# INFORMATIONSSÄKERHETSPOLICY

Kraftkonsult ska kännetecknas av hög säkerhet, både den fysiska säkerheten för våra medarbetare och intressenter samt informationssäkerhetsmässigt. Vi ska arbeta enligt ställda krav med stort fokus på hållbara lösningar. Vår IT-policy är grundläggande i vårt arbete för att ständigt förbättra vår och våra kunders säkerhet.

Syftet med denna policy är både en vägledning samt förhållningssätt av användande av företagets IT resurser. Den ska även bidra till att säkerställa att företagets resurser, data, samt personuppgifter hanteras på ett tillbörligt och lagligt sätt. Medarbetare är skyldig att följa denna policy.

Medarbetaren är skyldig att följa lagar samt rutiner och policys som upprättats i syfte att följa den nya lagstiftningen gällande hantering av personuppgifter.

## 1. SYSTEM OCH RESURSER

Endast godkända system och programvaror får användas. Datorer, telefoner, surfplattor ska vara ägda av företaget, de ska vara konfigurerade av Kraftkonsults IT avdelning. Om användare behöver ytterligare programvaror eller utrustning ska detta godkännas av IT avdelningen. Syftet är att säkerställa att gällande licensieringsmodeller efterföljs, att utrustning uppfyller företagets krav på säkerhet gällande virusskydd, behörigheter samt att programvaror med så kallade. Malware inte installeras.

IT utrustning ska hanteras varsamt. Användare ska iaktta försiktighet så att stöldrisk, fall och dataförlust minimeras. Alla enheter tillhörande datorn ska krypteras där krypteringsskyddet inte får ändras. Nyckeln för kryptering får inte skrivas ut, lagras eller distribueras. Datorn får användas för privat bruk i enlighet med denna policy dock får inte datorn lånas ut till obehöriga utan kontinuerlig övervakning.

För tiden uppsatt regelverk för lösenordshantering och tvåfaktorautentisering (2FA). Dator får inte lämnas olåst utan direkt uppsikt och 2FA-certifikatet får inte lagras tillsammans med datorn. 2FA-certifikatet ska hanteras som en personlig säkerhetstillgång, får inte lämnas ut till obehöriga och oövervakat. Datorn ska alltid låsas när den inte används där 2FA säkerheten avlägsnas från datorn. Detta gör att datorn automatiskt låses och skyddar datorn från att obehöriga ges åtkomst och kan orsaka skada i användarens namn.

När så är möjligt ska utloggning alltid ske från system när datorn inte används. Det räcker inte med att endast låsa datorn utan använda system bör loggas ur och stängas ner. Datorn ska alltid låsas där 2FA säkerheten ska avlägsnas.

Mobila enheter ska alltid förses med pinkod eller biometriskt lås. Åtkomst till bolagets system genom mobila enheter ska skyddas där bolaget ska vidta möjliga åtgärder för att skydda denna data. Applikationer på företagets mobila enheter ska installeras med försiktighet där Säkerhetsansvarig eller Administratör bör rådfrågas vid osäkerhet.



Kraftkonsult i Skandinavien AB
Box 130, 826 23 Söderhamn
Web: kraftkonsult.nu

Fakturaadress:
Fack 2171, Box 226,
851 04 Uppsala

Telefon: 0270-104 50
Fax: 0270-106 50
Mail: info@kraftkonsult.nu

Orgnr: 556143-8648
Momsregnr: SE556143864801
Godkänd för F-skatt

## 2. HANTERING AV DATA

All data tillhör företaget. Det ska lagras på företagets server, i avsedd filstruktur enligt gällande processer. Tillfälligt lagrat data på lokal disk ska så snart det är möjligt flyttas till servern. Detta för att säkerställa att informationen blir säkerhetskopierad via företagets backup-system.

- Externa lagringslösningar, såsom Dropbox, Google Drive mm ska ej användas då de inte uppfyller dels Kraftkonsults krav på informationssäkerhet, dels att det inte kan garanteras uppfylla kravet för GDPR. Detta gäller inte OneDrive som ingår i vårt Office 365.
- Data innehållande personuppgifter ska hanteras enligt GDPR. Alla medarbetare ska ha genomgått grundläggande kurs i GDPR. Utförandeprocesserna beskriver hur GDPR ska följas i det praktiska arbetet. En särskild policy finns upprättad för detta.
- Känsliga data ska inte skickas som epost då informationen/informationsbäraren inte är krypterad och därmed kan läsas av obehöriga. Överväg andra säkra medier för att skicka känsliga data.
- Känsliga data som överförs till mobil lagringsmedia, så som USB minne eller extern hårddisk, ska krypteras. Avsteg från detta får endast göras om kund kräver att informationen inte krypteras. I dessa fall ska kunden upplysas om risken med att skicka icke krypterade data. Om kund inte vill ta emot krypterade data finns möjligheten att komprimera, det vill säga skapa en ZIP-fil, med låsning för uppladdning till USB-minne. Alla medarbetare ska undvika mobil lagring av data där GIDA ska övervägas för distribution. Kraftkonsult förbehåller sig rätten att spärra åtkomst till extern lagringsmedia som inte är krypterad och verifierad som media tillhörande Kraftkonsult. Vid frågor om kryptering kan alla medarbetare vända sig till bolagets Administratör eller Säkerhetsansvarig.
- Som data räknas även utskriven information vilket gör att skrivbord ska hållas rena, skyddsvärd information ska förvaras låst, skyddsvärd information ska destrueras genom strimling eller avsett låst sopkärl för dokumentåtervinning och utskrifter av dokument ska hanteras på ett säkert sätt där dokument inte lämnas oövervakat. Till låst förvaring räknas låsning av separata kontorsrum där begräsning av åtkomst är begränsad.

