STUK

GUIDE **YVL A.12** / 22 NOVEMBER 2013

INFORMATION SECURITY MANAGEMENT OF A NUCLEAR FACILITY

continues

With regard to new nuclear facilities, this Guide shall apply as of 1 December 2013 until further notice. With regard to operating nuclear facilities and those under construction, this Guide shall be enforced through a separate decision to be taken by STUK.

First edition
Helsinki 2014

ISBN 978-952-309-067-5 (print) Kopijyvä Oy 2014
ISBN 978-952-309-068-2 (pdf)
ISBN 978-952-309-069-9 (html)

STUK • **SÄTEILYTURVAKESKUS**
STRÅLSÄKERHETSCENTRALEN
RADIATION AND NUCLEAR SAFETY AUTHORITY

Osoite/Address • Laippatie 4, 00880 Helsinki
Postiosoite / Postal address • PL / P.O. Box 14, FI-00881 Helsinki, FINLAND
Puh./Tel. (09) 759 881, +358 9 759 881 • Fax (09) 759 88 500, +358 9 759 88 500 • www.stuk.fi

Authorisation

According to Section 7 r of the Nuclear Energy Act (990/1987), *the Radiation and Nuclear Safety Authority (STUK) shall specify detailed safety requirements for the implementation of the safety level in accordance with the Nuclear Energy Act.*

Rules for application

The publication of a YVL Guide shall not, as such, alter any previous decisions made by STUK. After having heard the parties concerned STUK will issue a separate decision as to how a new or revised YVL Guide is to be applied to operating nuclear facilities or those under construction, and to licensees' operational activities. The Guide shall apply as it stands to new nuclear facilities.

When considering how the new safety requirements presented in the YVL Guides shall be applied to the operating nuclear facilities, or to those under construction, STUK will take due account of the principles laid down in Section 7 a of the Nuclear Energy Act (990/1987): *The safety of nuclear energy use shall be maintained at as high a level as practically possible. For the further development of safety, measures shall be implemented that can be considered justified considering operating experience, safety research and advances in science and technology.*

In accordance with Section 7 r(3) of the Nuclear Energy Act, *the safety requirements of the Radiation and Nuclear Safety Authority (STUK) are binding on the licensee, while preserving the licensee's right to propose an alternative procedure or solution to that provided for in the regulations. If the licensee can convincingly demonstrate that the proposed procedure or solution will implement safety standards in accordance with this Act, the Radiation and Nuclear Safety Authority (STUK) may approve a procedure or solution by which the safety level set forth is achieved.*

Translation. Original text in Finnish.

1 Introduction

101. This Guide sets out requirements for the management of information security at a nuclear facility, and it specifies in more detail the design requirements set forth in the Government Decree on Security in the Use of Nuclear Energy (734/2008) [2]. According to Section 4 of the Decree, advanced information security principles shall be applied in the planning of any nuclear facility and its information, communications and I&C systems. Unauthorised access to the protection, control and adjustment systems of the nuclear facility shall be prevented.

102. Otherwise, the provisions of the Act on the Openness of Government Activities (621/1999) [4] on the publicity of documents shall apply, and this also covers information security. Section 78 of the Nuclear Energy Act (990/1987) [1] contains provisions for non-disclosure obligation. The non-disclosure obligation applies to the plans concerning nuclear security arrangements.

103. The Nuclear Energy Act (990/1987) [1], and the Government Decrees on Security in the Use of Nuclear Energy (734/2008) [2] and on the Safety of Nuclear Power Plants (717/2013) [3] issued based on the Act, present the general requirements concerning nuclear security arrangements. The international nuclear industry agreements that have been signed by Finland, other intergovernmental agreements, and the commitments made by Finland also include a number of obligations. The Design Basis Threat (DBT) is presented in a separate document "Design Basis Threat to the Use of Nuclear Energy and the Use of Radiation" that is provided to the licensees of the appropriate nuclear facility categories defined in Guide YVL A.11, and it shall be used as basis when designing the security arrangements and information security management. Together with the documents mentioned above, STUK's Guides YVL A.11 and YVL A.12 form the basis for the security arrangements of nuclear facilities. By virtue of Section 55 of the Nuclear Energy Act, the Finnish Radiation and Nuclear Safety Authority (STUK) is the authority that regulates security arrangements at nuclear facilities in Finland. Pursuant to Section 9 of the Nuclear Energy Act, the licensee is responsible for the security arrangements insofar as they do not fall under the responsibility of the authorities [1].

