Säkerhetsrekommendationer

COMPACT, GOLD, SuperWISE I och II

Swegon

Innehåll

Dokumentets ursprungsspråk är svenska

1. Inledning

Alla organisationer är måna om att deras tillgångar är skyddade från obehörig åtkomst, vilket innebär att alla uppkopplade produkter/system bör ha verkningsfulla och kostnadseffektiva skydd.

Swegons produkter är i första hand förknippade med inomhusklimat, men produkterna är också tekniskt avancerade och uppkopplade enheter.

Driftstörningar påverkar inomhusmiljön, oavsett om det handlar om arbetsutrymmen, serverhallar eller andra utrymmen där känsliga tillgångar förvaras.

Detta dokument beskriver hur Swegons produkter förhåller sig till IT- och informationssäkerhet.

1.1 Syfte

Detta dokument har två huvudsyften:

- Att beskriva på vilket sätt Swegons produkter uppfyller krav och rekommendationer enligt etablerade standarder, ramverk samt mallar som ISO 27000-serien, NIST SP 800-53, COBIT, BITS med flera.
- Att ge konkreta rekommendationer angående installation, konfiguration och underhåll av Swegons produkter för att maximera drift- och informationssäkerhet.

Rekommendationer som beskrivs i detta dokument är tillämpliga, oavsett om en organisation avser följa en etablerad standard eller ej.

1.2 Målgrupp

Detta dokument har fem målgrupper:

- Kravhantering.

Information om hur Swegon uppfyller krav avseende informations- och IT-säkerhet.

- System/informationsägare.

Rekommendationer för produktens hela livscykel och hjälp i valet av skyddsåtgärder.

- Installation.

Rekommendationer avseende bland annat placering, anslutningar och konfiguration.

- Förvaltning.

Rekommendationer avseende bland annat underhåll, ändringshantering och säkerhetskopiering.

- Granskning/revision.

Jämförelse av rekommenderad konfiguration mot faktisk konfiguration.

1.3 Läsanvisning

För att underlätta för läsaren är de följande kapitlen i detta dokument rubricerade i enlighet med rubriceringen i ISO 27000.

Respektive kapitel inleds med en kort beskrivning av området och hur det relaterar till Swegons produkter. I förekommande fall visas var konfiguration kan utföras.

Därefter följer en konkret rekommendation från Swegon avseende hur en organisation bör agera för att uppfylla både krav beskrivna i ISO 27000 och bästa praxis.

2. Ansvar och ägarskap

Referens: SS-ISO/IEC 27002:2014, avsnitt 8.1 Ansvar för tillgångar.

2.1 Bakgrund

För att säkerställa en säker och välfungerande IT-miljö bör servrar och annan utrustning, som hanterar känslig information eller är kritiska för verksamheten, identifieras. En förteckning över dessa bör sammanställas och ägarskap samt ansvar fördelas.

Exempel på typiska ansvarsområden för ägaren är att säkerställa att servrar och annan utrustning:

- Finns med i förteckningen.
- Är informationsklassad och uppmärkt avseende konfidentialitet, integritet och tillgänglighet.
- Hanteras korrekt med avseende på implementering, underhåll, förändring och avveckling.
- Används i enlighet med fastställda regler och rutiner.

2.2 Rekommendationer

Swegons produkter är inte avsedda att behandla annan information än data som har direkt anknytning till luftbehandling.

Dessa data inbegriper emellertid användarnamn/lösenord till enheten, systemkonfiguration, loggfiler samt potentiella anslutningar till andra system varför ägarskap bör tilldelas respektive enhet.

Swegon rekommenderar att de avsnitt som beskrivs i detta dokument utgör grunden för vilka ansvarsområden som beaktas då en ägare utses.

3. Styrning av åtkomst

Referens: SS-ISO/IEC 27002:2014, avsnitt 9.4 Styrning av åtkomst till system och tillämpningar.

