Tekniska bestämmelser för elektrisk utrustning	Beteckning / Document TBE 100:2
	Utgåva / Issue 2 (S)
Rubrik / Title Gemensamma Tekniska bestämmelser för IT-säkerhet	Datum / Date 2017-05-22
	Ersätter / Supersedes 1 (S)

Innehåll

1 Allmänt

Denna Tekniska Bestämmelse anger de gemensamma IT-säkerhetskrav som ställs på el- och kontrollutrustning avsedd för användning i kärnkraftverk.

För varje anskaffningsärende finns en Teknisk Specifikation (TS). TS sammanställer alla krav på produkten och anger vilka TBE och KBE som skall tillämpas.

Detta dokument ska kompletteras med kraftverkens specifika krav på IT-säkerhet.

2 Definitioner

Access Control

Means to ensure that access to assets is authorized and restricted based on business and information requirements.

Attack (IT-attack)

Försök att förstöra, exponera, förändra, inaktivera, stjäla eller skaffa sig obehörig åtkomst till en tillgång eller använda den på ett obehörigt sätt.

Svensk anmärkning: I Terminologi för informationssäkerhet (SIS-TR 50) definieras ”attack” som enskild aktivitet som syftar till att åstadkomma skada eller störningar för en verksamhet’. **(**ISO/IEC 27000:2016) (Att i syfte direkt eller på sikt orsaka skadlig verkan.)

Informationssäkerhet

Bevarande av konfidentialitet, riktighet och tillgänglighet hos information; vidare kan andra egenskaper såsom autenticitet, spårbarhet, oavvislighet och tillförlitlighet också inbegripas (ISO/IEC 27002:2005) (Begreppet är endast med som information och jämförelse med IT-säkerhet.)

IT-security

All aspects to define, reach, and keep confidentiality, availability, traceability and integrity of digitally stored data

IT-security program

Part of manufacturer management system that implement IT-security issues

Ledningssystem

Grupp av samverkande eller varandra påverkande delar av en organisation för att upprätta policyer och mål samt processer för att nå dessa mål (ISO 9000:2015)

(Begreppet är endast med som information och jämförelse med IT-säkerhetsprogram)

Tillgång

Allt som är av värde för organisationen (ISO/IEC 27002:2005)

3 Generella produktkrav

3.1 Grundläggande krav

Produkten ska vara konstruerad och tillverkad så att IT-säkerhetsaspekterna inte negativt påverkar produktens funktionalitet i form av till exempel prestanda, säkerhet och tillförlitlighet.

IT-säkerhetsprogrammet ska tillämpas på produkten under dess hela livscykel.
Leverantören/Tillverkaren ska redovisa hur:

- integriteten mot oavsiktlig eller otillåten tillgång till programvara och data har upprätthållits
- oavsiktlig eller otillåten ändring, förstörelse av programvara och data har förhindrats
- ovanstående punkter upprätthålls hos Beställaren.

Detta redovisas i form av datatekniska, fysiska eller andra lämpliga skyddsåtgärder.
Redovisningen ska även omfatta kommunikationsanslutningar (interna/externa), nätverk, hjälpmedel, lagringsmedia, behörigheter m.m.

3.2 Standardisering

Konstruktion, tillverkning, provning och verifiering av produkten ska följa krav på IT-säkerhet motsvarande ISO 27002 eller annan likvärdig standard efter Beställarens godkännande.

Tillverkaren/Leverantören ska i Anbudet redovisa vilka IT-säkerhetskrav som produkten/leveransen uppfyller.

4 Kärnkraftspecifika krav

Reaktorsäkerhetskrav är överordnade IT-säkerhetskrav. Detta anges i TS.

Funktioner som inte används ska i möjligaste mån vara blockerade eller borttagna.

5 Övriga krav

5.1 Konstruktion, tillverkning, provning och verifiering

Tillverkaren/Leverantören ska redovisa hur IT-säkerhetskraven upprätthålls vid konstruktion, tillverkning, provning och verifiering av produkten.

5.2 Installation och driftsättning

Tillverkaren/Leverantören ska redovisa hur IT-säkerhetskraven upprätthålls vid installation och driftsättning.

5.3 Avveckling

Tillverkaren/Leverantören ska redovisa hur IT-säkerhetskraven upprätthålls vid avveckling av produkten.

5.4 Reservdelar

Förändringar i konstruktion av programvara, komponentval för kretskort och tillverkningsmetoder som kan påverka IT-säkerheten ska meddelas till Beställaren.

6 Överenskommelser mellan Tillverkare/Leverantör och Beställare

Nedanstående checklista bör tjäna som underlag för genomgång mellan Tillverkare/Leverantör och Beställare i samband med offert eller beställning.

1	Accept av Teknisk Specifikation, TS samt eventuella avvikelser	
2	Tillämpning av riktlinjer/standard	
3	Fortlöpande information från Leverantören/Tillverkaren till Beställaren om identifierade IT-säkerhetsbrister i produkten och vidtagna åtgärder.	
4	Fjärråtkomst via icke godkänt nätverk Åtkomst via trådlösa nätverk/mobiler eller externt lagringsmedia Barriärer mellan zoner Olika typer av identitetskontroll och behörighetsstyrning och möjlighet till uppföljning i efterhand (händelselogg) Åtkomst av händelselogg: Åtkomstkontroll, fel, drifthändelser, systemhändelser, backup, återstarter, konfigurationsändringar Åtgärder för omstart och återställning av angripet system Förebygga, detektera och logga installation av skadlig kod/oauktoriserad kod Lagringskapacitet för händelseloggar Tidssynkronisering Larm för icke förväntad händelse	