

Telenor Networks

Security requirements for Signalling System No. 7 Norwegian national interconnect (informative text in English)

CONTENTS

- 1.1 Technical system requirements..... 3
- 1.2 Personnel requirements..... 3
 - 1.2.1 General..... 3
 - 1.2.2 Clearance of personnel 4
- 1.3 Access and information security requirements 4
 - 1.3.1 Physical security 4
 - 1.3.2 Declaration of non-disclosure of confidential information 5
 - 1.3.3 Document security 5
 - 1.3.4 IT security..... 5

1.1 Technical system requirements

The parties shall establish a national signalling network that is functionally separate from Telenor's national signalling network, and this is realised through the use of national network indicator 3. All switches that are used as interconnect points shall be located within Norway's national borders.

The parties' system, i.e. the technical equipment and associated software, shall normally have a documented significant previous operating period with SS7 in national or international telecommunication networks. Quality assurance system for upgrading/installation of new equipment and/or software shall be documented. The parties shall confirm that the quality assurance systems are used in their day-to-day operations.

If the parties implement equipment/software without a documented previous operating period, then the quality assurance system for installation, upgrading, start-up and test shall be documented. The parties shall confirm that the quality assurance systems are used in their day-to-day operations. If one of the parties demand an expanded test after this, then this must be agreed on separately. If equipment/software without a documented previous operating period is implemented, then the parties can demand special testing as agreed. The results shall be documented and accepted by the parties before start-up.

The parties shall be able to implement and complete the test procedure on SS7 in accordance with the procedures described for Telenor's standard interconnect contract. Implementation of the test procedure applies also in connection with the updating/installation of new equipment and/or software and modifications that can have significant consequences for the other party's network and/or services.

The parties shall establish and maintain a system for monitoring and tracing signalling information to prevent faulty operations and misuse.

If any changes are made to the signalling system's standards the parties are obligated to upgrade their systems at their own expense.

1.2 Personnel requirements

1.2.1 General

The parties shall always have at least 1 person with documented SS7 competence as the principal manager in this area. Documented competence is defined as a description of the individual's formal competence and at least 1 year of documented experience from work with SS7 during the last 2 years.

The parties shall have an operations centre that is operative round the clock. The parties shall have 24-hour access to SS7 competence. If the operation of SS7 is based on the use of subcontractors, then documentation that the subcontractor in question satisfies the requirements stipulated by these conditions shall be submitted.

If the parties fulfil the requirements for a 24-hour operations centre and access to competence through the use of resources outside of Norway's national borders, through for example remote operation, then the parties shall document how the other requirements that are defined in this contract shall be fulfilled, including the routines and measures for physical and logical security as well as personnel security.

1.2.2 Clearance of personnel

The parties shall have a security manager in their own organisation that reports directly to the company's management in connection with security matters.

The security manager or the parties' personnel with operative access to SS7 cannot have any convictions for violation of the penal code. Exceptions to this requirement can be made upon application by one of the parties if the offence committed by the individual is not regarded as having any relevance for the other party's security clearance evaluation.

The parties shall themselves initiate the clearance of their personnel in relation to the requesting authority if this is required by public law.

A list of the parties' security managers and personnel who have operative access to SS7 that complies with the requirements stipulated in the contract shall be available. This list shall be kept up-to-date and stored in a proper manner. The parties can obtain a confirmation that the security clearance requirement has been met from the requesting authority.

1.3 Access and information security requirements

1.3.1 Physical security

The parties' buildings containing network elements where it is possible to log onto operating functions for SS7 shall be secured in accordance with the following minimum requirements:

External doors shall be manufactured in accordance with NS 3170 class 2. Doors shall be equipped with at least one approved lock.

Technical telecommunication equipment shall be located in rooms without any windows. If windows cannot be avoided due to special conditions, then the glass shall at least comply with class B1/C1 in accordance with NS 3217, or the windows must be

equipped with steel shutters that are at least 5 mm thick. External windows shall have a two-point lock and double glazing as a minimum.

The building shall be equipped with an approved AIA (Automatic Intruder Alarm). Buildings that are especially vulnerable (for example buildings that are subject to break-ins based on previous experience) or parts of buildings shall be equipped with access control and/or ITV.

If the building as a whole cannot be secured in accordance with this requirement for any reason, then the requirement must be met for rooms where equipment and operating terminals are located.

1.3.2 Declaration of non-disclosure of confidential information

The parties shall have an internal system for obtaining a declaration of non-disclosure of confidential information from their own personnel who come in contact with other operators' networks. The declaration shall be signed and stored in a proper manner. It shall prevent confidential information from getting into the wrong hands or being abused.

1.3.3 Document security

Information from the parties and documentation related to the SS7 concerning interconnect shall be stored in a proper manner, at least in accordance with the guidelines prepared by Telenor (Policy and Guidelines for Document Security). Chapter 1.7.4 below applies accordingly.

1.3.4 IT security

The parties shall develop and establish standards and procedures for IT security, including procedures for the maintenance of user rights. Strong authentication of users and/or encryption of the link if one is to have access to SS7 from a location other than the switch, in connection with remote operation for example, is required. One-time password systems are often used for strong authentication. For remote logon it is possible to use other alternatives for strong authentication such as RLN (Remote LAN Node) or TTP and smart cards with digital signatures.