Incidenthanteringsplan

*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. Förberedelse

### 1.1 Roller och ansvar

Incidenthanteringsteamet utgör kärnan i organisationens incidenthanteringsförmåga. Teamet består av dedikerade resurser med specifika roller och ansvarsområden för att säkerställa effektiv hantering av säkerhetsincidenter.

#### Kärnroller och kontaktvägar

| Roll | Huvudansvar | Primär kontakt | Sekundär kontakt |
| --- | --- | --- | --- |
| Incidentsamordnare | Leder incidenthantering, Beslutar om eskalering, Rapporterar till ledning | [Namn, Tel, Email] | [Namn, Tel, Email] |
| Teknisk analytiker | Teknisk analys, Implementerar åtgärder, Systemövervakning | [Namn, Tel, Email] | [Namn, Tel, Email] |
| Forensiker | Digital bevisinsamling, Teknisk spårning, Dokumentation | [Namn, Tel, Email] | [Namn, Tel, Email] |

Vid hantering av incidenter är det kritiskt att rätt personer involveras vid rätt tidpunkt. Nedan beskrivs eskaleringsprocessen för olika typer av incidenter.

#### Eskaleringsvägar

| Eskaleringsnivå | Kontakt | När ska eskalering ske |
| --- | --- | --- |
| Nivå 1 - Initial | [Namn, Tel, Email] | Vid första indikation på incident, När incident bekräftats, Vid osäkerhet om omfattning |
| Nivå 2 - Teknisk | [Namn, Tel, Email] | Vid behov av specialistkompetens, Vid omfattande systemstörningar, Vid risk för spridning |
| Nivå 3 - Ledning | [Namn, Tel, Email] | Vid kritisk verksamhetspåverkan, Vid behov av större resurser, Vid extern påverkan/media |

### 1.2 Resursinventering

För att effektivt kunna hantera incidenter krävs en tydlig bild av organisationens kritiska system och tillgångar. Denna inventering uppdateras regelbundet och innehåller information om systemägare, klassificering och beroenden.

#### Systeminventering

Nedan listas organisationens mest kritiska system med tillhörande information:

| System | Klassificering | Systemägare | Driftansvarig | Kritiska beroenden |
| --- | --- | --- | --- | --- |
| Ekonomisystem | Hög | [Namn, Tel, Email] | [Namn, Tel, Email] | Databas X, Integrationer Y & Z, Backupsystem |
| Kundregister | Hög | [Namn, Tel, Email] | [Namn, Tel, Email] | AD-koppling, Backup, Webbgränssnitt |
| Produktionsystem | Kritisk | [Namn, Tel, Email] | [Namn, Tel, Email] | Processnätverk, Styrsystem, Databaser |
| Intranet | Medel | [Namn, Tel, Email] | [Namn, Tel, Email] | Filserver, AD-koppling |

Systemens kritikalitet är bedömd utifrån påverkan på verksamheten vid eventuellt avbrott eller intrång. Särskild hänsyn har tagits till:

* Verksamhetskritiska processer
* Regulatoriska krav
* Kundpåverkan
* Ekonomisk påverkan

#### Datakategorisering

Organisationens information är kategoriserad enligt följande för att säkerställa rätt skyddsnivå:

| Kategori | Klassificering | Hanteringskrav | Lagringsplats | Ansvarig |
| --- | --- | --- | --- | --- |
| Personuppgifter | Hög | Krypterad lagring, Åtkomstkontroll, Loggning | [System/Plats] | [Namn, Roll] |
| Kunddata | Hög | Säkerhetskopiering, Behörighetsstyrning | [System/Plats] | [Namn, Roll] |
| Ekonomidata | Kritisk | Daglig backup, Revisionsspår | [System/Plats] | [Namn, Roll] |
| Teknisk dokumentation | Medel | Versionshantering, Backup | [System/Plats] | [Namn, Roll] |

För varje datakategori finns detaljerade hanteringsrutiner som beskriver:

* Krav på åtkomstkontroll
* Backuprutiner
* Krypteringskrav
* Gallringsrutiner

## 2. Förebyggande åtgärder

### 2.1 Systematiskt arbete

Det förebyggande säkerhetsarbetet syftar till att minimera risken för incidenter och begränsa eventuell skada när incidenter inträffar. Arbetet baseras på regelbunden riskanalys och implementering av säkerhetskontroller inom både tekniska och organisatoriska områden.