104. Information security refers to the appropriate protection of information, systems, services, and data communication under normal and exceptional conditions by means of administrative, technical, and other measures. The integrity, non-repudiation, availability and confidentiality of information shall be protected against threats and damage caused by equipment and software failures, natural disasters and wilful or accidental acts. Information security is part of the licensee's activity management system and security arrangements.

105. Information security covers maintaining the integrity, non-repudiation, availability and confidentiality of information in all its forms, from the creation of information until its destruction. Information refers to all information that is stored, processed, or transferred in different formats. Information may be contained, for example, in a single paper document, file, database, executable program, on film, or as a sound or image recording.

2 Scope of application

201. This Guide sets forth the regulations concerning information security at nuclear facilities, and the requirements for their application. The Guide is applied to nuclear facilities in all stages of their lifecycles. The Guide is intended for use by licence applicants and licensees, and it shall be applied to other organisations that have an impact on information security at nuclear facilities, as well as to other use of nuclear energy. General requirements and the regulatory control performed by STUK are also described in the YVL A series Guides, and in the Guides YVL B.1, B.2, B.7, C.5, D.1, D.2, D.3, D.5, and E.7.

3 Information security management

3.1 General requirements

301. The management of the nuclear facility shall demonstrate commitment to information security management.

302. The information security management system shall be part of the licence applicant's/licensee's management system meeting the requirements of Guide YVL A.3.

303. The information security management system shall cover the actions and procedures related to both administrative and technical information security, and it shall also include the guidance and supervision of external resources in terms of information security.

304. Where applicable, the international information security standards and guidelines [5–8, 12, 14, 18] and national guidelines [9–11, 13] shall be taken into consideration in the development of the information security management system.

305. Guide YVL A.11 sets forth the requirements for communicating situational awaressness. Information security shall be taken into account when communicating the situational awaressness; however, information security shall not jeopardise communicating an up-to-date situational awaressness.

306. According to Section 28 of Government Decree (717/2013) [3] and Section 19 of Government Decree (736/2008) [17], a good safety culture shall be maintained when designing, constructing, operating and decommissioning a nuclear facility. This requirement also applies to the management of information security.

307. The Design Basis Threat defines the threat that is used as the basis for the requirements set for, and the planning and assessment of, nuclear security arrangements. The licensee shall design the information security management system to be effective in countering the DBT in accordance with the protection objectives of the DBT as effectively as is reasonably achievable.

3.2 Information security management system

308. The licensee shall define the scope and limits of the information security management system, and the information security management policy. The information security management policy may be an individual document or part of a larger set of documentation. The scope and the information security management policy shall be evaluated both at regular intervals, and whenever significant changes occur that apply to safety or information security, or when new threats appear.

309. The information security management system shall include the objectives for information security. Attention shall be paid to measuring how the information security objectives are met, meeting the goals shall be tracked, and the goals shall be evaluated by applying the principle of continuous improvement. The implementation plans shall include the responsibilities and duties of the different parties involved, the actions, required resources, implementation/maintenance schedules, and how the effectiveness of the actions is evaluated and developed.

310. Information security shall be taken into account at all levels of the organisation's activities. The information security management system shall describe the information security organisation. The description shall also take into consideration any external parties and their responsibilities, if the parties or their activities have an effect on the information security of the nuclear facility. Where necessary, the tasks and areas of responsibility shall be separated in order to reduce the risk of unauthorised or accidental modification or abuse of the organisation's protected assets.

