvarig person/företag. Den data som lagras på servrar eller på datorns hårddiskar tillhör företaget under iakttagande av gällande sekretessbestämmelser.

Hårdvara/Enheter

Anställda eller inhyrd personal får ej på eget bevåg införskaffa eller installera hårdvara eller annan utrustning såsom mobila enheter, bärbara datorer, stationära datorer, som inte först har godkänts av IT-ansvarig person/företag. Brukaren av företagets IT-utrustning skall alltid behandla utrustningen varsamt och med aktsamhet.

Säkerhet

Varje användare ansvarar för sina konton. Konton får inte göras tillgängliga för andra. Lösenordet är personligt och får inte lämnas vidare. IT-miljön får inte användas på ett sätt som vållar problem eller skadar enskild person eller företagets anseende. Detta inkluderar att göra intrång eller på annat sätt skaffa sig tillgång till information, konton eller system som den anställde ej har behörighet till.

Krav vid lösenordshantering:

- Lösenordet skall innehålla minst åtta (8) tecken.
- Lösenordet skall inte kunna kopplas till dig eller någon av dina familjemedlemmar eller på annat sätt vara lätt för en utomstående att gissa sig till.
- Använd både bokstäver, siffror och specialtecken. Använd både stora och små bokstäver.

Om användaruppgifter lagras i pappersform (eller digitalt, exempelvis mobiltelefon) skall valt media förvaras och hanteras som en personlig värdehandling. Lösenord skall omgående bytas om misstanke finns att det har avslöjats.

Användning av Apple ID/Samsung ID av företagets egendom

Vid användning av Apple ID/Samsung ID av företagets egendom ska varje anställd följa företagets regler för användning, hantering, säkerhet och återvinning. Det är endast tillåtet att lägga in Apple ID / Samsung ID som är knutna till den av företagets tilldelade mailadress. Mobiltelefon, dator, platta eller motsvarande kan räknas som företagets egendom och ska återlämnas vid anställnings avslutande, om inte annat överenskommes.
Vid avslutad anställning ska SIM pin-kod, telefonlås-kod, lösenord till Apple ID/Samsung ID skall uppges till arbetsgivaren. Om detta ej görs kommer kostande för egendomen regleras på slutlönen.

Planerade underhåll

Utsedd IT-ansvarig kommer att utföra schemalagt underhåll på alla maskiner för att säkerställa driften och säkerheten i IT-miljön enligt företagets rutiner. Under detta underhåll kan funktioner i IT-miljön vara nedsatta eller icke fungerande.

Sekretess

Ingen anställd, inhyrd personal eller annan person som omfattas av företagets IT-policy får lämna ut konfidentiell information till någon utomstående.

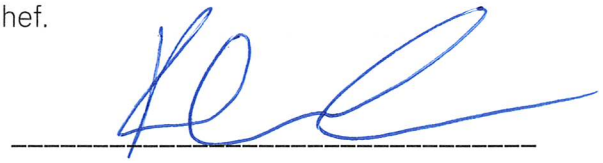
Vid upphörande av anställning skall konfidentiell information återlämnas till företaget av utsedd person.

Överträdelse

Om det av kontrollerna framgår att riktlinjerna överträtts kan ärendet komma att utredas. Arbetsgivaren kommer i första hand att försöka åstadkomma rättelse eller påpekanden eller liknande förfaranden. Vid allvarligare missbruk kan disciplinära åtgärder komma att vidtas. Lagöverträdelse polisanmäls enligt företagets rutiner.

Support

Användare som vid nyttjande av företagets IT-resurser upptäcker fel eller annat som kan vara av betydelse för IT- driften inom företaget (incident), skall genast rapportera detta till företagets IT-support och närmaste chef.



Klas Larsson, Koncernchef Currentum

Policy antagen av ledningsgruppen för Currentum AB 2022-04-26