#### Grundprinciper för förebyggande arbete:

* Försvarsstrategi på djupet (flera säkerhetslager)
* Löpande uppdatering och patchning
* Principen om minsta möjliga behörighet
* Kontinuerlig övervakning och loggning
* Regelbunden säkerhetsutbildning
* Dokumenterade rutiner och processer

### 2.2 Kritiska säkerhetsåtgärder

Följande åtgärder ska prioriteras i det förebyggande arbetet:

| Kategori | Åtgärd | Frekvens | Ansvarig | Uppföljning |
| --- | --- | --- | --- | --- |
| Teknisk Säkerhet | Sårbarhetsscanning | Månadsvis | IT-säkerhet | Rapport till CISO |
| Systemmiljö | Säkerhetspatchar | Veckovis | IT-drift | Patchrapport |
| Användare | Säkerhetsutbildning | Årligen | HR/Säkerhet | Utbildningsstatistik |
| Behörigheter | Behörighetsgenomgång | Kvartalsvis | Systemägare | Access-rapport |
| Övervakning | SIEM/IDS-översyn | Löpande | SOC | Månadsrapport |

### 2.3 Riskbaserad prioritering

Förebyggande åtgärder prioriteras baserat på:

1. Potentiell påverkan på verksamheten
2. Sannolikhet för incident
3. Kostnad vs nytta för åtgärden
4. Regulatoriska krav
5. Teknisk genomförbarhet

#### Riskbedömningsmatris

| Sannolikhet/Påverkan | Låg påverkan | Medel påverkan | Hög påverkan |
| --- | --- | --- | --- |
| Hög sannolikhet | Medel prio | Hög prio | Akut prio |
| Medel sannolikhet | Låg prio | Medel prio | Hög prio |
| Låg sannolikhet | Låg prio | Låg prio | Medel prio |

### 2.4 Övervakning och kontroller

#### Tekniska kontroller

* Nätverksövervakning (IDS/IPS)
* Endpoint protection
* Logganalys och korrelation
* Accesskontroll och MFA
* Kryptering av känslig data

#### Administrativa kontroller

* Policyer och rutiner
* Utbildning och medvetenhet
* Behörighetshantering
* Ändringshantering
* Leverantörskontroll

### 2.5 Mätning och uppföljning

Effektiviteten i det förebyggande arbetet mäts genom:

| Mätetal | Målvärde | Mätfrekvens | Rapportering |
| --- | --- | --- | --- |
| Antal kritiska sårbarheter | Max 5 | Månadsvis | IT-ledning |
| Patchtid kritiska system | Max 7 dagar | Månadsvis | CISO |
| Utbildningsgenomförande | Min 95% | Kvartalsvis | Ledningsgrupp |
| Incidenter per kvartal | Max 10 | Kvartalsvis | Styrelse |
| Upptäcktstid (MTTD) | Max 24h | Löpande | SOC |

Det förebyggande arbetet utvärderas kvartalsvis och justeras baserat på:

* Inträffade incidenter
* Nya eller förändrade hot
* Verksamhetsförändringar
* Resultat från säkerhetstester
* Upptäckta sårbarheter

## 3. Identifiering

### 3.1 Detektionssystem

Organisationen använder flera olika tekniska system och rutiner för att upptäcka säkerhetsincidenter. En kombination av automatiserad övervakning och manuell granskning används för att säkerställa effektiv detektion.