311. The licensee shall document the criteria and standards that have been used in the setting up of the information security management system. The procedures followed by the authorities [10] shall be used to protect non-public information given to the licensee by the authorities, and the National Security Auditing Criteria (KATAKRI) [13] shall be used to evaluate the level of information security in the protection.

312. Risk assessment and management is part of the information security management system. The risks related to information security shall be evaluated using the methods that are the most suited to each discipline and system. The licensee

shall ensure that the methods used to evaluate information security risks are sufficient in terms of the safety and security of the nuclear facility, and that any significant risks have been identified.

313. The overall risk management system shall be documented.

314. The licensee shall draw up an information security threat and risk analysis, and it shall be updated annually and whenever significant changes with an impact on information security take place or new threats emerge.

315. Threats and risks related to information security shall be analysed in a systematic manner, and protective measures and methods shall be selected on the basis of the analysis. The analysis shall be maintained and developed continuously.

316. The assets to be protected shall be identified and defined at a sufficient level of detail. The related threats, vulnerabilities and effects of information security breaches shall be analysed, and the necessary protective actions shall be defined. The protective measures shall be documented.

317. Access to the protected assets shall be monitored using log procedures. The log entries shall include the necessary information that is required to trace the event and the user. The log files shall be protected against unauthorised modifications.

3.3 Requirements for documentation

318. The general requirements for the licensee's documents are presented in Guides YVL A.1, YVL A.3, and YVL A.11, and they shall be followed in documents concerning information security.

319. The documents shall be protected against unauthorised use, modification and deletion, and their availability to authorised users shall be ensured. The documents shall be classified according to their significance for the information security and physical security arrangements of the facility. The documents shall be protected as required by the classification.

3.4 Resource management

320. The licensee shall ensure the availability of adequate resources and competences for the planning, implementation, evaluation and continuous improvement of information security management. Guides YVL A.4 and A.11 present the general requirements in terms of resource management. The resources shall include personnel resources, the necessary expertise, and technological resources.

321. The key personnel and other resources related to information security management shall be employed or owned by the licence applicant/licensee. A risk assessment shall be completed before the maintenance, service or operation of information systems may be outsourced, and it shall be demonstrated that the residual risk is at an acceptable level.

322. The training and the maintenance of competence of the persons participating in the training, development and maintenance of information security shall be sufficient in order to allow them to perform their duties. The entire personnel of the nuclear facility and external resources shall be aware of issues related to information security to the extent that is required for the appropriate maintenance of their tasks. Training and learning events related to information security shall be documented.

323. When using external resources, the licensee shall employ agreements and inspections to ensure that the level of information security is at a level that at least corresponds to the licensee's standards for similar activities. The licensee shall present the measures that it uses to supervise the information security of a supplier or a similar external resource. The verification shall take into account any subcontracting chains.

3.5 Audits and reviews of the information security management system

324. To verify the correct level of information security, the licensee shall arrange an annual self-assessment of information security. The scope of the assessment shall ensure that all areas of the information security management system are assessed at least once every three years. Any

changes to the risk assessment and the envisioned threats, and the effect of the information security events on the management system, shall also be analysed during the assessment.

325. At regular intervals, however at least once every four years, the licensee shall perform an extensive information security audit using a separately assembled expert group that is independent of the activities of the licensee.

326. STUK shall be notified in good time of self-assessments as well as any assessments, audits and reviews performed by independent expert groups or external resources, in order to allow STUK to monitor the implementation of the audits at STUK's discretion.

327. When assessing deviations, special attention shall be paid to repeated observations and deviations. The root causes of such observations and deviations shall be evaluated, and any corrective and preventive actions shall be constructed in a manner that makes it possible to bring repeated deviations under control.

