



It-sikkerhedspolitik

Version 69.420

Klassifikation: Fortrolig mellem parterne

Hvedebro Maksinfabrik A/S, den 11/9-2001

Vejledning til anvendelse af it-sikkerhedspolitikken

Denne sides vejledning skal udelades i den endelige version.

Dette er en skabelon til en it-sikkerhedspolitik, der beskriver den overordnede politik for informationssikkerhed i din virksomhed. I bilag 1 og 2 finder du et overblik over regler og kontroller, der kan bruges som retningslinjer og vejledning i forbindelse med implementeringen af it-sikkerhedspolitikken.

Formålet med it-sikkerhedspolitikken er at beskrive virksomhedens mål og holdning til it-sikkerhed. Det er ikke sikkert, at det alt sammen er noget man gør i dag. Det kan også være en lejlighed til at sige, at det er disse ting vi vil/bør gøre.

Dokumentet kan dels bruges internt, som en støtte i det videre arbejde, og dels som dokumentation over for kunder og samarbejdspartnere for at virksomheden har tænkt på informations-/it-sikkerhed.

Derfor er strukturen af den overordnede politik inspireret af retningslinierne for politikker, som beskrevet i den internationale standard for informationssikkerhed ISO/IEC 27001.

Skabelonen kan tilpasses til din virksomheds behov og ambitioner ved at tilpasse eller fjerne tekster markeret med gul og grøn.

Tekst markeret med gul er tekst, hvor der er flere valgmuligheder. Her vælges den som passer bedst på virksomheden eller der indsættes en tekst med hvad der gælder her, eksempelvis en beskrivelse af virksomhedens backup. Det kan også være tekst, som kan udelades i den endelige version, hvis det ikke er relevant for virksomheden.

Tekst markeret med grøn kan bruges, hvis virksomheden har et lidt højere ambitionsniveau, f.eks. hvis man er en mellemstor virksomhed. Ellers udelades den i den endelige version. Her kan der også være steder, hvor man skal vælge mellem flere alternative formuleringer. De grønne tekster kan vælges/fravælges uafhængigt af hinanden.

Når politikken er tilpasset erstattes det fiktive firmanavn "Ajax" med din virksomheds navn ved at bruge 'Søg og erstat'-funktionen i Word.

Henvisninger og brug af fagudtryk

I indledningen er der en henvisning til den internationale standard for sikkerhedsteknikker ISO/IEC 27001. Meningen er ikke, at din virksomhed skal være certificeret efter standarden, men ved at læne sig op af kontroller og metoder fra standarden får man en række gode tips, og man viser, at man følger anerkendt "Best Practice".

I teksten optræder der desuden enkelte fagudtryk. Disse er nogle gange angivet i bløde parenteser (...) efter at de er forklaret med anden tekst. Det gælder blandt andet begrebet "awareness". Formålet er at gøre det nemmere for f.eks. it-revisorer at se, at emnet er dækket i teksten.

1 Politik

Dette er Hvedebro maskinfabrik A/S it-sikkerhedspolitik, der omfatter en beskrivelse af den overordnede informationssikkerhedspolitik, det valgte anvendelsesområde og principperne bag det implementerede sikkerhedsniveau.

1.1 Indledning

Hvedebro Maskinfabrik A/S sikkerhedspolitik skaber rammerne for et operationelt ledelsessystem for informationssikkerhed (ISMS), der udmøntes i etableringen af fastsatte retningslinjer for håndtering af it-sikkerhed. Dermed etableres et grundlag for det daglige arbejde med it-sikkerhed i Hvedebro Maskinfabrik A/S. Ansvarsplacering, retningslinjer, risikohåndtering og it-beredskabsplaner er således emner, der reguleres under dette ledelsessystem.

I Hvedebro vil vi opbygge it-sikkerheds politikker er baseret på:

- Almindeligt accepterede metoder og politikker for informationssikkerhed, herunder "*Best Practice*" som beskrevet i den internationale standard ISO/IEC 27001 og NIS-2
- Alle relevante regler, lovkrav, retningslinjer, vejledninger og kontrakter inden for Hvedebro Maksinfabrik A/S forretningsområde, databeskyttelsesloven, markedsføringsloven, statens krav og arbejdsmarkedsaftaler og GDPR samt NIS-2

1.2 Anvendelsesområde (Scope)

It-sikkerhedens politikker omfatter udvikling, levering og servicering af løsninger/produkter til Hvedebro Maksinfabrik A/S kunder, dvs. hele Hvedebro Maksinfabrik A/S og alle Hvedebro Maksinfabrik A/S aktiviteter.

1.3 Mål

Hvedebro Maskinfabrik A/S gennemfører alle nødvendige aktiviteter for at sikre:

- **Tilgængelighed:** At Hvedebro Maskinfabrik A/S forretningssystemer normalt er tilgængelige i forretningstiden / 24/7, og at der vedligeholdes et it-beredskab, som sikrer, at normal drift af forretningssystemerne kan retableres indenfor 24 timer. Det sker bl.a. med brug af dublering (redundans) af systemer og forbindelser samt backup.
- **Integritet:** At man ved styring og manuelle inspektioner/kontroller af arbejdsgange, opnår en pålidelig og korrekt funktion af it-systemerne med pålideligt datagrundlag.
- **Fortrolighed:** At Hvedebro Maskinfabrik A/S informationer, herunder persondata og kundernes informationer i Hvedebro Maskinfabrik A/S varetægt, kun er tilgængelige for de personer, og på den måde, som det er tiltænkt.