### 2.1. E-POSTHANTERING MED PERSONUPPGIFTER

E-post innehåller nästan alltid personuppgifter, vilket innebär att dataskyddsförordningen gäller även för e-post. Det betyder att en bedömning för behandlingen av personuppgifter behöver göras där det ska finnas rättslig grund. För att minimera risk för förlust eller felhantering av personuppgifter i e-post, ska följande principer följas:

- *Begränsa användningen personuppgifter i e-post* till vad som är nödvändigt för att uppfylla ändamålet. Det följs av den så kallade uppgiftsminimeringsprincipen.
- *Tänk på vilka som behöver ta del av e-post* som innehåller personuppgifter. Som huvudregel ska endast personer som har behov av tillgång till personuppgiften för att kunna utföra sitt arbete också ha tillgång till dem. Därför finns anledning att överväga till vilka e-postmeddelanden skickas.
- *Radera e-post.* Personuppgifter får bara behandlas så länge de behövs för att uppfylla ändamålen med behandlingen. Lagra bara e-post som är ändamålsenligt och radera övrig epost. Bolagets tillämpning av efterlevandeprincip för automatisk radering av epost ska efterföljas vilket möjliggör automatisk hantering av denna princip.
- *Sprid inte personuppgifter i onödan*. Vid distribution av epost till en större mängd mottagare bör fältet för dold kopia (bcc) användas.
- *Om personuppgifter i e-post ska sparas* exempelvis kontaktuppgifter till markägare, skriv in dessa i projektets dokumentation och radera mailet. Huvudprincipen är alltid att flytta uppgifterna till det system/lista de hör till och sedan radera.

### 2.2. HANTERING AV KÄNSLIGA OCH EXTRA SKYDDSVÄRD DATA

För att underlätta gallringsrutin ska personuppgifter av känslig och extra skyddsvärd karaktär, exempelvis personnummer, biometriska data och religiös tillhörighet, sparas i strukturerade fält. Spara inte personuppgifter av denna karaktär i fält som inte är strukturerade, exempelvis i textdokument, Word, Excel eller fritextfält i system, där inte behandlingen är dokumenterad i bolagets system för behandlingar av informationstillgångar. Vid frågor rådfråga bolagets Säkerhetsansvarige.

## 3. EPOST OCH ANVÄNDANDE AV FÖRETAGETS NAMN OCH VARUMÄRKE

Medarbetaren representerar företaget bland annat via sin epost-adress. E-postadresser är konstruerad enligt modellen ”fornamn.efternamn@kraftkonsult.nu”.

- Användning av e-post för privat bruk är tillåtet i begränsad omfattning.
- Vid användning privat ska beaktas att den e-post som skickas företagets epostkonto kan uppfattas av mottagaren som företagspost.
- Privat e-post endast innehålla neutralt material som inte kan kopplas till företaget.
- Deltagande i Epostlistor ska vara relaterade till företagets verksamhet.
- E-postadressen tillhör företaget.

### 3.1. SOCIALA MEDIER

Utgångspunkten är att företaget ser positivt på att anställda deltar på olika sätt i sociala medier. Vårt engagemang i sociala medier sprider våra budskap och stärker vårt varumärke. Det stärker också bilden av organisationen som öppen och tillgänglig.

Du som person är alltid närvarande som en enskild individ, men din medverkan i sociala medier påverkar inte bara bilden av dig utan också bilden av företaget. Det är mycket viktigt att varje medarbetare skiljer på när deltagande i sociala medier faller inom ramen för anställningen och när deltagande faller inom ramen för det privata. Varje medarbetare är alltid personligt ansvarig för publicerat material oavsett om publiceringen skett i din egenskap som arbetstagare eller privat. Uppgifter som är till skada för företaget kan utgöra brott mot lojalitetsplikten i anställningsavtalet.

## 4. IT-SÄKERHET, RISKER, FÖRHÅLLNINGSSÄTT OCH LAGLIGHET

Det sammanlagda informationsinnehållet i företagets servrar och datorer utgör ett stort intresse från våra konkurrenter att ta del av. Detta innebär ett mycket starkt behov av att skydda företagets information så den inte hamnar i orätta händer, vilket kan resultera i mycket stora ekonomiska konsekvenser för vårt företag.

