# Riktlinje för säkerhet i OT-installationer

REGION SKÅNE

| Begrepp | Beskrivning |
|---|---|
| IT (Information Technology) | Digital information och kommunikationsteknik |
| OT (Operational Technology) | Teknik som styr, övervakar och optimerar fysiska processer och maskiner inom industrin |
| HVAC (Heating, Ventilation, Air Conditioning) | System för att övervaka och styra fysiska processer i t.ex. byggnader. |
| PLC (Programmable Logic Controller) | Programmerbar styrmodul för industriella och byggnadstekniska system. |
| DUC (Data Under Central) | Enhet för central styrning och övervakning av fastighetssystem |
| ÖS (överordnat system) | Ett system som samordnar flera underliggande system i en byggnad |
| Layer-3 | Nätverksnivå som hanterar kopplingar mellan olika nätverk |
| Jump server | En enhet som fungerar som en mellanhand för fjärråtkomst till ett nätverk |
| Maskincertifikat | Digitalt certifikat som identifierar och säkrar nätverksenheter |
| Redundans | Säkerhetsåtgärd som innebär att kritiska system har backup-lösningar för att förhindra driftstopp |
| Säkerhetspatch | En programuppdatering som syftar till att täppa till säkerhetshål i mjukvara |
| Riskbedömning | Process för att identifiera och hantera potentiella säkerhetsrisker |
| Testmiljö | Testmiljö där system kan provas innan implementering i drift |
| Driftdatorer | Datorer som används för att övervaka och styra fastighetssystem |

| | |
|---|---|
| Systemförvaltare | Ansvarig person för drift och underhåll av IT- och OT-system |
| Firmware | en form av mikrokod eller program som är inbäddat i hårdvaruenheter för att hjälpa dem att fungera effektivt |
| Soft-Scan | En åtgärd för att läsa av inkopplade hårdvaror i ett nätverk/segment |

# Innehållsförteckning

# 1 Inledning

Denna riktlinje för hantering av Operational Technology (OT) i fastighetssystem omfattar samtliga system och komponenter som styr och övervakar byggnadens kritiska funktioner, såsom uppvärmning, ventilation, belysning och accesskontroll. Eftersom dessa system blir alltmer uppkopplade ökar risken för cyberattacker och fysiska intrång.

## 1.1 Syfte och mål

Denna riktlinje syftar till att skapa en säker grund för installation och drift av OT-system i fastigheter.
Syftet är att minska sårbarheter och risker i OT-system kopplade till fastighetsnätverk, och att skapa förutsättningar för en säker och robust installation och drift av nya OT-komponenter i driftmiljö.

Riktlinjen ska bidra till ökad förståelse för att skydda systemen mot både cyberhot och fysiska intrång, samtidigt som ansvarsfördelning och rekommenderade åtgärder tydliggörs.

Målet är att förebygga sårbarheter som kan orsaka driftstörningar eller säkerhetsincidenter.

## 1.2 Omfattning

Riktlinjen omfattar hela Regionfastigheters fastighetsbestånd där OT-system är integrerade i fastighetsnätverken. Detta inkluderar till exempel: styrsystem för HVAC, belysning samt passagesystem. Riktlinjen gäller både vid installation av nya komponenter och vid uppdatering av befintliga system. Fokus ligger på säkerhet ur både ett nätverkstekniskt och ett fysiskt skyddsperspektiv.

Riktlinjen är relevant för samtliga berörda parter, såsom fastighetsägare, IT, driftpersonal och externa leverantörer.

## 1.3 Ansvar

Samtliga projektmedlemmar, entreprenörer, underentreprenörer och leverantörer, ska ha tillgång till riktlinjen och förstå hur den ska tillämpas.

I byggprojekt är det projektchefens eller projektledarens ansvar att tydliggöra vägledning kring identifierade nya OT-System och komponenter, samt att säkerställa en effektiv hantering av dessa under projektets gång.

