



Yara Management System

Document type:

Procedure

Valid for Organization:

Porsgrunn

Valid for Location/Facility:

Yara Porsgrunn

L-230 Security i POR

Innholdsfortegnelse

1. ANVENDELSE OG HENSIKT	1
2. REFERANSER.....	1
3. ANSVAR OG MYNDIGHET	2
4. DEFINISJONER.....	2
5. BESKRIVELSE	3
5.1. Organisering av security	3
5.1.1. Security-vurdering.....	3
5.1.2. Beredskap.....	3
5.2. Fotografering.....	3
5.3. Krav til språk kunnskaper hos kontraktører/underkontraktører.....	3
5.4. Taushetserklæring Yara Porsgrunn ansatte	4
5.5. Informasjonssikring.....	4
5.5.1. Organisering og ansvar (Ref. 8 og 9)	4
5.5.2. Oppfølging	4
5.6. Bruk av telefon og telefaks.....	4
5.7. Security på reiser	4
5.8. Brudd på securitybestemmelser	5
5.9. Avviksrapportering	5
6. Vedlegg.....	5

1. ANVENDELSE OG HENSIKT

Denne prosedyren er en beskrivelse av de rutiner som skal praktiseres i Yara Porsgrunn for å beskytte Yara Porsgrunns verdier, aktiviteter, interesser og ansatte mot industrispionasje, sabotasje, terrorhandlinger, tyveri og tilsvarende handlinger.

2. REFERANSER

Ref 2 [YSS HESQ Directive](#)

Ref. 3: Prosedyre L-104, "Dokumentbehandling og arkivering"

Ref 4: [YSS Yara HOPS 0-14 Health Safety and security for business travels](#)

Document Owner:
Karianne Lindalen

Approved by:
Terje Nilsen

Approval Date:
2020-02-26

Next Review Date:
2023-02-20

Document ID:
YMS0-134-736

Version: 8.0

A paper copy is an uncontrolled copy of the document

Changes in this version:
Approved

- Ref 5: YSS Yara HOPS 0-51 Physical Security
Ref 6: YSS Yara HOPS 0-53 Personnel Security
Ref. 7: YSS YARA HOPS 0-50; "Security"
Ref. 8: YSS YARA TOPS 1-17; "Production IT Security Standard"
Ref. 9: YSS YARA Informational Handling
Ref. 10: Arbeidstilsynet om «Språk og kommunikasjon på bygge – og anleggsplasser»

3. ANSVAR OG MYNDIGHET

POR's ledelse har ansvar for at det blir foretatt security-vurderinger, utarbeidet security-instruksjoner samt å føre tilsyn med POR's securityarbeid

Ledelsen er ansvarlig for opprettelse og vedlikehold av forsvarlige sikringsnivåer innen POR, samt sørge for at alle ansatte forstår betydningen av å opprettholde sikringsnivåene.

Avd. sjef har myndighet til å autorisere egne ansatte for tilgang til gradert informasjon innen sitt ansvarsområde.

Alle som har graderte informasjon til behandling, eller på annen måte håndterer slik informasjon, er ansvarlig for at behandlingen skjer i samsvar med Yara's bestemmelser.

Det operative ansvaret for adgangskontrollen er lagt til driftssjefer/vedlikeholdssjefer og avdelingssjefer. Disse kan delegerer ansvar videre til stedfortredere eller skiftledere.

Kvalitetsansvarlig i HMSK-avdelingen er Lokal Security-Representant (LSR).

4. DEFINISJONER

Security:

Er en del av Yaras totale sikkerhetsbegrep og omfatter tiltak som iverksettes som vern mot ulovlige handlinger, samt mot utilsiktet tap eller kvalitetsforringelse av data og informasjon.

Security-nivå:

Uttrykk for de fysiske og organisatoriske sikringstiltak som er nødvendige for å opprettholde krav til vern mot de trusler som eksisterer mot en gitt funksjon, aktivitet eller område.

Fysisk sikring:

Tiltak som iverksettes for å oppdage, hindre eller forsinke inntrenger/urvedkommende inntil vakt eller politi kommer til stedet.

