POLICY FOR SIKKERHET

Rufo AS

1. Godkjenning

Dokumentnavn	STY-02-NO-Rufo_Policy_Sikkerhet
Dokumenttype	Styrende
Versjon	2.1
Versjonsdato	20.04.2026
Godkjent av	Daglig leder

2. Formål

Formålet med denne policyen er å sikre at Rufo AS beskytter:

- Mennesker, verdier og eiendeler
- Informasjon, data og IT-systemer
- Drift, leveranser og omdømme

Policyen skal sikre at virksomheten drives på en trygg, robust og pålitelig måte, i tråd med:

- Gjeldende lover og forskrifter (bl.a. personvern og informasjonssikkerhet)
- Krav og forventninger fra kunder og samarbeidspartnere
- Anerkjente prinsipper for fysisk sikkerhet og IT-sikkerhet

Sikkerhetsarbeidet skal være systematisk, dokumentert, basert på kontinuerlig forbedring, samt funderes på oppdatert kunnskap fra troverdige kilder som cybersjekk.no og sikkert.no.

Anerkjente prinsipper for **fysisk sikkerhet** er som følger:

- ✓ **Forebygging**
  Tiltak skal redusere sannsynlighet for uønskede hendelser før de oppstår.
- ✓ **Lagvis beskyttelse (defence in depth)**
  Flere sikkerhetsnivåer kombineres (område, bygg, rom, utstyr).
- ✓ **Adgangskontroll**
  Fysisk tilgang skal være kontrollert og begrenset til autoriserte personer.
- ✓ **Tilgang basert på behov**
  Kun personer med tjenstlig behov skal ha adgang til lokaler og områder.
- ✓ **Sikring av verdier og kritisk infrastruktur**
  Utstyr, lager, dokumentasjon og kritiske installasjoner skal beskyttes mot tyveri og skade.
- ✓ **Oversikt og tilsyn**
  Lokaler og uteområder skal være utformet slik at tilsyn er mulig.
- ✓ **Ansvar og eierskap**
  Roller og ansvar for fysisk sikkerhet skal være tydelig definert.

- ✓ **Robusthet og beredskap**
  Tiltak skal redusere konsekvensene av brann, innbrudd, hærverk og driftsavbrudd.
- ✓ **Bevisstgjøring**
  Ansatte skal opptre sikkerhetsbevisst og følge etablerte rutiner.
- ✓ **Hendelses- og avvikshåndtering**
  Uønskede hendelser skal registreres, følges opp og brukes til læring.
- ✓ **Kontinuerlig forbedring**
  Fysisk sikkerhet vurderes jevnlig og forbedres ved endrede forhold.

Anerkjente prinsipper for **informasjonssikkerhet** er som følger:

- ✓ **Konfidensialitet**
  Informasjon skal kun være tilgjengelig for autoriserte personer.
- ✓ **Integritet**
  Informasjon skal være korrekt, fullstendig og beskyttet mot uautorisert endring.
- ✓ **Tilgjengelighet**
  Informasjon og systemer skal være tilgjengelige når de trengs.
- ✓ **Tilgang basert på behov (need-to-know / least privilege)**
  Brukere skal kun ha tilgang til den informasjonen de trenger for å utføre sine oppgaver.
- ✓ **Forebygging**
  Tiltak skal redusere sannsynlighet for sikkerhetsbrudd før de oppstår.
- ✓ **Lagvis beskyttelse (defence in depth)**
  Flere tekniske og organisatoriske sikkerhetstiltak kombineres.
- ✓ **Risikobasert tilnærming**
  Sikkerhetstiltak baseres på identifiserte risikoer og konsekvenser.
- ✓ **Ansvar og eierskap**
  Roller, ansvar og eierskap for informasjon og systemer skal være tydelig definert.
- ✓ **Bevisstgjøring og opplæring**
  Ansatte skal kjenne trusler, ansvar og hvordan de bidrar til sikkerhet.
- ✓ **Sporbarhet og kontroll**
  Hendelser og tilganger skal kunne etterprøves ved behov.
- ✓ **Hendelseshåndtering**
  Sikkerhetshendelser skal oppdages, håndteres og følges opp systematisk.
- ✓ **Kontinuerlig forbedring**
  Informasjonssikkerheten skal forbedres basert på avvik, hendelser og endrede forhold.