Alla medarbetare ska ha ett ifrågasättande förhållningssätt mot obehöriga som frågar om åtkomst. Detta kan vara allt ifrån ett samtal från okänd person till besökare som frågar om åtkomst. Medarbetare ska även tänka på hur information hanteras på offentliga platser, dels vad som visas på datorskärmen samt vad som behandlas i telefonsamtal, för att undvika att obehöriga kommer åt känslig information.

## 4.1. RAPPORTERINGSSKYLDIGHET

Vid upptäckande av fel och brister avseende säkerhetsrutiner och system är alla medarbetare skyldig att rapportera upptäckten via avvikelserapporteringssystemet alternativt till IT-administratör eller säkerhetsansvarig. Vid akuta fel eller brister ska alltid IT-administratören kontaktas i första hand. Exempel på brister, fel och incidenter:

- Förlorad utrustning, information, misstanke om dataintrång eller virussmitta ska omedelbart anmälas till företaget.
- Vid inbrott eller stöld måste detta omedelbart anmälas till ansvarig chef, polis samt till företagets IT-partner som ser till att lösenord för VPN uppkoppling ändras för att förhindra obehörig åtkomst till nätverket.

## 4.2. SKYDD MOT SKADLIG KOD

Det finns ett stort hot mot datorer i form av virus och andra så kallade Malware (skräpprogram). Dessa sprids på internet mestadels genom e-post eller programfiler. De kan även nyttja säkerhetshål i operativsystemen, (Windows, AppleOS, Android med flera). Exempel på vad dessa program kan utföra är:

- Läsa av lösenord som knappas in på tangentbordet och sedan skicka dessa till en adress någonstans ute i världen eller i landet
- Kontrollera vilka program som används i datorn
- Skicka information som visas på skärmen till okänd mottagare
- Ladda ner information från hårddisken eller servern
- Ta över datorn utifrån
- Samla information om besökta hemsidor och öppna oönskade reklamfönster med (o)jämna mellanrum.
- En smittad dator eller ännu värre ett smittat nätverk kan innebära stora kostnader för företaget i form av konsultkostnader för borttagning av virus och spionprogram, stillestånd i nätverket under borttagningen och eventuella dataförluster.
- Dator utan virusskydd får ej anslutas i Kraftkonsults nätverk

## 4.3. GENERELLEA REGLER

Utskickade säkerhetsuppdateringar ska installeras, inga ändringar eller åsidosättningar av fördefinierade säkerhetsinställningar får göras och man är skyldig att följa nedanstående förhållningsregler.

- Det är inte tillåtet att utan tillstånd av ansvarig chef skriva ut information för att ta med utanför företaget annat än då det behövs för att ”utföra sitt arbete”.
- Man får heller inte kopiera data till externt minne t ex i form av hårddisk eller USB minne om inte informationen hanteras enligt denna policy.
- Företagets IT-resurser får inte användas för att på otillbörligt sätt sprida, förvara eller förmedla information i strid mot gällande lagstiftning, t.ex. hets mot folkgrupp, barnpornografibrott, olaga våldsskildring, förtal, ofredande, dataintrång eller upphovsrättsbrott.
- Privat surfing är tillåten i begränsad omfattning och med gott omdöme. Vid frågor vad som anses vara tillåtet rådfråga Säkerhetsansvarig eller Administratör. Det är inte tillåtet att surfa till sidor som innehåller eller erbjuder olagligt material, pornografiska tjänster eller visar pornografiskt innehåll.
- Fildelning av upphovsrättsskyddat material såsom musik och film med mera är enligt lag förbjuden.
- Lagring av ljud- och video-filer får endast lagras om det är arbetsrelaterat.

## 4.4. SÄKER EPOSTHANTERING

För intern distribution av epost ska certifikat användas för att verifiera användare om detta finns tillgängligt. Syftet med certifikatet är att verifiera riktigheten i avsändaren.

## 4.5. LÖSENORDSHANTERING

Lösenord ska lagras enligt upprättad rutin. Lösenord ska hanteras som en skyddsvärd tillgång och får inte skrivas ut, distribueras eller lagras i annat system än vad som föreskrivs av rutinen.

## 4.6. NÄTVERK

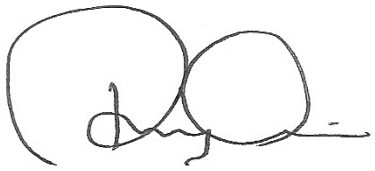
Interna trådbundna nätverk ska i första hand användas vid kontorsarbete och därefter det interna trådlösa nätverket. Vid uppkoppling till publika trådlösa nätverk ska endast kända nätverkspunkter användas. Kan inte accesspunkten verifieras, det vill säga uppkopplingspunkten för WIFI, ska mobila uppkopplingen via telefonen användas.

## 5. KUNDSYSTEM OCH KUNDDATA

Som konsult har man i regel tillgång via egen inloggning till kundspecifika system och portaler. Det är varje medarbetares skyldighet att förhålla sig till de företagens policy, sekretess- och säkerhetsregler.

Om kundavtal kräver krav på hur datatillgångar ska hanteras ska detta efterlevas. Vid frågor rådfråga Säkerhetsansvarig eller Administratör.

Söderhamn den 12 februari 2020



Tommy Norgren, VD