328. When necessary, the licensee shall subject external resources to sufficient information security audits. The audits of external resources shall cover to a necessary degree those functions that are similar to the licensee's own functions. Detailed requirements for the supervision of suppliers are presented in Guides YVL A.3 and A.5.

329. The audits and reviews shall be documented.

3.6 Improving the information security management system

330. Continuous improvement shall take into account the operating experience from information security management in both the licensee's own field of business and other fields of business.

331. The licensee's management shall promote ways by which the entire personnel can participate in the implementation and continuous improvement of the information security management system.

332. The licensee's management shall ensure that any improvements made to the management system are aligned with the set goals.

4 Protecting systems that are important to safety and security

401. Pursuant to Section 4 of Government Decree (734/2008) [2], *advanced data security principles shall be utilised in the planning of the nuclear facility and its information, communications and I&C systems. Unauthorised access to the protection, control and adjustment systems of the nuclear facility shall be prevented.*

4.1 General requirements

402. The information security and security architecture of any systems that directly or indirectly affect the nuclear safety of a nuclear facility, such as the information systems, communications systems, and electrical and I&C systems, shall be designed in a manner that employs sufficient physical, technological and administrative security arrangements to prevent unauthorised access as well as is reasonably achievable.

403. The installation of inappropriate devices and software shall be reliably prevented. Changes made to the software shall be detectable and traceable.

404. The security arrangements of a nuclear facility shall be based on zones in accordance with Guide YVL A.11. All of the information systems, communications systems and electrical and I&C systems, the networked equipment and standalone systems, and the systems for nuclear security and communication systems for emergency preparedness of a nuclear facility shall be appropriately protected.

405. Networked equipment means all devices that are connected to other devices by means of a network or of a cable that can be used for communication. The related cabling and communications

shall be protected against unlawful actions. The physical and logical separation of the networks and the monitoring of the communication taking place in the networks shall be implemented as well as is practically achievable, while taking the security significance of the networks into consideration.

406. The licensee shall aim to prevent that an individual person could install a malicious functionality in several redundant devices or software programs. The effect of a single device or a piece of software on the reduction of the nuclear facility's overall security shall be as low as is reasonably achievable. A system shall be in place to reliably detect the installation of any malicious functionalities or the deactivation of any protection functions.

407. The documents and information pertaining to the nuclear facility and its information systems, communications systems, electrical and I&C systems, security surveillance systems and communications systems shall be protected to a degree necessitated by their security significance and in a manner where they can only be accessed by authorised persons.

4.2 Management and control of communications and operation

408. The licensee shall have in place written procedures for secure information processing services. The procedures shall be updated, and they shall be available to all users who require them.

409. Change management of information security shall follow the configuration management procedures presented in Guide YVL B.1.

4.3 Procurement, development and maintenance of systems related to information security

410. The procurement, development and maintenance of systems shall be implemented in a manner where information security is taken into account during all stages of the system's operating life. The licensee shall pay special attention to preventive information security and collecting and utilising operating experience from other organisations.

411. The information security documentation related to the purchase, development and maintenance of systems shall be comprehensive and up-to-date. The documentation shall be integrated with the other system documentation.

412. The dependencies between systems and their subcomponents shall be identified, their effect on information security shall be analysed and assessed, and any harmful dependencies shall be removed.

413. For networked systems, the interfaces and connections between different systems, the protocols used, and the communicating parties shall be described in a comprehensive and unambiguous manner.

414. The systems and their interconnections shall be designed so that only those functions that are necessary for the performance of operations in question are available.

4.4 Information security incident management

415. The licensee shall have in place procedures to ensure that any abnormalities detected or protection-related vulnerabilities suspected in the development or use of the information systems or services which emerge are reported to the licensee, supplier and, when necessary, STUK as soon as possible.

416. The licensee shall establish procedures to systematically react to incidents in information security.

417. Procedures shall be put in place for reporting information security incidents. Any incidents in information security that are significant in terms of nuclear safety shall be reported to STUK as soon as possible. Guide YVL A.3 discusses the management of incidents, and it shall be taken into consideration when processing information security incidents.