3.1 Bakgrund

För att förhindra att känslig information hamnar i orätta händer, tas bort eller förändras på ett otillbörligt sätt, bör åtkomst till informationen begränsas.

Innan en användare kan ta del av information eller göra konfigurationsändringar, måste användaren identifiera och autentisera sig med giltiga användaruppgifter. Möjlighet finns att skapa unika användarkonton kopplade mot någon av nedanstående åtkomstnivåer:

GOLD version E/F, SuperWISE II

- Local (begränsad åtkomst) är avsedd för att läsa mätvärden.
- Installation (utökad åtkomst) är avsedd för att läsa och skriva enhetskonfiguration.
- Service (priviligierad åtkomst) är avsedd för enhetskonfiguration och hantering av användare.

Funktionen för att administrera användarkonton finns under menyvalet Användare.

GOLD version C/D, Compact, SuperWISE I

- Reader (begränsad åtkomst) är avsedd för att läsa mätvärden. Larm kan nollställas.
- Writer (utökad åtkomst) är avsedd för att läsa/skriva grundläggande enhetskonfiguration.
- Service (utökad åtkomst) är avsedd för att läsa/skriva utökad enhetskonfiguration.
- Admin (priviligierad åtkomst) är avsedd för utökad enhetskonfiguration, hantering av användare och kommunikationsinställningar.

Funktionen för att administrera användarkonton finns under menyvalet Admin/Användare.

3.2 Rekommendationer

Swegon rekommenderar att standardanvändarnas namn och lösenord ändras i samband med att enheten driftsätts.

För att undvika utelåsning bör ett särskilt konto, avsett att enbart användas i nödfall, skapas. Autentiseringsuppgifter skrivs ut och förvaras säkert.

Varje användare bör tillägnas ett unikt och personligt användarkonto, och uppmanas att byta lösenordet vid första inloggning.

Användarkonton med priviligierad åtkomst bör enbart användas för konfiguration av enheten.

För övervakning eller avläsning av enheten är åtkomstnivå Local respektive Reader tillräcklig.

4. Kryptering

(Endast GOLD version E/F och SuperWISE II med programversion 1.80 eller senare)

Referens: SS-ISO/IEC 27002:2014, avsnitt 10.1 Kryptografiska säkerhetsåtgärder.

4.1 Bakgrund

För att skydda känslig och rörlig information från obehörig åtkomst, bör krypteringsteknik användas.

GOLD version E/F

GOLD stödjer kryptering med krypteringsmetoden SSL/TLS för webb- och e-postkommunikation.

Funktionen för att aktivera kryptering för respektive protokoll finns under menyvalet Kommunikation.

SuperWISE II (med programversion 1.80 eller senare)

I SuperWISE II är e-postkommunikation alltid krypterad med krypteringsmetoden TLS.

Funktionen för att kryptera webb-kommunikation finns under menyvalet Inställningar/Kommunikation från och med version 1.80

4.2 Rekommendationer

Swegon rekommenderar att krypteringsteknik används, exempelvis genom att aktivera https och e-post via SSL/TLS. Ej krypterade kommunikationskanaler blockeras genom konfiguration av brandvägg i den egna IT-miljön.

5. Fysisk säkerhet

Referens: SS-ISO/IEC 27002:2014, avsnitt 11.2.1 Placering av utrustning och skydd

5.1 Bakgrund

För att förhindra obehörig fysisk åtkomst till utrustning bör fysiska avgränsningar definieras och implementeras. Tillträde bör enbart beviljas till behörig personal.

Enheterna har en eller flera digitala in- och utgångar. I händelse av obehörig åtkomst skulle dessa kunna användas för avlyssning, eller för att koppla in ej godkända enheter till nätverk.

5.2 Rekommendationer

Swegon rekommenderar att enheten placeras så att obehörig åtkomst minimeras, exempelvis genom att placera den i ett låst utrymme.

Även data- och strömkablar bör skyddas och hållas åtskilda för att förhindra störningar.