# 2 Säkerhetsåtgärder

Vid nya installationer inom byggprojekt eller vid verksamhetsförändringar i nya eller befintliga byggnader ska nedan säkerhetsåtgärder följas.

Syftet med säkerhetsåtgärder är att säkerställa en trygg och skyddad miljö för både nätverk och servrar, samt att minimera sårbarhet och obehörig åtkomst.

## 2.1 Installation och konfiguration

En stabil och säker installation av styr- och övervakningssystem är avgörande för att minimera risker och optimera drift. Vid installation och konfiguration av PLC/DUC-system ska följande åtgärder vidtas:

- Alla nya enheter ska först installeras och testas i en lämplig testmiljö innan de tas i drift.
- Funktionalitet och kompatibilitet ska verifieras innan befintliga enheter ersätts.

- Flera PLC-modeller från olika tillverkare ska utvärderas för att säkerställa att de uppfyller kraven på nätverkssäkerhet och kommunikation (Layer 3-krav).
- Varje PLC/DUC-enhet ska ha en separat anslutning (uttag) till nätverket och får inte användas som JUMP server.

## 2.2 Uppdatering av mjukvara och firmware

Regelbundna uppdateringar av mjukvara och firmware är avgörande för att upprätthålla systemens säkerhet och funktionalitet:

- Uppdateringar ska utföras enligt överenskommelse med beställaren och testas och verifieras innan implementering.
- Operativsystem och applikationer ska vara i den senaste eller näst senaste **stabila** versionen.
- Noggrann planering och riskbedömning ska genomföras inför varje uppdatering för att undvika driftsstörningar.
- Uppdateringsprocessen ska hanteras utifrån ett livscykelperspektiv, från övergripande systemnivå (ÖS) ner till byggnads- och komponentnivå.
- Säkerhetspatchar ska testas i en kontrollerad miljö. Om testerna inte visar på någon negativ påverkan på systemets funktion eller stabilitet, ska patchen implementeras skyndsamt enligt fastställd process.

## 2.3 Nätverks- och säkerhetsinställningar

Säkerheten i nätverkskommunikation är central för att skydda styr- och övervakningssystem från obehörig åtkomst. Följande åtgärder ska vidtas:

- Endast ensidig kommunikation ska tillåtas mellan PLC/DUC och servrar för att minimera säkerhetsrisker.
- Redundans och robusthet bör implementeras genom dubbla nätverkskort och separata kommunikationskanaler i PLC/DUC.

- Maskincertifikat bör installeras för att identifiera och autentisera enheter för att förhindra obehörig åtkomst.
- Alla oanvända portar och protokoll ska stängas innan systemet tas i drift.
- Styr- och övervakningssystemet ska härdas genom att inaktivera onödiga tjänster och funktioner.

## 2.4 Fysisk Säkerhet

Fysisk åtkomstkontroll är en viktig del av ett säkert OT-system:

- Alla kritiska enheter ska skyddas genom fysisk åtkomstbegränsning, exempelvis genom skalskydd och låsbara skåp.
- Skåp innehållandes OT-utrustning som finns i allmänna utrymmen ska ha rättighetsbaserad åtkomst via passersystem (elektroniska låssystem med tillträdeskontroll).
- USB-portar och andra fysiska anslutningsmöjligheter i respektive enhet ska inaktiveras om de inte är nödvändiga.

## 2.5 Lösenordshantering

En strikt lösenordshantering minskar risken för obehörig åtkomst mot enheten:

- Standardlösenord ska aldrig användas.
- Alla enheter ska ha unika lösenord.
- Lösenord ska vara komplexa (minst 8 tecken, inklusive stora och små bokstäver samt specialtecken).
- Lösenord bör **endast** bytas vid säkerhetsincidenter eller vid misstanke om kompromettering.