Personellsikring:

Omfatter tiltak innen bruk av ID-kort, tilgangsbegrensning og security-opplæring, samt lederes, ansattes og innleides særlige plikter i security-sammenheng.

Autorisasjon:

Tillatelse til at en person gis adgang til informasjon med angitt beskyttelsesgrad eller til område med angitt security-nivå.

Tillatelse gis av informasjonseier.

Graderte områder:

Avhengig av graden av behov for sikring, deles områdene inn i 4 security-nivåer:

- Beskyttet (securitynivå 1),
- Kontrollert (securitynivå 2),
- Følsomt (securitynivå 3),
- Sperret område (security nivå 4)

Gradert informasjon:

Avhengig av behov for beskyttelse, graderes informasjon i følgende 4 securitynivåer:

- Åpen
- Internt/internal
- Fortrolig/confidential
- Strengt fortrolig/strictly confidential (se Ref 2)

5. BESKRIVELSE

5.1. Organisering av security

5.1.1. Security-vurdering

Utvikling, etablering og vedlikehold av security-tiltak skal gjøres på bakgrunn av en vurdering i henhold til de krav som er satt i styrende dokumenter (Jfr. pkt 2, REFERANSER).
HMSK-avdelingen koordinerer utførelsen av security-vurderingene.

5.1.2. Beredskap

Beredskapsplaner for håndtering av trussel og terror situasjoner er utarbeidet ved Herøya Industripark (HIP).

5.2. Fotografering

Det er generelt forbud mot å fotografere i Yara Porsgrunns områder. Tillatelse til fotografering kan gis til eksternt personell/besøkende av driftssjef/produksjonssjef i hvert område/hver fabrikk. Disse bestemmelsene gjelder også for personell fra andre Yara-enheter enn Yara Porsgrunn.

Etter avtale kan følgende gi tillatelse til fotografering på vegne av driftssjefer/produksjonssjefer:

- Vedlikeholdssjefer
- Prosjektledere
- HES Manager i YPPS HUB i Porsgrunn

Fototillatelsen skal begrenses til et minimum, og gjelder kun innenfor avtalt område. Tillatelsen er tidsbegrenset. Alle fotografier og kopier av disse skal regnes som Yaras eiendom, og skal ikke benyttes i andre sammenhenger enn det som er avtalt. Etter at bildene er ferdig benyttet skal fotografiene lagres av Yara eller slettes/ ødelegges.

Skjema «Tillatelse til Fotografering» (vedlegg 3) skal gjennomgås av den enkelte som skal ha tillatelse, og signeres. Dersom flere personer fra samme firma skal ha tillatelse, kan dette gjøres samlet pr. firma ved bruk side 2 i skjemaet. Signaturen dokumenterer at forutsetningene for fototillatelsen er gjennomgått. Skjemaet oppbevares av den enkelte som har fått tillatelse, hvis ikke annet avtales (f.eks. i prosjekter). Kopi av tillatelse lagres lokalt i Yara. Tillatelsen markeres med et klistremerke på hjelmen (vedlegg 4).

5.3. Krav til språk kunnskaper hos kontraktører/underkontraktører

Kontraktøren som benytter arbeidskraft som ikke er engelsk- eller skandinavisktalende, må sørge for individuell sikkerhetsklarering av alle arbeidere.

Kontraktørens arbeidsleder må sørge for at alle arbeidere kjenner til innholdet i prosedyrer. Dersom arbeidsleder er engelsktalende må Yara prosjektleder/ansvarlig sørge for at kontraktøren kjenner til prosedyrer som kun forefinnes på norsk. (Tid/ kostnader forbundet med dette må legges inn i evalueringen av anbudet).

5.4. Taushetserklæring Yara Porsgrunn ansatte

Alle Yara-ansatte og innleide skal skrive under på en "Taushetserklæring", -se vedlegg 1 og 2. Disse skal oppbevares hos HR-avdelingen

5.5. Informasjonssikring

5.5.1. Organisering og ansvar (Ref. 8 og 9)

For all informasjon og alle informasjonssystemer skal det være definert en eier. Det skilles mellom:

informasjonseier (dvs. eier av den aktuelle informasjon) og
informasjonssystemeier (dvs. eier av f.eks. programvare/software/driftsopplegg som behandler informasjonen)

Bruker av informasjonssystemer er ansvarlig for at utstyr, program og informasjon gjennom vedkommende tilgangsrettigheter brukes slik at egen eller andres informasjon ikke kompromitteres eller ødelegges.