4.5 Access control

418. The licensee shall draw up, document and review the principles for access control.

419. The administrator rights to the different systems shall be limited. Access shall only be granted when it is required to perform work tasks.

420. The users' access rights shall be reviewed regularly and whenever work tasks are changed.

421. A password policy shall be defined and implemented. The implementation shall be monitored.

422. Principles of secure information processing and system use shall be prepared for telecommuting purposes and for work performed by external resources; the implementation of these principles shall be monitored.

4.6 Information security testing of systems related to nuclear safety and security

423. Systems related to security arrangements monitoring shall be tested against information security attacks. Testing can be performed during the drills arranged to demonstrate the effectiveness of security arrangements pursuant to Guide YVL A.11.

424. The system qualification and testing of electrical and I&C equipment and systems of a nuclear facility where such testing is required under Guide YVL E.7 shall take information security into consideration.

425. In addition to functional testing, the testing of networked systems important to safety and security shall utilise advanced testing procedures to a sufficient degree. For standalone systems, testing shall be performed on the basis of the risk assessment created for these systems. The test results shall be documented.

426. Special attention shall be paid to evaluating the information security of the overall system consisting of the new and any old systems.

5 Documents submitted for the regulatory oversight by the Radiation and Nuclear Safety Authority

5.1 Decision-in-principle stage

501. In accordance with Section 24 of the Nuclear Energy Decree (161/1988) [15], an application for a decision-in-principle for a nuclear facility shall also include a description of the suitability of the planned location for its purpose, taking account of the impact of local conditions on security arrangements [16].

5.2 Construction licence stage

502. Together with the application for a construction licence, the licence applicant shall submit the following documents to STUK for approval:

1. A description of the construction licence phase information security management system and related documents, such as the information security policy
2. Information security risk assessment plan, and the results from the risk assessments.
3. The information security requirements and the information security testing requirements
4. The system-level information security plans, including assets to be protected and related protection arrangements, information security zones, and an overall architecture plan
5. The information security organisation for the construction phase
6. A plan concerning the information security control and supervision activities that are applied to suppliers during the construction of the nuclear facility.

503. The following documents shall be submitted to STUK for information:

1. The descriptions related to the classification and processing of documents and information during construction
2. The information security procedures related to system procurement
3. The requirements for system design, including intersystem connections

504. For justified reasons, the documents or similar information indicated in requirement 503 to be submitted to STUK may also be verified at a location indicated by the party applying for a construction licence.

505. The documents referred to in requirements 502 and 503 shall be kept up to date. Approval from STUK shall be applied for the above plans and documents and any changes made to them, or they shall be submitted to STUK for information as stated above.

5.3 Construction stage

506. During the construction of a nuclear facility, the following documents shall be submitted to STUK for approval:

1. Any significant changes to the information security management system
2. Detailed information security test plans
3. A construction phase information security risk assessment plan, and the results from the risk assessments

507. The following documents and the updates made to them shall be submitted to STUK for information:

1. Minor changes to the information security management system
2. Updated information security plans
3. Reports from the information security inspections and reviews, and information security testing reports

508. For justified reasons, the documents indicated in requirement 507 to be submitted to STUK may also be verified at a location indicated by the construction licence applicant.

509. The documents referred to in requirements 506 and 507 shall be kept up to date. Approval from STUK shall be applied for the above plans and documents and any changes made to them, or they shall be submitted to STUK for information as stated above.

5.4 Operating licence stage

510. When applying for an operating licence, STUK submits a statement concerning the application to the Ministry of Employment and the Economy, and includes in the statement its own safety assessment and an assessment of the documents required in Section 36 of the Nuclear Energy Decree (161/1988); the assessment also discusses the planned information security arrangements, among other things. When preparing the safety assessment, STUK requests from the Ministry of the Interior a statement on the documents referred to in Section 36(7) of the Nuclear Energy Decree concerning the nuclear security and emergency arrangements [15].