#### Säkerhetsövervakning

Följande system utgör grunden i vår säkerhetsövervakning:

| System | Syfte | Placering | Ansvarig | Backup |
| --- | --- | --- | --- | --- |
| SIEM | Centraliserad logganalys | [Nätsegment] | [Namn, Roll] | [Namn, Roll] |
| IDS/IPS | Intrångsdetektering | [Nätsegment] | [Namn, Roll] | [Namn, Roll] |
| Antivirus | Endpoint-skydd | [Omfattning] | [Namn, Roll] | [Namn, Roll] |
| Brandvägg | Nätverkssegmentering | [Nätsegment] | [Namn, Roll] | [Namn, Roll] |

Övervakningssystemen är konfigurerade för att:

* Generera realtidsvarningar vid kritiska händelser
* Samla forensisk data för efteranalys
* Möjliggöra korrelation mellan olika händelser
* Skapa trendanalyser och rapporter

#### Logghantering

Systematisk logghantering är kritisk för att kunna upptäcka och analysera incidenter:

| Källa | Typ av data | Retentionstid | Granskning |
| --- | --- | --- | --- |
| Windows Events | Säkerhetshändelser | 180 dagar | Daglig |
| Brandväggsloggar | Nätverkstrafik | 90 dagar | Veckovis |
| Accessloggar | Inloggningar | 365 dagar | Daglig |
| Systemloggar | Drifthändelser | 90 dagar | Veckovis |

### 3.2 Incidentklassificering

För att säkerställa effektiv respons klassificeras incidenter baserat på allvarlighetsgrad och påverkan på verksamheten.

#### Prioritetsnivåer

Incidenter kategoriseras enligt följande prioritetsnivåer:

| Nivå | Beskrivning | Exempel |
| --- | --- | --- |
| P1 - Kritisk | Allvarlig påverkan på verksamheten | Ransomware, Totalt systemavbrott |
| P2 - Hög | Betydande påverkan på delar av verksamheten | Dataintrång, Omfattande malware |
| P3 - Medel | Begränsad påverkan | Enstaka malware, Phishing-försök |
| P4 - Låg | Minimal påverkan | Enstaka spam, Policyöverträdelser |

Vid bedömning av incidentens allvarlighetsgrad tas hänsyn till:

* Påverkan på verksamhetskritiska processer
* Antal påverkade system och användare
* Typ av information som kan vara komprometterad
* Risk för spridning inom organisationen

#### Påverkansbedömning

För varje incident görs en bedömning av påverkan inom följande områden:

| Faktor | Bedömning |
| --- | --- |
| Konfidentialitet | Ingen/Låg/Medel/Hög påverkan på informationssäkerhet |
| Riktighet | Ingen/Låg/Medel/Hög påverkan på datakvalitet |
| Tillgänglighet | Ingen/Låg/Medel/Hög påverkan på systemtillgänglighet |
| Spårbarhet | Ingen/Låg/Medel/Hög påverkan på granskningsförmåga |

## 4. Respons

### 4.1 Initial respons

När en incident upptäcks är de första åtgärderna kritiska för att begränsa eventuell skada och säkerställa effektiv hantering. Följande steg ska genomföras:

1. Bekräfta och dokumentera incidenten
   * Samla initial information
   * Dokumentera tidpunkt och upptäcktsmetod
   * Säkra preliminära bevis
2. Utför initial klassificering enligt prioritetsnivåerna:

| Åtgärd | P1 - Kritisk | P2 - Hög | P3 - Medel | P4 - Låg |
| --- | --- | --- | --- | --- |
| Initial respons | Omedelbar | Inom 30 min | Inom 2h | Inom 8h |
| Eskalering | Direkt till ledning | Till ansvarig chef | Till teamledare | Inom teamet |
| Rapportering | Direkt | Inom 1h | Inom 4h | Inom 24h |

### 4.2 Teknisk analys

Den tekniska analysen syftar till att:

* Fastställa incidentens omfattning
* Identifiera påverkade system
* Kartlägga spridningsrisk
* Samla teknisk bevisning

#### Analyssteg

| Steg | Syfte | Ansvarig | Verktyg/Metod |
| --- | --- | --- | --- |
| Initial scanning | Identifiera omfattning | [Roll] | [Verktyg] |
| Logganalys | Kartlägga händelseförlopp | [Roll] | [Verktyg] |
| Malwareanalys | Identifiera skadlig kod | [Roll] | [Verktyg] |
| Nätverksanalys | Spåra kommunikation | [Roll] | [Verktyg] |

