IT POLICY

INNEHÅLL

1. BAKGRUND OCH SYFTE

Denna policy beskriver regler och riktlinjer för användningen av IT-resurser inom Sdiptech koncernen.
Med Sdiptech koncernen avses Sdiptech AB och koncernens dotterbolag.

Med IT-resurser menas all den teknik (datorer, mobila enheter, tjänster, nätverksutrustning etc.) som används för att kommunicera, lagra och bearbeta information i digitaliserad form.

Policyn omfattar Sdiptech koncernens (”Bolagets”) samtliga IT-resurser, samtliga anställda samt inhyrd personal. Som anställd förbinder du dig att följa dessa regler vid varje tidpunkt.

Syftet med policyn för IT är att skydda Bolagets verksamhet, kunder, partners, anställda och andra intressenter.

2. RIKTLINJER OCH RUTINER

Den grundläggande principen i denna policy, är att Bolagets IT resurser ägs av Bolaget och utgör ett arbetsredskap som skall användas för Bolagets verksamhet. Bolaget ska inte lida skada eller onödiga kostnader genom olämplig användning av dessa arbetsredskap.

Bolagets IT-resurser får inte användas för att på otillbörligt sätt sprida, förvara eller förmedla information vilket:

- Är i strid mot gällande lagstiftning, t.ex. hets mot folkgrupp, barnpornografibrott, olaga
  våldsskildring, förtal, ofredande, dataintrång eller upphovsrättsbrott.
- Är att betrakta som politisk, ideologisk eller religiös propaganda.
- Är i strid mot dataskyddsförordningen (GDPR) avseende behandling av personuppgifter.
- I annat fall kan uppfattas som kränkande och stötande.
- Syftar till att marknadsföra produkter eller tjänster som saknar anknytning till Företaget.
- På något annat sätt kan störa företagets IT-verksamhet.

2.1. IT-styrning

Bolaget ska arbeta strategiskt med IT och kritiska system vilket omfattar att:

- Strategiska beslut tas av CEO med stöd av ledningsgruppen.
- Det finns en dokumenterad IT-arkitektur vilken är grunden för utveckling och förvaltning av IT-lösningar i Bolaget.
- Processer för systemförvaltning finns dokumenterade.
- Processer gällande förändringshantering finns dokumenterade vilka omfattar samtliga IT-system och funktioner inom Bolaget.
- Bolaget arbetar för att minska personberoende genom informationsdelning om system och dokumentation av IT-miljön.
- System och infrastruktur kontinuerligt övervakas och granskas.
- Informationssäkerhet, IT-säkerhet och personuppgiftshantering beskrivs i dokumenterad och godkända policys.

2.2. IT-strategi

IT strategin definierar hur IT inom Bolaget ska möta de förväntningar som verksamheten har samt stötta Bolagets affärsstrategi. IT-strategin ska beskriva visionen och målet med IT för Bolaget. IT-strategin ska sin utgångspunkt i Bolagets affärsstrategi.

2.3. Risk management

Bolaget ska i sitt arbete med övergripande risker ta hänsyn till IT-miljön och kritiska system där IT ska dokumenteras som en del i Bolagets riskdokumentation.

2.4. Individuellt ansvar

I rollen som användare förväntas du känna till och följa dessa regler och riktlinjer. Det är också viktigt att användandet av företagets IT-resurser genomförs på sådant sätt att företagets namn, anseende och goda rykte bibehålls.

2.5. Behörigheter och inloggningar

Åtkomst och behörighet till Bolagets IT-resurser (datorer, telefoner, bärbara dator, digitala plattor etc.) är individuell och får inte överlåtas eller på annat sätt göras tillgänglig för annan anställd eller extern part. Det är inte tillåtet att nyttja någon annans behörighet eller utnyttja felaktiga konfigurationer, programfel eller på annat sätt manipulera Bolagets IT-resurser. Om IT-resurser lämnas utan övervakning ska den låsas eller stängas av så att obehörig åtkomst förhindras.

Lösenordshantering skall hålla en så hög säkerhet som möjligt. För eventuella externa system eller privata enheter som IT-avdelningen inte hanterar är det

användarens ansvar att säkerställa att en så hög säkerhetsnivå som möjligt (multifaktorsautentisering är önskvärt, komplexa lösenord är minst accepterade nivå) tillämpas. Lösenord som används till Bolagets IT-resurser får inte användas i något system eller tjänst vilket inte berör bolaget.

Lösenord skall bytas regelbundet, exempelvis var 6:e månad. På grund av mångfalden inom Bolaget kan lokala regler finnas.

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

Delning av filer och dokument ska ske i linje med Bolagets tilldelade behörigheter. Användare ansvarar för att delning av dokument och filer endast sker till personer med likvärdiga eller högre behörigheter än en själv. Användare ska vara restriktiva med extern delning och följa regler definierade i denna policy och liknande policy som informationssäkerhetspolicyn. Överväg till vem information delas, samt dela inte mer information än arbetsuppgiften kräver.

2.6. Säkerhet

För att skydda Bolaget mot spridning av virus och mot obehörig åtkomst skyddas IT-resurser av säkerhetssystem, såsom antivirusskydd och brandväggar. Medarbetare inom Bolaget får inte avaktivera eller på något sätt manipulera dessa skydd.

Alla anslutningar och installationer av datorer eller annan utrustning i Bolagets nätverk ska utan undantag godkännas.

Det är inte tillåtet att ladda ner och installera programvaror som ej är godkända.

Användaren är ansvarig för en säker användning av sina personliga IT-resurser och att vidta alla rimliga åtgärder för att skydda IT-resurser mot virus, obehörigt tillträde eller andra attacker mot systemets säkerhet och integritet. Detta gäller även privata enheter som används för att komma åt företagets IT-resurser (antivirus och lokal brandvägg är ett krav och kryptering av hårddiskar är önskvärt).

