# Technical Requirements for Electrical Equipment Rubrik/Title General Technical Requirements on IT-security	Beteckning/Document TBE 100:2
	Utgåva/Issue 4
	Datum/Date 2018-10-03
	Ersätter/Supersedes 3 (E)

Contents

1 General

These Technical Requirements state the general technical requirements on IT-security for electrical equipment intended for use in nuclear power stations.

For each acquisition there is a Technical Specification (TS). The TS compiles all requirements of the product and indicates applicable TBE and KBE.

Additional to this document, plant specific requirements regarding IT- security shall apply.

2 Definitions

Assets

Everything that is valuable for the organization. (ISO/IEC 27002:2005)

Access Control

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

Attack (IT-Attack)

Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. **(**ISO/IEC 27000:2016)

(Actions to directly or eventually cause harmful effects)

Information Security

Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved (ISO/IEC 27002:2005)

(This definition is only for information and comparison with IT-security)

IT-Security

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

IT-Security Program

Part of Manufacturer/Supplier management system that implement IT-security issues

Management System

Set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives. (ISO 9000:2015)

(This definition is only for information and comparison with IT-security program)

3 General Product Requirements

3.1 Basic Requirements

The product shall be designed and manufactured in a way that the IT-security aspects has no negative impact on the product functionality (performance, safety functions and reliability).

The IT- security program shall be applied on the product during the whole life cycle. The Supplier/Manufacturer shall state how:

- integrity against unintended or irregular access to software or data have been maintained
- unintended or unauthorized changes or destruction of software and data have been prevented
- above stated measures shall be maintained by the Purchaser.

This shall be stated by computerized, physical measures or other suitable protective actions. Communication (internal/external), networks, tools, storage media, authentication etc. shall also be included.

3.2 Standardization

Design, manufacturing, tests and verifications of the product shall follow requirements according to ISO 27002 or other equivalent standards prior to Purchasers approval.

The Manufacturer/Supplier shall state in the tender which IT- security requirements the product fulfil or can maintain..

4 Nuclear Specific Requirements

Reactor safety requirements are superior to IT-security requirements. This shall be stated in the TS.

Unused software features shall be defined and shall be blocked or deleted, to the extent it is possible.

5 Other Requirements

5.1 Design, Manufacturing, Inspections and Verifications

The Manufacturer/Supplier shall state in the tender how the IT-security requirements are maintained during installation, commissioning and start-up.

5.2 Installation and Commissioning

The Manufacturer/Supplier shall state in the tender how the IT-security requirements are maintained during installation and start-up.

5.3 Phase out

The Manufacturer/Supplier shall state in the tender how the IT-security requirements are maintained during the phase out of the product.

5.4 Spare Parts

Changes in software design, components on circuit boards and manufacturing methods that can affect the IT-security shall be reported to the Purchaser.

6 Agreements between Manufacturer/Supplier and Purchaser

This checklist should be used as a base between Manufacturer/Supplier and Purchaser when discussing tenders or orders.

1	Acceptance of Technical Specification, TS and deviations, if any	
2	Application of guidelines/standard	
3	Continuously information from Manufacturer/Supplier to the Purchaser concerning identified IT-security weaknesses in the product.	
4	Remote access from not approved networks Access by wireless and mobile networks or external media Barriers between zones Different types of identification and authentication control and the possibility to backtrack different events (event log) Access to event logs: access control, request errors, operating system events, and system events, backup and restore events, configuration changes Back up available for restart of attacked system Protect, detect and log installation of harmful/unauthorized code Storage capacity of event logs Time synchronisation	