### 4.3 Åtgärder

Baserat på analysresultatet implementeras lämpliga åtgärder:

#### Omedelbara åtgärder

| Typ | Åtgärd | Godkännande krävs | Dokumentation |
| --- | --- | --- | --- |
| Isolering | Koppla bort system | [Roll] | [Mall/Plats] |
| Blockering | Blockera trafik/access | [Roll] | [Mall/Plats] |
| Nedstängning | Stänga av tjänst | [Roll] | [Mall/Plats] |
| Återställning | Återställa backup | [Roll] | [Mall/Plats] |

### 4.4 Kommunikation

Effektiv kommunikation är kritisk under incidenthantering. Följande kommunikationsvägar används:

#### Intern kommunikation

| Målgrupp | Kanal | Frekvens | Ansvarig |
| --- | --- | --- | --- |
| Ledning | [Kanal] | Vid statusändring | [Roll] |
| IT-personal | [Kanal] | Löpande | [Roll] |
| Berörda användare | [Kanal] | Vid behov | [Roll] |
| Övrig personal | [Kanal] | Vid större påverkan | [Roll] |

#### Extern kommunikation

| Målgrupp | När | Ansvarig | Godkännande |
| --- | --- | --- | --- |
| Myndigheter | Enligt lag/krav | [Roll] | [Roll] |
| Kunder | Vid påverkan | [Roll] | [Roll] |
| Media | Vid publik påverkan | [Roll] | [Roll] |
| Partners | Vid delad påverkan | [Roll] | [Roll] |

## 5. Återhämtning

### 5.1 Återställningsprocess

Efter att en incident har hanterats är målet att återgå till normal drift på ett säkert sätt. Processen ska säkerställa att:

* Alla system är säkrade
* Normal funktionalitet är återställd
* Risken för återkommande incident är minimerad

#### Återställningsfaser

| Fas | Aktivitet | Verifiering | Ansvarig |
| --- | --- | --- | --- |
| Förberedelse | Säkerställ backuper, Planera återställning | Backup-verifiering | [Roll] |
| Återställning | Återställ system/data, Återaktivera tjänster | Funktionstest | [Roll] |
| Verifiering | Testa funktionalitet, Säkerhetskontroll | Säkerhetsgenomgång | [Roll] |
| Övervakning | Extra övervakning, Logganalys | Avvikelseanalys | [Roll] |

### 5.2 Verifiering

För att säkerställa säker återgång till produktion genomförs följande kontroller:

| Kontrollpunkt | Metod | Acceptanskriterier | Ansvarig |
| --- | --- | --- | --- |
| Systemsäkerhet | Säkerhetsskanning | Inga kritiska sårbarheter | [Roll] |
| Dataintegritet | Dataverifiering | Data komplett och korrekt | [Roll] |
| Funktionalitet | Funktionstester | All kritisk funktionalitet OK | [Roll] |
| Prestanda | Prestandatest | Normal svarstid/kapacitet | [Roll] |

## 6. Leverantörsrelaterade incidenter

### 6.1 Omfattning

* Incidenter som påverkar leverantörer av kritiska tjänster/produkter
* Incidenter som härstammar från leverantörers system/tjänster
* Incidenter i försörjningskedjan som påverkar vår verksamhet
* Säkerhetsbrister i leverantörsprodukter

### 6.2 Kritiska leverantörskategorier

| **Kategori** | **Exempel** | **Kritikalitet** | **Primär kontakt** |
| --- | --- | --- | --- |
| Molntjänstleverantörer | [Leverantör] | Hög | [Kontakt] |
| Infrastrukturleverantörer | [Leverantör] | Kritisk | [Kontakt] |
| Mjukvaruleverantörer | [Leverantör] | Medel | [Kontakt] |
| Hårdvaruleverantörer | [Leverantör] | Medel | [Kontakt] |
| Serviceleverantörer | [Leverantör] | Hög | [Kontakt] |

