Informationssäkerhetspolicy

*Denna mall tillhandahålls i befintligt skick och är endast avsedd som vägledning. ChainSec lämnar inga garantier, uttryckliga eller underförstådda, gällande mallens innehåll, korrekthet eller lämplighet för specifika ändamål. Vi tar inget ansvar för eventuella direkta eller indirekta skador som kan uppstå vid användning av mallen.*

*Det är organisationens eget ansvar att säkerställa att den resulterande policyn är korrekt utformad, juridiskt giltig och uppfyller alla relevanta krav och standarder. Vi rekommenderar att professionell rådgivning eller expertis inom området anlitas vid implementering av policyn.*

## § 1. Inledning och syfte

Denna policy har tagits fram av [organisationens namn] med organisationsnummer [\_\_] för att skapa en säker arbetsplats med hög informationssäkerhetsnivå.

Policyn syftar till att:

* Säkerställa att informationen alltid är tillgänglig när den behövs.
* Skydda informationens integritet genom att förhindra manipulation och förstörelse.
* Begränsa åtkomst till endast behöriga personer.

Policyn beskriver riktlinjer och mål för informationssäkerhetsarbetet på arbetsplatsen.

## § 2. Giltighet

Denna policy gäller för alla medarbetare samt för extern personal som utför arbete på uppdrag.

Den omfattar all teknik och alla typer av informationstillgångar på arbetsplatsen, oavsett om de hanteras manuellt eller digitalt, samt lagras elektroniskt, fysiskt eller i andra format.

## § 3. Ansvar

#### a) **Ledningen**

Ledningsgruppen ansvarar för att:

[Ange specifika ansvarsområden, t.ex. fastställa resurser för informationssäkerhet, besluta om övergripande säkerhetsmål eller övervaka efterlevnad av policyn.]

#### b) **Chefer**

Chefen/cheferna ansvarar för att:

[Ange specifika ansvarsområden, t.ex. implementera säkerhetsåtgärder inom sina avdelningar, utbilda medarbetare i informationssäkerhet eller rapportera säkerhetsincidenter till ledningen.]

#### c) **Medarbetare**

Medarbetarna ansvarar för att:

[Ange specifika ansvarsområden, t.ex. följa fastställda säkerhetsrutiner, rapportera säkerhetsbrister eller incidenter eller delta i obligatorisk säkerhetsutbildning.]

## § 4. Riskanalys

För att säkerställa en hög informationssäkerhetsnivå ska säkerhetsåtgärder baseras på en riskanalys.

Riskanalysen ska:

* Identifiera potentiella hot mot informationssäkerheten i verksamheten.
* Analysera konsekvenserna för varje identifierat hot.
* Bedöma risken för skada och sannolikheten för att hotet inträffar.

[Lägg till eller justera dessa punkter beroende på vilka ramverk (t.ex. ISO 27001 eller annan standard) eller metoder organisationen använder.]

På arbetsplatsen ska en riskanalys gällande informationssäkerheten genomföras enligt följande regelbundenhet: [Tidpunkt/frekvens för uppdatering]

Riskanalysen ska genomföras av följande person/-er: [Ange roll eller person, t.ex. IT-säkerhetschef, Riskanalytiker eller annan ansvarig]

## § 5. Principer

Följande principer ska ligga till grund för arbetet med informationssäkerhet på arbetsplatsen:

[Ange och anpassa principerna nedan efter organisationens behov och prioriteringar. Dessa kan ändras eller utökas baserat på verksamhetens unika krav.]

* Allt arbete ska följa gällande regler och lagar.
* Information ska klassificeras utifrån konfidentialitetsnivå.
* IT-system och IT-tjänster ska klassificeras utifrån konfidentialitetsnivå.
* Information och IT-system ska skyddas mot obehörig åtkomst med skyddsnivåer anpassade efter informationens känslighet.
* Kostnader för skyddsåtgärder ska balanseras mot värdet av det som skyddas.
* Alla medarbetare och eventuella konsulter ska ha tillräcklig kunskap i informationssäkerhet, anpassad efter deras arbetsuppgifter, för att säkerställa att önskad säkerhetsnivå kan upprätthållas.

## § 6. Säkerhetsåtgärder

#### a) **IT-säkerhet**

För att upprätthålla en hög nivå av IT-säkerhet ska följande åtgärder vidtas:

[Ange specifika säkerhetsåtgärder, t.ex. användning av brandväggar, antivirusprogram, regelbundna säkerhetsuppdateringar eller kryptering av känsliga data.]

#### b) **Fysisk säkerhet**

För att upprätthålla en hög nivå av fysisk säkerhet ska följande åtgärder vidtas:

[Ange specifika säkerhetsåtgärder, t.ex. tillgångsbegränsningar med passerkort, övervakningskameror eller säker förvaring av känslig information i låsta utrymmen.]

#### c) **Personalsäkerhet**

För att säkerställa att personalen hanterar information på ett säkert och ansvarsfullt sätt ska följande åtgärder vidtas:

[Ange specifika åtgärder, t.ex. bakgrundskontroller vid nyanställningar, regelbunden utbildning i informationssäkerhet eller rutiner för att granska och uppdatera behörigheter.]