6. Underhåll

Referens: SS-ISO/IEC 27002:2014, avsnitt 11.2.4 Underhåll av utrustning.

6.1 Bakgrund

För att säkerställa kontinuerlig funktion och säkerhet, bör utrustning underhållas enligt fastställda intervall.

Detta avsnitt avser underhåll utifrån ett säkerhetsperspektiv. För information om allmänt underhåll, se manual för respektive produkt.

Produkterna är utformade för att kräva minimalt allmänt underhåll. Därför är det särskilt viktigt att planera säkerhetsunderhåll för att undvika att att enheten ”glöms bort”.

6.2 Rekommendationer

Swegon rekommenderar att manuellt underhåll och funktionskontroll utförs av behörig personal minst en gång per år.

Underhållsaktiviteterna bör anpassas till de tjänster och funktioner som är aktiva, men några generella rekommendationer på aktiviteter är att:

- Säkerställa att inga gamla eller överflödiga användarkonton finns kvar (kapitel 3).
- Kontrollera att enhetens konfiguration överensstämmer med igångkörningsprotokollet (kapitel 7) och dokumenterade ändringar (kapitel 8).
- Kontrollera att det finns säkerhetskopior av enhetens konfiguration (kapitel 9) och att de är intakta.
- Säkerställ att enheten är uppdaterad med den senaste programvaran från Swegon (kapitel 12).

7. Dokumentation av enhetskonfiguration

(Endast GOLD version E/F och SuperWISE II)

Referens: SS-ISO/IEC 27002:2014, avsnitt 12.1.1 Dokumenterade driftsrutiner.

7.1 Bakgrund

För att säkerställa korrekt, effektiv drift och förvaltning av en IT-miljö bör nätverk, nätverkskomponenter, anslutningspunkter samt samband mellan system dokumenteras.

GOLD version E/F

GOLD ger möjlighet att skapa ett igångkörningsprotokoll som innehåller information bland annat om enhetens mjukvaru-, kommunikations-, och användarinställningar.

Funktionen för att skapa ett igångkörningsprotokoll finns under menyvalet Grundinställning.

SuperWISE II

SuperWISE ger möjlighet att skapa ett igångkörningsprotokoll som innehåller information bland annat om enhetens mjukvaruinställningar.

Funktionen för att skapa ett igångkörningsprotokoll finns under menyvalet Dokumentation/Injusteringsprotokoll.

7.2 Rekommendationer

Swegon rekommenderar att ett igångkörningsprotokoll skapas i samband med driftsättning.

Igångkörningsprotokollet laddas ned från enheten och förvaras skyddad från obehörig åtkomst tillsammans med övrig dokumentation av IT-miljön.

8. Ändringshantering

Referens: SS-ISO/IEC 27002:2014, avsnitt 12.1.2 Ändringshantering.

8.1 Bakgrund

För att minska risken för avbrott eller störningar bör systemförändringar planeras, testas, godkännas och dokumenteras innan de utförs.

Produkterna innehåller många funktioner och konfigurationsmöjligheter avseende luftbehandling. Produkterna inkluderar även nätverks- och kommunikationsinställningar, som kan påverka enhetens prestanda samt funktion.

8.2 Rekommendationer

Swegon rekommenderar att betydande förändringar inte utförs innan godkännande erhållits från ägaren av enheten (kapitel 1).

En säkerhetskopia på enhetens konfiguration (kapitel 9) bör skapas innan förändringen utförs. Detta för att enkelt kunna återställa den ursprungliga konfigurationen i händelse av en misslyckad förändring.

Efter genomförd förändring bör avsedd funktionalitet verifieras. De förändringar som utförts bör återspeglas i enhetens dokumentation (kapitel 7).

SuperWISE II

Möjlighet finns att exportera en ändringslog rörande ändringar av funktioner och deras inställningar. Funktionen för att skapa en ändringslog finns under menyvalet Ändringslog.