### 6.3. Krav på leverantörer

#### Grundläggande krav:

* Dokumenterad incidenthanteringsprocess
* Dedikerad kontaktperson för incidenthantering
* Definierade eskaleringsvägar
* Avtalad responstid baserad på incidentens allvarlighetsgrad
* Rutiner för säker informationsdelning
* Omedelbar notifiering vid kritiska incidenter
* Statusuppdateringar enligt överenskommen frekvens
* Detaljerad incidentrapport efter avslutad incident
* Dokumentation av åtgärder och lärdomar

#### Säkerhetskrav:

* Regelbunden säkerhetsrevidering
* Uppdaterad sårbarhetshantering
* Dokumenterade återställningsrutiner
* Regelbundna säkerhetstester

## 7. Uppföljning

### 7.1 Incidentrapportering

Efter varje incident skapas en detaljerad rapport som innehåller:

* Händelseförlopp och tidslinje
* Vidtagna åtgärder
* Påverkan på verksamheten
* Lärdomar och rekommendationer

#### Rapportstruktur

| Sektion | Innehåll | Ansvarig | Deadline |
| --- | --- | --- | --- |
| Sammanfattning | Övergripande beskrivning | Incidentledare | 24h efter avslut |
| Teknisk analys | Detaljerad teknisk genomgång | Teknisk analytiker | 72h efter avslut |
| Åtgärder | Lista över genomförda åtgärder | Åtgärdsansvarig | 72h efter avslut |
| Rekommendationer | Förslag på förbättringar | Incidentteam | 5 dagar efter avslut |

### 7.2 Förbättringsprocess

Baserat på incidentrapporter genomförs regelbundna förbättringsaktiviteter:

| Aktivitet | Frekvens | Deltagare | Resultat |
| --- | --- | --- | --- |
| Incidentgenomgång | Efter varje P1/P2 | Incidentteam | Direkta åtgärder |
| Kvartalsanalys | Var 3:e månad | Säkerhetsforum | Trendanalys |
| Årlig översyn | Årligen | Ledningsgrupp | Strategiska beslut |

## 8. Bilagor och referenser

### 8.1 Kontaktlistor och eskaleringsvägar

Nedan följer uppdaterade kontaktlistor för olika situationer. Kom ihåg att alltid utgå från incidentens klassificering vid eskalering.

#### Kritiska kontakter (alltid tillgängliga)

| Roll/Funktion | Kontorstid | Jour | Alternativ kontaktväg |
| --- | --- | --- | --- |
| IT Jour | [Tel] | [Tel] | [Email/Chat] |
| Säkerhetschef | [Tel] | [Tel] | [Email/Chat] |
| Kommunikation | [Tel] | [Tel] | [Email/Chat] |
| Ledningsjour | [Tel] | [Tel] | [Email/Chat] |

### 8.2 Checklistor

#### Initial incidentrespons

* Bekräfta incident
* Dokumentera initial information
* Klassificera incident
* Eskalera enligt nivå
* Starta loggföring
* Initiera kommunikation

#### Bevisinsamling

* Säkra loggar
* Ta skärmdumpar
* Dokumentera iakttagelser
* Spara nätverkstrafik
* Skapa systemavbildningar
* Dokumentera tidslinje

### 8.3 Referenser och länkar

#### Interna dokument

* Informationssäkerhetspolicy
* IT-säkerhetsinstruktioner
* Kontinuitetsplan
* Kommunikationsplan
* Återställningsrutiner

#### Externa referenser

* NIST Cybersecurity Framework
* ISO/IEC 27035 Incident Management
* Relevant lagstiftning (GDPR, NIS, etc)
* Myndigheters riktlinjer (MSB, IMY, etc)

### 8.4 Revisionshistorik

| Version | Datum | Ändring | Godkänd av |
| --- | --- | --- | --- |
| 1.0 | [Datum] | Initial version | [Roll] |
| 1.1 | [Datum] | Uppdaterad kontaktinfo | [Roll] |
| 1.2 | [Datum] | Reviderade rutiner | [Roll] |

Hela dokumentet bör revideras minst årligen eller vid större förändringar i:

* Organisationsstruktur
* IT-miljö
* Hotbild
* Regulatoriska krav