511. The documents from the construction licence phase shall be submitted in their final form during the operating licence phase, along with other documents and clarifications that are required by STUK, to verify the sufficient level of information security.

5.5 Operation stage

512. During the operation phase, the license applicant shall submit the following documents to STUK for approval:

1. A description of the information security management system
2. An information security risk assessment plan, and the results from the risk assessments performed during operation
3. System-level information security plans, a description of the information security zones, and an overall architecture plan
4. The information security requirements and a description of the information security testing procedures

513. The following documents and the updates made to them shall be submitted to STUK for information:

1. The descriptions related to the classification and processing of documents and information, and the protection instructions and procedures
2. The information security procedures related to the procurement and maintenance of systems
3. The information security objectives and indicators
4. The information security training programme
5. Procedures and reporting related to information security incidents

6. Audit and review reports
7. Instructions for system information security documentation (may be part of other documentation), including information security testing, and their implementation
8. Instructions for system design, including intersystem connections
9. The protected assets identified, and related protection arrangements
10. The information security organisation
11. The information security guidance and supervision of third parties

514. For justified reasons, the documents or similar information to be submitted for information may also be verified at a location indicated by the licensee.

5.6 Decommissioning stage

515. Before starting decommissioning activities, the licensee shall present to STUK for approval an analysis of the procedures that are used to implement information security during the decommissioning phase.

6 Regulatory oversight by the Radiation and Nuclear Safety Authority

6.1 Decision-in-principle stage

601. According to Section 25 of the Nuclear Energy Decree (161/1988) [15], *in its preliminary safety assessment of the application for a decision-in-principle, the Radiation and Nuclear Safety Authority must also include a statement from the advisory committee referred to in section 56 subsection 2 of the Nuclear Energy Act.*

6.2 Construction licence stage

602. When the construction license is applied for, STUK issues a statement on the application to the Ministry of Employment and the Economy and attaches into the statement its safety assessment and an assessment on the documents required in Nuclear Energy Decree, Section 35. While preparing the safety assessment, STUK requests the Ministry of Interior for a statement on the reports referred to in Section 35(6) of the Nuclear Energy Decree concerning the nuclear security and emergency arrangements [15].

603. STUK verifies the sufficiency of the documents mentioned in section 5.2 and the sufficiency of the methods and solutions presented in or related to them by using document reviews and by means of different types of inspections. The inspections may be either announced or unannounced. STUK's approval shall be sought for the above-mentioned plans and documents and for any revisions concerning them, or they shall be submitted for information, as mentioned in section 5.2.

604. The inspections on the information security and security culture of construction license phase may be integrated with STUK's other inspection activities.

605. At its discretion, STUK may participate in the audits and reviews performed by the licence applicant during construction licence phase. Any audits or reviews shall be notified of sufficiently early.

6.3 Construction stage

606. STUK's approval shall be sought for the plans and documents mentioned in section 5.3 and for any revisions concerning them, or they shall be submitted for information, as mentioned in section 5.3. STUK verifies the sufficiency of the documents mentioned above and the sufficiency of the methods and solutions presented in or related to them by using document reviews and by different types of inspections. The inspections may be either announced or un-announced.

607. The inspections on the information security and security culture of construction phase may be integrated with STUK's other inspection activities.

608. At its discretion, STUK may participate in the audits and reviews performed by the licence applicant during construction. STUK shall be notified of any audits or reviews sufficiently early.

6.4 Operating licence stage

609. When the operating licence is applied for, STUK issues a statement on the application to the Ministry of Employment and the Economy and attaches into the statement its safety assessment and an assessment on the documents required in the Nuclear Energy Decree, Section 36. While preparing the safety assessment, STUK requests the Ministry of Interior for a statement on the reports referred to in Section 36(7) of the Nuclear Energy Decree concerning the nuclear security and emergency arrangements [15].

