swissgrid

Guideline

Information Security in Substations

Valid from: 1. September 2015

Version: 1.0

Approved by: Chief Security Officer, Information Security Officer

Responsible: Information Security Officer

1. Introduction

Active safety awareness – especially in the area of information security – contributes to ensuring a secure power supply that is as uninterrupted as possible. This guideline governs the secure handling of information and communication technology (ICT) equipment and information in the substations.

2. Scope of application

This guideline applies to all persons who have access to the ICT components and secondary equipment of Swissgrid.

3. Use of mobile storage media

In order to prevent the infiltration/spread of malware, the use of mobile storage devices such as USB sticks or hard drives in the substations is forbidden. This does not include the use of USB sticks approved by Swissgrid, which must be used in accordance with the process for the handling of USB storage media (available in the substations).

4. Use of third-party devices

Only ICT devices approved by Swissgrid may be used. Private devices may not be connected to any systems.

5. Use of passwords

In order to prevent unauthorised access to the systems, the following points concerning the use of passwords must be strictly adhered to:

» The complexity of the password must comply with the requirements of the Swissgrid guideline on passwords (available in the substations).
» Predefined default passwords must always be changed before commissioning.
» Passwords must not be written down or made accessible on programmable function keys and must be stored securely.
» If an unauthorised person finds out a password, or there is a suspicion that this may be the case, the password must be changed immediately.
» If passwords have been temporarily passed on to third parties they must be changed subsequently.

6. Wireless access

All information obtained in association with Swissgrid wireless access is to be treated as confidential and must not be passed on. Swissgrid wireless access must only be used for business activities on behalf of Swissgrid.

7. Change management and maintenance work

In order to ensure stable and uninterrupted operation at the substations, all scheduled work on components of ICT or secondary equipment must be reported to the Swissgrid Service Desk.

E-mail: servicedesk@swissgrid.ch
Telephone: +41585803333

8. Obligation to report in the event of specific incidents

Incidents or defects in the area of information security (e.g. virus messages, disclosed passwords, unknown connected devices, etc.) are to be reported immediately to the Swissgrid Service Desk:

E-mail: servicedesk@swissgrid.ch
Telephone: +41585803333

9. Entry into force and changes

This guideline is effective as of 1 September 2015 and supersedes existing regulations concerning information security in substations. Any changes will be initialised by the Information Security Officer and jointly put into effect with the Chief Security Officer. Otherwise, this guideline will be checked every two years by the Information Security Officer and updated as necessary.

Swissgrid Ltd
Werkstrasse 12
CH-5080 Laufenburg

Dammstrasse 3
CH-5070 Frick

Route des Flumeaux 41
CH-1008 Prilly

Phone +41 58 580 21 11
Fax +41 58 580 21 21

info@swissgrid.ch
www.swissgrid.ch