2.7. Lagring

Användare är ansvariga för att lagra sina dokument och filer i därför avsedda platser enligt information från Bolaget. Det är inte tillåtet att spara data i externa lagringslösningar (såsom e-post och lagringstjänster etc.) som inte godkänts av Bolaget.

2.8. Backup

Användare ska säkerställa att lagring på lokalt skrivbord är kopplad till Bolagets backuprutiner för att data inte ska gå förlorad.

2.9. Kommunikation

Samtlig intern och extern kommunikation ska ske via de kanaler och IT-resurser som
tilldelats av Bolaget.

Medarbetare ska tänka på och vara medvetna om att de kommunicerar i Bolagets namn när Bolaget står som. Vid kommunikation via Bolagets tilldelade kanaler ska Bolaget säkerställa lämplig skyddsnivå såsom säker inloggning, spårning, backup, kryptering, etc.

2.10. Internet

Internet är avsett att användas för informationssökning och andra relevanta ändamål inom och för Bolagets verksamhet. Internet skall användas med sunt förnuft och gott omdöme.

Det är inte tillåtet att ladda ner filer eller program samt klicka på länkar, vare sig på hemsidor eller i mail, som kan påverka Bolagets IT-säkerhet.

Det är inte tillåtet att besöka sajter vars innehåll bryter mot Bolagets etiska regler. Detta kan till exempel vara sajter med rasistiskt, pornografiskt eller politiskt extremt innehåll etc. Detsamma gäller för sajter som innehåller någon form av olaglig eller brottslig information.

Det är inte tillåtet att sprida information på exempelvis forum eller liknande där det kan råda oklarhet i om du som individ företräder Bolaget eller inte.

Det är inte tillåtet att sprida och/eller förfoga över upphovsrättsligt skyddat material utan rättighetsinnehavarens tillstånd (exempelvis bild och textmaterial).

2.11. Mobiltelefoni och mobila enheter

Bolagets medarbetare ska hantera mobila enheter som telefoner, bärbara dator, digitala plattor etc. med största varsamhet och försiktighet då enheterna innehåller känslig information och kan ha hög åtkomst till hela Bolagets IT-miljö.

2.12. Privat användning av IT-resurser

Användare har fått tillgång till IT-resurser för att underlätta deras arbete för Bolaget och resurserna får inte missbrukas. Emellertid är privat användning acceptabelt under förutsättning att;

- Användningen inte stör några direkta eller indirekta åtaganden med eller för Bolaget.
- Användningen inte medför några kostnader för Bolaget.
- Användningen följer reglerna i denna policy.

2.13. Förlust eller skada

Vid förlust, misstanke om obehörig användning eller skada på företagets IT-resurser ska detta omgående meddelas till närmaste chef som i sin tur rapporterar till lokal IT-avdelningen/ansvarig för lämplig åtgärd.

2.14. Återlämnande av IT-resurser

Vid anställningens upphörande skall den anställde återlämna alla IT-resurser och annan egendom, handlingar, lagringsmedia och information som framtagits eller erhållits under anställningen i Bolaget.

2.15. IT-säkerhet

Ansvaret för Bolagets IT-säkerhet är tilldelat chefen för IT-funktionen på koncernnivå. Detta ansvar omfattar:

- Skydd mot intrång.
- Grundläggande skydd för information som lagras i system inom Bolagets centrala driftsmiljö.
- Säkerställa att leverantörer av centralt upphandlade IT-tjänster svarar upp mot koncernens krav på informationssäkerhet avseende både data och fysisk säkerhet (ex. skydd av datahallar).
- Säkerställa att kommunikationslösningar uppfyller säkerhets och tillgänglighetskrav.

IT-funktionen har möjlighet att styra åtkomst och behörigheter till kommunikationsnät i syfte att skydda verksamheten samt vid behov begränsa

åtkomst både på individ- och gruppnivå till alla IT-system och relaterad infrastruktur.

3. MÅLGRUPP

Denna policy ska tillämpas av samtliga bolag inom Sdiptech koncernen.

4. ROLLER OCH ANSVAR

Sdiptech koncernens CEO är ansvarig för denna policy.

5. UNDANTAG

Det finns inga avsteg från denna policy.

6. EFTERLEVNAD

- Riskbedömning vilken inkluderar IT rapporteras årligen till revisionskommittén och styrelsen.
- En självutvärdering av minimikrav avseende IT-kontroller utförs årligen och rapporteras till revisionskommittén och styrelsen
- CFO rapporterar årligen policyöverensstämmelse till styrelsen.
- Granskning och uppdatering av policyn genomförs årligen.
- System ska förvaltas i enlighet med verksamhetens krav.
- Ett register över IT-tillgångar ska finnas dokumenterat.
- IT-processer för förvaltning av kritiska system ska finnas dokumenterade.
- En kontinuitets- och katastrofplan för Bolaget ska finnas dokumenterad.

7. HÄNVISNING TILL DOKUMENT

- Sdiptechs Code of Conduct
- Sdiptechs Kommunikations policy
- Sdiptechs Informationssäkerhetspolicy
- Sdiptechs Integritetspolicy
- Sdiptech kontinuitets och katastrofplan

Förutom denna policy ska systemägare upprätta instruktioner för hur arbetet med hantering av IT-system genomförs i den löpande verksamheten.

8. LÄNKAR

Inga

Historik över ändringar i dokumentet

Date	Amendment	Approved by:
2020-11-25	2.1 Nytt avsnitt, IT-styrning	
2020-11-25	2.2 Nytt avsnitt, IT-strategi	
2020-11-25	2.3 Nytt avsnitt, Risk management	