Informationssäkerhetspolicy för Exempelföretaget ABC

Version: 2.0 **Datum:** 2025-04-10 **Godkänd av:** Ledningsgruppen

1. Vision och Strategiskt Åtagande

Exempelföretaget ABC:s vision är att [infoga företagets övergripande vision, t.ex. "vara den mest innovativa och pålitliga partnern inom vår bransch"]. För att uppnå detta är förtroende från våra kunder, partners och medarbetare avgörande. Informationssäkerhet är inte bara en teknisk fråga, utan en **strategisk grundpelare** för att bygga och bibehålla detta förtroende, skydda vårt varumärke och säkerställa vår långsiktiga konkurrenskraft och framgång.

Vi åtar oss att:

- **Integrera informationssäkerhet** som en naturlig del i alla verksamhetsprocesser och beslut.
- **Proaktivt identifiera och hantera risker** relaterade till våra informationstillgångar.
- **Säkerställa konfidentialitet, riktighet och tillgänglighet** för all information vi hanterar.
- **Uppfylla eller överträffa** legala, regulatoriska och avtalsmässiga krav på informationssäkerhet.
- **Främja en stark säkerhetskultur** där varje medarbetare förstår vikten av och aktivt bidrar till informationssäkerheten.

Vårt långsiktiga mål är att informationssäkerhet ska vara en **affärsmöjliggörare**, som stödjer innovation och effektivitet utan att kompromissa med skyddet av våra värdefulla tillgångar.

2. Syfte och Omfattning

Syftet med denna policy är att definiera ramverket och de grundläggande kraven för informationssäkerhet inom Exempelföretaget ABC. Den syftar till att ge både strategisk vägledning och konkreta operativa regler för att skydda företagets informationstillgångar.

Policyn omfattar all information som ägs, hanteras eller lagras av Exempelföretaget ABC, oavsett format eller plats. Den gäller för samtliga anställda, ledning, styrelse, konsulter, praktikanter och tredjepartsleverantörer som har tillgång till företagets information eller system.

3. Grundläggande Säkerhetsprinciper (Strategisk grund för operationella regler)

All hantering av information och system inom Exempelföretaget ABC ska vägledas av följande principer:

- **Konfidentialitet:** Information ska endast vara tillgänglig för behöriga individer.
- **Riktighet (Integritet):** Information ska vara korrekt, fullständig och skyddad mot otillåten ändring eller radering.
- **Tillgänglighet:** Information och tillhörande system ska vara tillgängliga för behöriga användare när de behövs.
- **Minsta möjliga behörighet:** Användare ska endast tilldelas de behörigheter som är nödvändiga för att utföra sina arbetsuppgifter.
- **Riskbaserat förhållningssätt:** Säkerhetsåtgärder ska baseras på en bedömning av risker och anpassas efter informationens värde och känslighet.

- **Ansvarsskyldighet:** Alla handlingar ska kunna spåras till en ansvarig individ eller process.

4. Operativa Riktlinjer och Ansvar (Dagligt arbete)

För att uppfylla våra strategiska mål och principer krävs följande av varje medarbetare i det dagliga arbetet:

- **4.1 Användarkonton och Lösenord:**
    - Ditt användarkonto är personligt och får inte delas. Du är ansvarig för all aktivitet som sker via ditt konto.
    - Använd starka, unika lösenord för alla system och byt dem enligt företagets riktlinjer. Aktivera multifaktorautentisering (MFA) där det är tillgängligt. Detta är en grundläggande åtgärd för att skydda både din och företagets information (*Konfidentialitet*).
    - Lås din dator och mobila enheter när du lämnar dem utan uppsikt.
- **4.2 E-post och Kommunikation:**
    - Var kritisk mot oväntad eller misstänkt e-post, särskilt gällande länkar och bilagor (nätfiske). Verifiera avsändarens identitet vid osäkerhet. Felaktig hantering kan leda till intrång och skada företagets *rykte*.
    - Skicka känslig eller konfidentiell information endast via godkända, säkra kanaler (t.ex. krypterad e-post).
- **4.3 Fysisk Säkerhet:**
    - Skydda fysiska dokument och lagringsmedia från obehörig åtkomst. Förvara känsligt material inlåst när det inte används.
    - Var uppmärksam på din omgivning och rapportera okända personer eller misstänkta aktiviteter i företagets lokaler. Bidra till att upprätthålla skalskyddet.
- **4.4 Användning av Utrustning och Programvara:**
    - Använd endast utrustning och programvara som tillhandahålls och godkänts av Exempelföretaget ABC för arbetsändamål.
    - Installation av icke-godkänd programvara är förbjuden då den kan introducera sårbarheter som hotar *alla* våra säkerhetsprinciper.
    - Håll system och programvara uppdaterade enligt IT-avdelningens instruktioner.
- **4.5 Hantering av Information:**
    - Hantera all företagsinformation (inklusive kunddata, personaldata, affärshemligheter) med lämplig sekretess och i enlighet med dess klassificering och gällande lagstiftning (t.ex. GDPR). Detta är avgörande för att uppfylla vårt *strategiska åtagande* om förtroende och regelefterlevnad.
    - Lagra eller behandla inte företagsinformation på privata enheter eller osäkra molntjänster utan uttryckligt godkännande.

    - Säkerställ korrekt radering eller destruktion av information när den inte längre behövs.

- **4.6 Distansarbete:**
    - Vid arbete utanför kontoret, säkerställ att du använder en säker nätverksanslutning (t.ex. VPN) och att din arbetsmiljö skyddar information från obehörig insyn. Flexibilitet får inte ske på bekostnad av säkerhet.

5. Incidenthantering

Alla misstänkta eller faktiska informationssäkerhetsincidenter (t.ex. virus, dataintrång, förlorad utrustning, misstänkt obehörig åtkomst) ska omedelbart rapporteras till IT-avdelningen eller närmaste chef enligt gällande rutin. Snabb och korrekt hantering är kritisk för att minimera skada och säkerställa *verksamhetens kontinuitet*.

6. Utbildning och Medvetenhet

Exempelföretaget ABC ser utbildning och medvetandehöjning som en **strategisk investering** i vår säkerhet. Alla medarbetare är skyldiga att delta i obligatorisk säkerhetsutbildning och att hålla sig informerade om gällande policyer och rutiner. En medveten personal är vår viktigaste försvarslinje.

7. Efterlevnad och Konsekvenser

Efterlevnad av denna policy är obligatorisk för alla som omfattas av den. Brott mot policyn kan leda till disciplinära åtgärder, inklusive varning, omplacering eller uppsägning/avslutat uppdrag, samt eventuella rättsliga påföljder. Bristande efterlevnad riskerar inte bara operativa störningar utan kan allvarligt skada företagets *strategiska tillgångar* som varumärke och kundförtroende.

8. Policyöversyn och Kontinuerlig Förbättring

Denna policy ska ses över minst årligen, eller vid behov, av ansvarig funktion (t.ex. Informationssäkerhetsrådet eller IT-chefen) för att säkerställa att den är aktuell, relevant och effektivt stödjer företagets *strategiska mål* och anpassas till en föränderlig omvärld och hotbild. Förslag till förbättringar uppmuntras.

9. Kontaktinformation

Vid frågor om denna policy eller för att rapportera en incident, vänligen kontakta:

- IT-supporten: [Telefonnummer], [E-postadress]
- Informationssäkerhetsansvarig: [Namn], [E-postadress]
- Din närmaste chef