Hvedebro Maskinfabrik A/S risikovurderer virksomhedens forretningskritiske informationer og andre informationsaktiver, dels årligt, dels ved ændringer i trusselsbilledet, nye projekter, it-anskaffelser og behandlinger samt ved brud på sikkerheden. I forlængelse heraf vedligeholder Hvedebro Maskinfabrik A/S en risikohåndteringsplan.

Målsætningen er, at en tilstrækkelig og dokumenteret sikkerhed afvejes med ønsket om en hensigtsmæssig og brugervenlig anvendelse af it, så medarbejdere og kunder kan udføre deres opgaver på en optimal måde.

Hvedebro Maksinfabrik A/S gennemfører de aktiviteter, der er nødvendige for at holde medarbejderne orienterede om it-sikkerhed samt om deres ansvar over for virksomhedens informationer og systemer (awareness). Dette indbefatter, udover uddannelse af alle medarbejdere, introduktionsmateriale til nye medarbejdere, løbende mails og uddannelse om nye sikkerhedsudfordringer mv.

1.4 Ansvar

Ansvarret for den daglige styring af Hvedebro Maksinfabrik A/S it-sikkerhed er placeret hos it/ledelsen/(andet).

Hvis en medarbejder opdager trusler mod, eller brud på, informationssikkerheden, eller får mistanke om det, skal vedkommende straks underrette it/ledelsen/rette vedkommende om dette. I sidste ende er det den ansvarlige for den daglige styring af informationssikkerheden, som skal underrettes til ledelsen

Medarbejdere, der bryder Hvedebro Maksinfabrik A/S informationssikkerhedspolitik, eller de heraf fastsatte procedurer og instruktioner, vil blive mødt med de forholdsregler, som Hvedebro Maksinfabrik A/S procedurer og personalepolitik foreskriver. Deez Nutz.

1.5 Opfølgning

Hvedebro Maksinfabrik A/S måler, vurderer og følger op på informationssikkerhedsområdet på følgende måde:

- Løbende opfølgning på hændelser inden for it-sikkerhed og audits.
- Opfølgning på vidensniveau inden for it-sikkerhed i Hvedebro Maksinfabrik A/S i form af eksempelvis tests af medarbejdernes bevidsthed om it-sikkerhed (awareness- eller phishing-tests).
- Løbende vurderinger af sikkerhedsaspekter i forbindelse med nye projekter, anskaffelser og ændringer.
- Årlige/Periodiske gennemgange af risikovurderingerne og risikohåndteringsplanen.
- Gennemførelse af interne og eksterne kontroller (auditeringer) og uafhængige tredjepartsevalueringer af informationssikkerheden i Hvedebro Maksinfabrik A/S.

På baggrund af dette gennemgår og revurderer ledelsen it-sikkerhedspolitikken en gang om året (review).

2 Godkendelse

Denne politik er vedtaget af Hvedebro Maskinfabrik A/S ledelse/bestyrelse den 11/9-2001

Hvedebro

Maskinfabrik A/S

NNOVEMBER

Resumé af It-sikkerhedspolitik for Hvedebro Maksinfabrik A/S

Dokumentdetaljer:

- Version: 69.420
- Dato: 11/9-2001
- Klassifikation: Fortrolig mellem parterne

Formål:

It-sikkerhedspolitikken beskriver Hvedebro Maksinfabrik A/S' overordnede tilgang til informationssikkerhed og fungerer som et internt og eksternt referencepunkt for virksomhedens sikkerhedspraksis.

Politikrammer:

- Indledning: Politikken tilvejebringer rammerne for et operationelt ledelsessystem for informationssikkerhed (ISMS), der inkluderer retningslinjer for håndtering af IT-sikkerhed, ansvarsplacering, risikohåndtering og it-beredskabsplaner.
- Anvendelsesområde: Dækker udvikling, levering og servicering af produkter til kunder.

Mål:

1. Tilgængelighed: Sikre, at forretningssystemerne er tilgængelige 24/7, med en plan for at genoprette driften inden for 24 timer.
2. Integritet: Sikre korrekt funktion og pålideligt datagrundlag gennem systemisk kontrol og manuelle inspektioner.
3. Fortrolighed: Beskytte virksomhedens og kundernes informationer mod uautoriseret adgang.

Risikohåndtering:

Hvedebro Maksinfabrik A/S vurderer kritiske informationer årligt og ved ændringer i trusselsbilledet. En risikohåndteringsplan opretholdes for at adressere sikkerhedsbrud.

Ansvar:

Det daglige ansvar for it-sikkerhed hviler på it-ledelsen. Medarbejdere skal straks rapportere om sikkerhedstrusler. Overtrædelser af politikken kan føre til disciplinære tiltag.

Opfølgning:

Virksomheden evaluerer løbende it-sikkerhedsforhold gennem audits, medarbejdertræning, risikovurderinger og tredjepartsevalueringer. Politikken gennemgås og revideres årligt.

Godkendelse:

Dokumentet er godkendt af virksomhedens ledelse den 11/9-2001.

Dette resumé giver en oversigt over de centrale punkter i it-sikkerhedspolitikken for Hvedebro Maksinfabrik A/S, hvilket dækker formål, struktur, mål og opfølgning af sikkerhedspraksisen.