## 2.6 Driftövervakning och ansvarsfördelning

För att säkerställa en effektiv drift och underhåll av systemet bör tydliga roller och ansvarsfördelning fastställas:

- En systemförvaltare per sjukhusområde med helhetsansvar för OT-system/ styr- och övervakningssystemet ska utses som intern resurs (detta saknas i dagsläget inom Regionfastigheter).
- En systemförvaltare ska ha djup förståelse och kunskap om systemen, vilket möjliggör en bättre kravställning.
- En systemförvaltare per sjukhusområde ska se till att drift- och övervakningsfunktioner centraliseras på sjukhusnivå för effektivare hantering och snabb respons vid incidenter.
- En systemförvaltare per sjukhusområde ska genomföra regelbundna kartläggningar av systemets säkerhet och externa anslutningar.
- En systemförvaltare på varje sjukhusområde ansvarar för att det finns minst två driftdatorer kopplade på rätt segment.
- En systemförvaltare per sjukhusområde ska ha aktiv kontakt med respektive leverantör för att hålla sig uppdaterad kring relevanta firmware och uppgraderingar av mjukvara/hårdvara.

## 2.7 Medvetenhet och utbildning

Driftpersonal och användare måste vara medvetna om vikten av säkerhetsåtgärder och robusthet:

- En regelbunden utbildningsplan som omfattar IT/OT systemsäkerhetskunskap bör upprättas inom organisationen.
- Cybersäkerhetsutbildning är obligatoriskt för samtliga RFA-anställda att genomföra en gång om året. Utbildningen finns i Lärportalen och linjechefer ansvarar för att detta uppfylls.
- Målgruppsanpassade utbildningar skall genomföras där systemförvaltare får djupare kunskap medan annan driftpersonal får en grundläggande förståelse.
- Säkerhetsarbete ska inkluderas i det dagliga arbetet genom kontinuerliga riskbedömningar och övningar.

# 3 Långsiktig planering för robusthet och uppdateringar

För att säkerställa ett hållbart och säkert styrsystem bör robusthets- och säkerhetsaspekter inkluderas i planeringsfasen**:**

- Uppdateringar och nyinstallationer ska föregås av noggrann planering och riskbedömning.
- Regelbundna uppdateringar ska implementeras med god framförhållning för att minimera driftstörningar.
- Fastighetsdigitalisering tillsammans med systemförvaltaren på sjukhusområdet ska minst tre gånger om året genomföra en Soft-Scan. Detta ska ske i syfte att granska sårbarheter på komponenter i respektive segment.

# 4 Regelverk och Riktlinjer

- **Kravkatalog för IT-stöd inom Region Skåne:** Arkitekturrådet - Region Skånes intranät . (Länken är intern och projektchef eller projektledare behöver ta vidare underlaget till extern part om behov föreligger).
- **Metodhandbok:** Riktlinjer för byggprojekt och fastighetsförvaltning - Region Skåne
- **Riktlinje för IT i fastighetstekniska system:** Policys uppsatta av IT organisationen
- **NIS2-direktivet:** Nya regler om cybersäkerhet, SOU 2024:18
- **Refernslitteratur-NCS3 Studie – Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3):** Standardserie ISA/IEC 62443

# 5 Kontakt för stöd

Vid behov av stöd och vägledning gällande riktlinjen kontaktas enheten för Fastighetsdigitalisering inom Regionfastigheter.

Fastighetsdigitalisering ansvarar för att hålla riktlinjerna aktuella och att informera om eventuella uppdateringar.

# Versionshistorik

| Version | Datum | Ändrat av | Ändringar |
|---|---|---|---|
| **0.1** | 2025-03-25 | Alve Kafren | Första utkast |
| **0.1** | 2025-04-02 | Alve Kafren | Justerad efter kommentarer |
| **0.2** | 2025-04-08 | Alve Kafren | Utkast klart för remissrunda |
| **1.0** | 2025-05-15 | Mia Albin-Bah | Version 1.0 klart för beslut i LG |
| **1.0** | 2025-06-09 | Mia Albin-Bah | Beslut i LG |