Avtaler og kontrakter

Forhold knyttet til sikkerhet skal kontraktstfestes og være kjent av brukere av informasjonssystemene (IS) og av IS-driftspersonell som er berørt:

Krav til gradering

All informasjon skal vurderes mht. behov for beskyttelse. Beskyttelsestiltakene skal omfatte alle faser av informasjonsbehandlingen så som produksjon, utstedelse, mottak, registrering, postgang, fordeling, saksbehandling, arkivering og tilintetgjøring.

Når det ikke er oppgitt noen beskyttelsesgrad (se pkt.4), skal informasjonen behandles som om den var gradert INTERNT, såfremt informasjonen ikke åpenbart er ment for publisering utenfor selskapet.

Helse - og personinformasjon

Informasjonssystemer som inneholder persondata skal være registrert og godkjent i Yara Porsgrunns personalfunksjon. Helseinformasjon skal kun oppbevares hos Bedrifts Helsen.

5.5.2. Oppfølging

HMSK-avdelingen skal på vegne av ledelsen i POR påse at security-tiltakene er i samsvar med eksisterende risiko- og sårbarhetsnivå. Etablerte security-tiltak skal kontrolleres.

5.6. Bruk av telefon og telefaks

Telefon og telefaks er enkle å avlytte, og det er lett å sende telefaks til feil mottaker. Alle ansatte skal utvise forsiktighet med hva som sies og sendes om selskapet og dets virksomheter over telefonlinjer. Informasjon som er gradert Fortrolig eller Strengt Fortrolig skal krypteres når den formidles over telenettet.

5.7. Security på reiser

Ansatte på tjenestereise skal særlig være oppmerksom på muligheten av å bli utsatt for tyveri, bli ledet inn i forhold som senere kan utnyttes i utpressingsforsøk, bli avlyttet på kommunikasjonsmidler, hoteller, restauranter o.l. Videre skal den ansatte ved reiser i utlandet i rimelig grad søke å gjøre seg kjent med lover og skikker, tollbestemmelser og trusselnivå for ikke å bli utsatt for unødige press eller sjikane.

Ved eventuelle konfliktsituasjoner med myndigheter i fremmed land skal norsk utenriksrepresentant om mulig oppsøkes.

Se ref 4 for ytterligere krav.

5.8. Brudd på securitybestemmelser

Alle securitybrudd, forsøk på eller mistanke om brudd skal straks rapporteres til nærmeste foresatte og LSR. (Lokal Security-representant, - jfr. pkt. 3). Eventuell bombetrussel meldes også umiddelbart til sjefsvakthavende ved HIP.

Leder skal i samarbeid med personalavdelingen. avgjøre om security-bruddet skal behandles som brudd på Arbeidsreglementet og/eller meldes til politiet for etterforskning.

LSR skal innrapportere eventuelle security-brudd, forsøk på eller mistanke om brudd til Fabrikk sjef og HESQ-sjef i Yara.

Rapporteringen begrenses til hendelser som oppfattes å være en trussel for fellesskapet, og til enkelttilfeller som har medført tap eller skade eller fare for slike, og som har en total økonomisk konsekvens på kr. 25.000 eller mer.

5.9. Avviksrapportering

Avvik fra denne prosedyre skal begrunnes og rapporteres til LSR. På vegne av Fabrikk sjef, søker LSR nødvendig godkjenning for slike avvik hos HESQ-ansvarlig i Yara Konsern

6. Vedlegg

Vedlegg 1: [Taushetserklæring](#)

Vedlegg 2: [Taushetserklæring konsulenter](#)

Vedlegg 3: [Tillatelse til fotografering \(skjema\)](#)

Vedlegg 4: [Klistremerke for fototillatelse.](#)