610. STUK verifies the sufficiency of the documents mentioned in section 5.4 and the sufficiency of the methods and solutions presented in or related to them by using document reviews and by different types of inspections. The inspections may be either announced or un-announced.

611. The inspections on the information security and security culture of operation license phase may be integrated with STUK's other inspection activities.

6.5 Operation stage

612. STUK's approval shall be sought for the plans and documents mentioned in section 5.5 and for any revisions concerning them, or they shall be submitted for information, as mentioned in section 5.5. STUK verifies the sufficiency of the documents mentioned in section 5.5 and the sufficiency of the methods and solutions presented in or related to them by using document reviews and by means of different types of inspections. The inspections may be either announced or un-announced.

613. The inspections on the information security and security culture of the operation phase may be integrated with STUK's other inspection activities.

614. At its discretion, STUK may participate in the audits and reviews related to information security that are performed by the licence applicant during operation. Any audits or reviews shall be notified of sufficiently early.

615. STUK supervises the functions of the information security management system as part of the operation stage inspection program. In addition, STUK makes inspections at the request of the licensee and at its discretion. The inspections may be targeted at the licensee or at a supplier working for the licensee. The inspections may be either announced or un-announced.

6.6 Decommissioning stage

616. In the decommissioning stage, STUK supervises the storage of the licensee's information security related information, and the safe destruction of the information and systems.

617. STUK supervises that the information security functions are sufficient to repel the threat of unlawful action and to ensure nuclear safety even during the decommissioning.

618. STUK verifies the sufficiency of the documents related to decommissioning, and the sufficiency of the methods and solutions presented in or related to them, by using document reviews and by means of different types of inspections. The inspections may be either announced or un-announced.

Definitions

Risk analysis

Risk analysis shall refer to examinations performed by using systematic measures in order to identify threats, problems, and vulnerabilities, surveying the causes and consequences thereof, and assess the related risks. (Government Decree 734/2008)

Security arrangements

Security arrangements shall refer to the measures needed to protect the use of nuclear energy against illegal activities in the nuclear facility, its precincts other places or vehicles where nuclear energy is used.

System (information security)

System in the context of information security shall refer to a system consisting of persons, information processing equipment, data transfer equipment and software intended to intensify or facilitate a certain function or to make it possible. The system may be an information system, a communications system, an electrical or I&C system, or a communication system for security surveillance or emergency preparedness.

Information security management system

An information security management system shall refer to a part of the nuclear facility's general management system that is created and implemented, used, supervised, reviewed, maintained, and continuously improved. The information security management system comprises the structure of the organisation, the information security management policy, planning activities, responsibilities, procedures, methods, processes, and resources.

References

1. Nuclear Energy Act (990/1987).
2. Government Decree on the Security in the Use of Nuclear Energy (734/2008).
3. Government Decree on the Safety of Nuclear Power Plants (717/2013).
4. Act on the Openness of Government Activities (621/1999).
5. ISO/IEC 27002. Information technology — Security techniques — Code of practice for information security management.
6. ISO/IEC 27001:fi. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden Hallintajärjestelmät. Vaatimukset.
7. ISO/IEC 27005. Information technology – Security techniques – Information security risk management.
8. IEC 62443 series.
9. Vahti 6/2006. Setting and measuring information security objectives.
10. Vahti 2/2010. Instructions on Implementing the Decree on Information Security in Central Government.
11. Vahti 1/2013. Information security procedure for application development.
12. COBIT. Control Objectives for Information and Related Technology.
13. KATAKRI II National Security Auditing Criteria, or the latest confirmed version.
14. NIST 800 series.
15. Nuclear Energy Decree (161/1988).
16. Government Decree on amending the Nuclear Energy Decree (755/2013).
17. Government Decree on the Safety of Disposal of Nuclear Waste (736/2008).
18. ISO/IEC 31000. Risk management – Principles and guidelines.