3. Omfang

Denne policyen gjelder for:

- Hele Rufo AS
- Alle ansatte og innleide ressurser
- Alle lokasjoner, systemer og arbeidsformer

Policyen omfatter blant annet:

- Fysisk sikkerhet (lokaler, utstyr, adgang)
- Informasjonssikkerhet og IT-sikkerhet
- Personvern og håndtering av personopplysninger
- Digitale arbeidsverktøy, skyløsninger og eksterne leverandører

4. Overordnede prinsipper

Rufo AS baserer sitt sikkerhetsarbeid på følgende prinsipper:

- **Forebygging** av uønskede hendelser og sikkerhetsbrudd
- **Beskyttelse** av konfidensialitet, integritet og tilgjengelighet på informasjon
- **Minimering av risiko** gjennom risikovurderinger og tiltak
- **Tydelig ansvar og eierskap** for sikkerhet
- **Bevisstgjøring og opplæring** av ansatte
- **Kontinuerlig forbedring** basert på avvik, hendelser og endringer

Sikkerhet skal være en integrert del av planlegging, beslutninger og daglig drift.

5. Målsettinger

Sikkerhetsstyringen i Rufo AS skal bidra til å:

- Redusere risiko for personskader, tap og driftsavbrudd
- Beskytte virksomhetens og kunders informasjon mot uautorisert tilgang
- Sikre stabil og pålitelig IT-drift
- Etterleve krav til personvern og informasjonssikkerhet
- Skape trygghet for ansatte, kunder og samarbeidspartnere

Konkrete sikkerhetsmål fastsettes og følges opp som del av ledelsens gjennomgang.

6. Roller og ansvar

Daglig leder

- Har overordnet ansvar for sikkerhetsstyringen
- Sikrer at nødvendige ressurser, prioriteringer og tiltak er på plass
- Godkjenner policy, mål og vesentlige tiltak

Ansatte

- Ansvarlige for etterlevelse innen egne ansvarsområder
- Skal følge opp risiko, avvik og forbedringstiltak
- Skal følge gjeldende sikkerhetsrutiner og retningslinjer
- Skal opptre aktsomt og sikkerhetsbevisst i arbeidshverdagen
- Skal melde fra om avvik, hendelser og mistenkelige forhold

7. Etterlevelse og avvik

Manglende etterlevelse av denne policyen eller tilhørende rutiner skal:

- Registreres som avvik eller hendelse
- Behandles i henhold til etablerte avviksrutiner
- Følges opp med korrigerende og forebyggende tiltak

Sikkerhetshendelser brukes aktivt i arbeidet med læring og kontinuerlig forbedring.

8. Dokumentasjon og tilknytning

Denne policyen understøttes av blant annet:

- Risikovurderinger for fysisk sikkerhet og IT
- Rutiner for tilgangsstyring, passord og brukeradministrasjon
- Retningslinjer for bruk av IT-utstyr, e-post og skyløsninger
- Rutiner for sikkerhetskopiering og gjenoppretting
- Personvernerklæring og rutiner for håndtering av personopplysninger
- Avviks- og forbedringssystem

Dokumentasjonen er strukturert i Rufo sitt styringssystem.

9. Revisjon og forbedring

- Policyen revideres minimum hvert annet år
- Revideres ved vesentlige endringer i risiko, teknologi eller krav
- Inngår i ledelsens gjennomgang

Behov for forbedringer identifiseres gjennom risikovurderinger, hendelser, avvik og revisjoner.