Operativ Informationssäkerhetspolicy för Exempelföretaget ABC

Version: 1.0 **Datum:** 2025-04-10 **Godkänd av:** Ledningsgruppen

1. Inledning och Syfte (Strategiskt)

Informationssäkerhet är en grundläggande och kritisk komponent för Exempelföretaget ABC:s framgång, rykte och fortsatta verksamhet. Denna policy *ska* utgöra grunden för hur vi skyddar våra informationstillgångar – från kunddata och affärshemligheter till personuppgifter och intern kommunikation. Varje medarbetare *måste* vara medveten om sitt ansvar och aktivt bidra till en säker arbetsmiljö. Att upprätthålla hög säkerhet är *inte* en engångsinsats, utan en kontinuerlig process som kräver vaksamhet från alla. Syftet med policyn är att ge tydlig vägledning för det dagliga arbetet och säkerställa att alla förstår vikten av att skydda företagets information.

2. Omfattning

Denna policy gäller för samtliga anställda, konsulter, praktikanter och inhyrd personal som har tillgång till Exempelföretaget ABC:s informationssystem, nätverk och data, oavsett var arbetet utförs (på kontoret, hemifrån eller på annan plats).

3. Riktlinjer för Dagligt Arbete (Operativt)

För att upprätthålla en god cybersäkerhetsnivå i det dagliga arbetet gäller följande:

- **3.1 Åtkomst och Lösenord:**
    - Ditt lösenord är personligt. Dela *aldrig* ditt lösenord med någon annan, varken internt eller externt.
    - Lösenord *ska* vara komplexa (innehålla stora och små bokstäver, siffror och specialtecken) och bytas regelbundet enligt IT-avdelningens instruktioner.
    - Du *bör* aktivera multifaktorautentisering (MFA) där det erbjuds.
    - Logga ut eller lås din datorskärm när du lämnar din arbetsplats, även för korta pauser. Detta *måste* göras för att förhindra obehörig åtkomst.
- **3.2 E-post och Kommunikation:**
    - Var kritisk till e-postmeddelanden, särskilt de som innehåller länkar eller bilagor, eller som uppmanar till brådskande handlingar gällande känslig information. Klicka *ej* på misstänkta länkar och öppna inte oväntade bilagor.
    - Skicka *inte* känslig eller konfidentiell information via okrypterad e-post. Använd företagets godkända verktyg för säker kommunikation.
    - Du *behöver* vara extra uppmärksam på avsändaradressen vid extern kommunikation för att undvika nätfiske (phishing).
- **3.3 Fysisk Säkerhet:**
    - Lämna *inte* känsliga dokument synliga på skrivbordet när du lämnar det obevakat. Förvara dem inlåsta.
    - Var uppmärksam på okända personer i företagets lokaler. Besökare *ska* alltid anmälas och bära synlig besöksbricka.

    - Se till att dörrar till säkra utrymmen hålls stängda och låsta.

- **3.4 Användning av Utrustning och Programvara:**
    - Använd endast utrustning (datorer, mobiler etc.) och programvara som är godkänd av Exempelföretaget ABC.
    - Installation av icke-godkänd programvara eller anslutning av privat utrustning till företagets nätverk utan tillstånd är strängt *förbjuden*.
    - Håll operativsystem och programvara uppdaterade enligt IT-avdelningens riktlinjer. Detta *skall* göras för att skydda mot kända sårbarheter.

4. Datahantering och Klassificering (Strategiskt och Operativt)

All information som hanteras inom Exempelföretaget ABC har ett värde och *behöver* skyddas utifrån dess känslighet. Informationen *ska* klassificeras och hanteras enligt företagets interna riktlinjer för dataklassificering och gällande lagstiftning (t.ex. GDPR). Lagring av känslig företagsinformation på privata enheter eller molntjänster är som huvudregel *inte* tillåten.

5. Incidentrapportering

Alla misstänkta eller konstaterade säkerhetsincidenter (t.ex. misstänkt intrång, förlorad utrustning, virusinfektion, misstänkt nätfiske) *skall* omedelbart rapporteras till IT-avdelningen eller närmaste chef enligt gällande incidenthanteringsrutin. Snabb rapportering är avgörande för att minimera eventuell skada.

6. Ansvar och Efterlevnad (Strategiskt)

Varje anställd *är* personligt ansvarig för att följa denna policy. Chefer *har* ett särskilt ansvar att säkerställa att deras medarbetare känner till, förstår och följer policyn. IT-avdelningen ansvarar för att tillhandahålla nödvändiga tekniska skydd och stöd. Medveten eller upprepad överträdelse av denna policy kan leda till disciplinära åtgärder. Att upprätthålla säkerheten är *inte* valfritt, det är en förutsättning för vår verksamhet.

7. Granskning och Uppdatering

Denna policy *skall* granskas minst en gång per år, eller oftare vid behov (t.ex. vid förändringar i hotbild, teknologi eller lagstiftning), för att säkerställa att den förblir relevant och effektiv.

8. Kontakt

Vid frågor kring denna policy eller osäkerhet kring informationssäkerhet, kontakta IT-supporten eller din närmaste chef. Du *behöver* inte tveka att fråga om något är oklart.