9. Säkerhetskopiering

(Endast GOLD version E/F och SuperWISE II)

Referens: SS-ISO/IEC 27002:2014, avsnitt 12.3 Säkerhetskopiering.

9.1 Bakgrund

Säkerhetskopior av information och konfigurationsinställningar bör skapas för att förhindra förlust av data, för att höja driftsäkerheten samt för att underlätta felsökning.

Produkterna ger dig möjlighet att skapa säkerhetskopior på både luftbehandlingsinställningar och kommunikationsinställningar.

GOLD version E/F

Funktionen för att skapa en säkerhetskopia av respektive inställning finns under menyvalet Grundinställning.

SuperWISE II

Funktionen för att skapa en säkerhetskopia av respektive inställning finns under menyvalet Inställningar/Säkerhetskopia & återställning.

9.2 Rekommendationer

Swegon rekommenderar att säkerhetskopior skapas efter enhetens initiala idrifttagning och innan större förändringar görs avseende enhetens konfiguration.

10. Loggning och övervakning

(Endast GOLD version E/F och SuperWISE II)

Referens: SS-ISO/IEC 27002:2014, avsnitt 12.4 Loggning och övervakning.

10.1 Bakgrund

Loggning av driftstatus och händelser i IT-system är en förutsättning för att säkerställa en säker och välfungerande IT-miljö.

GOLD version E/F

GOLD ger dig möjlighet att både skapa och övervaka loginformation av klimatdata. GOLD kan även automatiskt överföra loggar till en central loggningsfacilitet via e-post och/eller FTP.

Funktionen för automatisk överföring av logginformation är tillgänglig via menyvalet Logg.

SuperWISE II

SuperWISE II ger dig möjlighet att både skapa och övervaka logginformation av klimatdata. SuperWISE II kan även ändra och övervaka funktioners inställningsvärden.

Filer med logginformation är tillgängliga via menyvalet Graf & Logg/Logg.

Funktionen för att skapa en ändringslogg finns under menyvalet Ändringslog.

10.2 Rekommendationer

GOLD

För säker överföring av logginformation via FTP bör ett unikt användarkonto med begränsade rättigheter skapas på destinationsvärden.

GOLD behöver endast skrivrättigheter till en katalog avsedd för systemloggar för att kunna överföra logginformation.

11. Synkronisering av tid

(Endast GOLD version E/F och SuperWISE II)

Referens: SS-ISO/IEC 27002:2014, avsnitt 12.4.4 Synkronisering av tid.

11.1 Bakgrund

För att säkerställa korrekt angivelse av datum/tid i händelseloggar, larm och annan information bör enhetens systemklocka synkroniseras mot en central referenskälla för tid.

GOLD version E/F

GOLD stödjer tidssynkronisering via SNTP och BACNet. Inställningarna för automatisk synkronisering av tid finns under menyvalet Tid och Schema.

SuperWISE II

Swegon SuperWISE II stödjer tidssynkronisering via NTP.

Inställningarna för automatisk synkronisering av tid finns under menyvalet Inställningar/Tid & datum.

11.2 Rekommendationer

Swegon rekommenderar att funktionen för automatisk tidssynkronisering används.

12. Säkerhetsuppdateringar

Referens: SS-ISO/IEC 27002:2014, avsnitt 12.6.1 Hantering av tekniska sårbarheter.

12.1 Bakgrund

För att förhindra att tekniska sårbarheter utnyttjas, bör information om säkerhetsuppdateringar erhållas och hanteras snabbt.

Swegon tillser att säkerhetsuppdateringar installeras i samband med schemalagd service av enheten. Om en organisation saknar serviceavtal, ankommer det på organisationen själv att tillse att säkerhetsuppdateringar installeras.

12.2 Rekommendationer

Swegon rekommenderar att säkerhetsuppdateringar samordnas med underhåll (kapitel 6) och ändringshantering (kapitel 8).