## § 7. Incidenthantering

Om en incident som påverkar informationssäkerheten inträffar ska följande åtgärder vidtas:

[Anpassa åtgärderna nedan efter organisationens specifika processer och behov. Dessa kan ändras eller utökas vid behov.]

* Incidenten ska rapporteras omedelbart till ansvarig chef eller IT-avdelningen.
* En utredning ska genomföras för att fastställa orsaken till incidenten.
* Vid behov ska åtgärder vidtas för att begränsa skadan och återställa normal drift.
* En rapport om incidenten och dess hantering ska arkiveras för framtida referens och lärdomar.

##

## § 8. Överträdelse

Bryter någon mot denna policy ska det hanteras enligt följande:

[Ange specifika åtgärder, t.ex. varning, disciplinära åtgärder, utbildning eller rapportering till ansvarig chef/avdelning.]

## § 9. Policyförvaltning

#### Ansvar och kontroll

[Ange roll/funktion] ansvarar för att kontrollera att verksamheten följer policyn samt regler och lagar på området.

Kontroll sker genom följande aktiviteter:

[Ange specifika aktiviteter, t.ex. regelbundna revisioner, stickprovskontroller, rapportering av avvikelser eller uppföljningsmöten.]

#### Tillgänglighet och kommunikation

Denna policy ska finnas tillgänglig för samtliga medarbetare på följande platser:

[Ange specifika platser, t.ex. intranät, fysisk pärm i receptionen eller annat relevant format. Anpassa och lägg till enligt organisationens behov.]

#### Uppdatering och versionshantering

Denna policy ska uppdateras:

* När? [Ange frekvens, t.ex. årligen, vid behov eller efter större förändringar i verksamheten eller lagkrav.]
* Hur? [Ange metod, t.ex. genom en dedikerad granskningsprocess eller vid ledningsmöten.]
* Av vem? [Ange ansvarig roll eller funktion, t.ex. säkerhetschef, IT-avdelning eller compliance-ansvarig.]

Uppdateringar meddelas berörda parter genom: [Ange metoder, t.ex. e-postutskick, interna möten eller notifikationer på intranätet.]

Dokumentation av ändringar ska innehålla: [Ange vad dokumentationen ska omfatta, t.ex. datum för ändringen, vem som gjorde ändringen och en beskrivning av vad som ändrats.]

## Bilaga 1: Definitioner

Denna bilaga innehåller förklaringar av de termer som används i Informationssäkerhetspolicyn. Syftet är att säkerställa en enhetlig tolkning.

**Extern personal**

Personer som arbetar på arbetsplatsen på uppdrag men som inte är anställda av organisationen.

**Fysisk säkerhet**

Åtgärder för att förhindra obehörig åtkomst till områden, lokaler, byggnader och andra platser där skyddsklassificerad eller konfidentiell information hanteras.

**Personalsäkerhet**

Åtgärder för att säkerställa att personal som hanterar eller har tillgång till känslig information är pålitlig, har rätt kompetens och utbildning, samt att deras behörigheter granskas och uppdateras regelbundet.

**Informationsrisk**

Hot som kan leda till att information sprids, förstörs eller förvanskas, vilket kan påverka verksamhetens integritet, tillgänglighet eller konfidentialitet.

**Informationssäkerhet**

Åtgärder och processer som säkerställer att information är tillgänglig vid behov, skyddad mot manipulation, förlust och obehörig åtkomst.

**Informationstillgångar**

Alla resurser som används för att hantera och lagra information, såsom datorer, databaser, nätverk, dokument, system och andra digitala eller analoga tillgångar.

**IT-säkerhet**

Skydd av elektronisk information och IT-relaterade resurser genom rutiner, tekniska lösningar och åtgärder för att förhindra obehörig åtkomst, manipulation eller förlust.

**Ledning**

Gruppen av personer som har övergripande ansvar för att fatta beslut inom organisationen. Ledningen utses av styrelsen.

**Medarbetare**

Personer som är anställda av organisationen och som arbetar på arbetsplatsen.

**Personalsäkerhet**

Åtgärder för att säkerställa att personal som har tillgång till känslig information har rätt kompetens, bakgrund och utbildning, samt att behörigheter regelbundet ses över.

**Incidenthantering**

Processen för att identifiera, rapportera, analysera och åtgärda säkerhetsincidenter som påverkar informationstillgångar eller IT-system, för att minimera skador och förhindra framtida incidenter.

**Policyförvaltning**

Rutin och ansvar för att upprätthålla, uppdatera och kommunicera policyn för att säkerställa att den förblir relevant och efterlevs av alla medarbetare och externa parter.

**Tillgänglighet**

Att information och system är tillgängliga och användbara när de behövs av behöriga personer, utan avbrott.

**Konfidentialitet**

Skydd av information för att säkerställa att den endast är tillgänglig för behöriga personer och inte röjs för obehöriga.

**Integritet**

Säkerställande av att information är korrekt, fullständig och skyddad mot oavsiktliga eller avsiktliga ändringar.