13. Kommunikationssäkerhet

13.1 Säkerhetsåtgärder för nätverk

(Endast GOLD version E/F och SuperWISE II)

Referens: SS-ISO/IEC 27002:2014, avsnitt 13.1.1 Säkerhetsåtgärder för nätverk.

För att säkerställa säkerheten för information i nätverk samt skyddet av anslutna tjänster, bör sådana tjänster och funktioner hanteras i samverkan med lämpliga säkerhetsåtgärder.

Produkterna har flera digitala in-/utgångar, tjänster och protokoll med olika tillämpningsområden.

GOLD version E/F
Funktionen för att aktivera eller inaktivera tjänster och protokoll finns under menyvalet Kommunikation.

SuperWISE II
Funktionen för att aktivera eller inaktivera tjänster och protokoll finns under menyvalen Inställningar/Kommunikation samt Inställningar/BACnet.

13.2 Rekommendationer

(Endast GOLD version E/F och SuperWISE II)
Swegon rekommenderar att nätverk separeras (avsnitt 13.3). Tjänster samt protokoll som inte används inaktiveras.

Exempel på tjänster och protokoll som bör tas i beaktande är:

GOLD version E/F
- SSH
- Trådlöst nätverk
- Modbus
- BACNet
- Exoline

Ett igångkörningsprotokoll kan skapas och användas för att få en överblick över konfigurationen av alla tjänster och protokoll.

SuperWISE II
- SSH (endast programversion 1.80 eller senare)
- Modbus
- BACNet

13.3 Separation av nätverk

Referens: SS-ISO/IEC 27002:2014, avsnitt 13.1.2 Separation av nätverk.

13.3.1 Bakgrund

En väldefinierad avgränsning mellan olika nätverksdomäner baserat på förtroendenivåer, organisationsenheter och funktionalitet kan förhindra att känslig information hamnar i orätta händer eller att andra överträdelser inträffar.

Produkterna kommunicerar via standardiserade protokoll. Åtkomst till- och från enheten bör styras i samverkan med lämpliga skyddsåtgärder.

13.3.2 Rekommendationer

Swegon rekommenderar att driftnätet segmenteras för endast Swegons produkter, detta för att säkerställa driften av inneklimatsystemet.

Detta kan uppnås exempelvis genom att skapa ett unikt VLAN för driftnätet, genom brandväggskonfiguration eller genom att skapa ett separat fysiskt- eller trådlöst nätverk.

13.4 Fjärråtkomst

Referens: SS-ISO/IEC 27002:2014, avsnitt 6.2.2 Distansarbete

13.4.1 Bakgrund

Distansarbete och fjärråtkomst till interna system kan vara ett effektivt hjälpmedel för att underlätta förvaltning, felsökning med mera.

För att förhindra att kommunikation avlyssnas, då den passerar via potentiellt osäkra kommunikationskanaler, bör denna typ av funktionalitet hanteras i samverkan med lämpliga säkerhetsåtgärder.

Fjärråtkomst till produkterna är möjlig genom tillämpning av en VPN-tunnel eller brandväggskonfiguration i den egna IT-miljön.

13.4.2 Rekommendationer

Swegon rekommenderar att åtkomst till produkterna begränsas till organisationens interna nätverk och avråder från exponering mot Internet.

Om fjärråtkomst är nödvändigt bör anslutningen krypteras med SSL/TLS (se kapitel 4) eller IPsec.

Tillåten användning av fjärråtkomst bör begränsas till av organisationen tillhandahållen och godkänd utrustning.

13.5 Portar och protokoll

GOLD version E/F:

Nedanstående tabell illustrerar vilka portar och protokoll som GOLD version E/F använder. Tabellen kan användas som referens under installation och brandväggskonfiguration.

Tjänst	Riktning	Port	Protokoll	Måladress	Beskrivning
DHCP (Client)	Utgående	68	UDP		DHCP
DHCP (Server)	Inkommande	67	UDP		DHCP
SNTP	Utgående	123	UDP		Tidssynkronisering
SSH	Inkommande	22	TCP		Fjärråtkomst
HTTP	Inkommande	80*	TCP		Administration
HTTPS	Inkommande	443	TCP		Administration
DNS	Utgående	53	UDP		DNS
DNS	Utgående	53	TCP		DNS
SMTP	Utgående	25*	TCP		E-post
SMTPS	Utgående	465	TCP		E-post
Rsync	Inkommande	873	TCP		Handterminal sync
Modbus	Inkommande	502*	TCP		Överordnad åtkomst
BACnet	Inkommande	47808*	UDP		Överordnad åtkomst
Exoline	Inkommande	26486*	TCP		Överordnad åtkomst

** Möjligt för användaren att välja portnummer.*

SuperWISE II:

Nedanstående tabell illustrerar vilka portar och protokoll som SuperWISE II använder. Tabellen kan användas som referens under installation och brandväggskonfiguration.

Se gärna även dokumentet Projekteringsguiden El & Styr för mer information.

Tjänst	Riktning	Port	Protokoll	Måladress	Beskrivning
DHCP (Client)	Utgående	68	UDP		DHCP
DHCP (Server)	Inkommande	67	UDP		DHCP på Serviceport
NTP	Utgående	123	UDP		Tidssynkronisering
SSH	Inkommande	22	TCP		Fjärråtkomst
HTTP	Inkommande	80	TCP		Administration
HTTPS	Inkommande	443	TCP		Administration
DNS	Utgående	53	UDP		DNS
DNS	Utgående	53	TCP		DNS
SMTP	Utgående	25*	TCP		E-post
SMTP	Utgående	587	TCP		E-post Swegon Connect
Rsync	Inkommande	873	TCP		Handterminal synkronisering via Serviceport. Mjukvaruppgradering via Driftsnätport.
Modbus	Inkommande	502**	TCP		Överordnad åtkomst
BACnet	Inkommande	47808*	UDP		Överordnad åtkomst
MQTT	Inkommande	1883	TCP		Intern kom.
Swegon GOLD	Utgående	10080	TCP		Intern kom.
Swegon	Inkommande	12347	UDP		Intern kom.

** Möjligt för användaren att välja portnummer.*
*** Möjligt för användaren att välja portnummer endast från programversion 1.80 eller senare.*

GOLD Version C/D, Compact, SuperWISE I:
Nedanstående tabell illustrerar vilka portar och protokoll som GOLD version C/D, Compact oxh SuperWISE I använder. Tabellen kan användas som referens under installation och brandväggskonfiguration.

Tjänst	Riktning	Port	Protokoll	Måladress	Beskrivning
DHCP (Client)	Utgående	68	UDP		DHCP
DHCP (Server)	Inkommande	67	UDP		DHCP
SSH	Inkommande	22	TCP		Fjärråtkomst
Winsock	Inkommande	10001	TCP		Fjärråtkomst
HTTP	Inkommande	80*	TCP		Administration
DNS	Utgående	53	UDP		DNS
DNS	Utgående	53	TCP		DNS
SMTP	Utgående	25*	TCP		E-post
Modbus	Inkommande	502*	TCP		Överordnad åtkomst
BACnet	Inkommande	47808*	UDP		Överordnad åtkomst

** Möjligt för användaren att välja portnummer.*

14. Säkerhetsincidenter

Referens: SS-ISO/IEC 27002:2014, avsnitt 16.1 Hantering av informationssäkerhetsincidenter.

14.1 Bakgrund

För en snabb och verkningsfull hantering av säkerhetsincidenter bör det finnas fastställda rutiner för hur incidenter identifieras, rapporteras och hanteras.

14.2 Rekommendationer

I händelse av att en säkerhetsincident kan härledas till ett tillkortakommande i Swegons produkter bör Swegon kontaktas omgående. Kontaktuppgifter finns på swegon.com.