# GUIDE YVL A.12

# INFORMATION SECURITY MANAGEMENT OF A NUCLEAR FACILITY



Definitions

## 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.*

According to 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.*

With regard to new nuclear facilities, this Guide shall apply as of 1 March 2021 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. This Guide replaces Guide YVL A.12 (22.11.2013).

Translation. Original text in Finnish.

**STUK • SÄTEILYTURVAKESKUS**
**STRÅLSÄKERHETSCENTRALEN**
**RADIATION AND NUCLEAR SAFETY AUTHORITY**
Osoite / Address • Laippatie 4, 00880 Helsinki
Postiosoite / Postal address • PL / P.O.Box 14, FI-00811 Helsinki, FINLAND
Puh. / Tel. (09) 759 881, +358 9 759 881 • Fax (09) 759 88 500, +358 9 759 88 500 • www.stuk.fi

# 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 STUK Regulation on Security in the Use of Nuclear Energy (STUK Y/3/2020) [2]. According to Section 4(5) of the Regulation, *appropriate information/cyber security principles shall be used in the design and maintenance of systems and components. Appropriate methods and related plans shall be in place for detecting and preventing unauthorised action targeted towards systems and components that are important to safety and information/cyber security deviations, as well as for limiting their detrimental consequences.* According to Section 4(6) of the Regulation STUK Y/3/2020, *in the use of nuclear energy, preparations shall be made for managing abnormal situations arising from information/cyber security threats.* **[**2021-02-12 **]**

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. **[**2021-02-12 **]**

103. The Nuclear Energy Act (990/1987) [1], and the STUK Regulations on Security in the Use of Nuclear Energy (STUK Y/3/2020) [2] and on the Safety of Nuclear Power Plant (STUK Y/1/2018) [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 “Security of a nuclear facility”, 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. **[**2021-02-12 **]**

104. Information security refers to the appropriate protection of information, systems, equipment, services and data communication under normal and exceptional conditions. The integrity, availability and confidentiality of information shall be protected against threats and

damage caused by equipment and software failures, natural disasters and negligent or accidental acts. Information security is part of the licensee's management system and security arrangements. **[**2021-02-12 **]**

105. Information security covers maintaining the integrity, availability and confidentiality of information in all its forms, from the creation of information until its destruction. **[**2021-02-12 **]**

## 2 Scope of application

201. This Guide sets forth the regulations concerning information security of an organisation applying for a construction or operating licence for a nuclear facility, or one constructing or operating a nuclear facility, 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. Chapters 1, 2 and 3 of the Guide, excluding requirements 324, 325 and 326, shall be applied to other use of nuclear energy. Requirements important to information security and the regulatory control performed by STUK are also described in the A series YVL Guides and in the Guides

- B.1 Safety design of a nuclear power plant
- B.2 Classification of systems, structures and components of a nuclear facility
- B.7 Provisions for internal and external hazards at a nuclear facility
- C.5 Emergency arrangements of a nuclear power plant
- E.7 Electrical and I&C equipment of a nuclear facility.

**[**2021-02-12 **]**

# 3 Information security management

## 3.1 Information security management system

301. The management of the licensee shall demonstrate commitment to information security management. **[**2021-02-12 **]**

302. The licencee shall have an information security management system that is part of the management system. **[**2021-02-12 **]**

303. According to standard SFS:EN ISO/IEC 27000 [19], *an information security management system consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.* **[**2021-02-12 **]**

303a. The information security management system shall cover the actions and procedures to select, implement and improve appropriate controls. **[**2021-02-12 **]**

303b. The information security management system shall cover the guidance and supervision of external resources in terms of information security. **[**2021-02-12 **]**

304. Where applicable, the international information security standards and guidelines [19] shall be taken into consideration in the development of the information security management system. **[**2021-02-12 **]**

304a. Where applicable, the national guidelines [9, 10, 13] shall be taken into consideration in the development of the information security management system. **[**2021-02-12 **]**

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; information security shall not jeopardise communicating an up-to-date situational awaressness. **[**2021-02-12 **]**

306. According to Section 25 of Regulation STUK Y/1/2018 and Section 38 of Regulation STUK Y/4/2018, *when designing, constructing, operating and decommissioning a nuclear facility, a good safety culture shall be maintained.* This requirement also applies to the management of information security. **[**2021-02-12 **]**

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. **[**2013-11-22 **]**

308. The licensee shall define the information security management policy, which may be an individual document or part of a larger set of documentation. **[**2021-02-12 **]**

309. The information security management system shall include the objectives for information security. **[**2021-02-12 **]**

309a. Meeting the information security objectives shall be tracked, and the objectives shall be evaluated by applying the principle of continuous improvement. **[**2021-02-12 **]**

310. The information security management system shall describe the information security organisation. The description shall also take into consideration any external parties and their responsibilities. **[**2021-02-12 **]**

310a. 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. **[**2021-02-12 **]**

311. The procedures according to the Government Decree (1101/2019) [20] and the Council Decision (2013/488/EU) shall be used to protect non-public information given to the licensee by the authorities. Instructions are available, for example, in the VAHTI instructions [9]. The National Security Auditing Criteria (KATAKRI) [13], for example, may be used to evaluate the level of information security in the protection. **[**2021-02-12 **]**

311a. According to Section 6 of the Government Decree on Security Classification of Documents in Central Government (1101/2019), *a central government authority shall ensure in advance that the protection of a classified document is duly organised if the authority grants access to a classified document to a party other than a central government authority.*
Before disclosure of documentation containing information that is classified by an authority, confidential or derived from these types of information to a third party, the licensee shall have the approval of the Radiation and Nuclear Safety Authority for disclosure of the information. **[**2021-02-12 **]**

312. The licensee shall have procedures in place for the assessment and management of information security risks. **[**2021-02-12 **]**

312a. The licensee shall ensure that the procedures used to assess information security risks are sufficient and that any significant risks have been identified. **[**2021-02-12 **]**

313. Removed. **[**2021-02-12 **]**

314. The licensee shall draw up an information security threat and risk analysis, and it shall be updated regularly and whenever significant changes with an impact on information security take

place or new threats emerge. [2021-02-12 ]

315. Threats and risks to information security shall be analysed in a systematic manner, and protective measures and methods shall be selected on the basis of the analysis. [2021-02-12 ]

316. The assets to be protected shall be identified and defined in sufficient detail. [2021-02-12 ]

316a. The threats, vulnerabilities and effects of information security events related to the assets to be protected shall be analysed, and the necessary controls shall be defined based on them. [2021-02-12 ]

316b. The controls shall be documented. [2021-02-12 ]

317. Moved to para. 419a and 419b. [2021-02-12 ]

### 3.2 Requirements for protecting information

318. The general requirements for the documents are presented in Guides YVL A.1 “Regulatory oversight of safety in the use of nuclear energy”, YVL A.3 “Leadership and management for safety”, and YVL A.11 “Security of nuclear facility”. [2021-02-12 ]

319. Information shall be classified according to its significance for the information security and safety of the facility. [2021-02-12 ]

319a. Information shall be protected against unauthorised use, modification and deletion as required by the classification. The availability of information to authorised users shall be ensured. [2021-02-12 ]

### 3.3 Resource management

320. Guides YVL A.4 “Organisation and personnel of a nuclear facility” and A.11 “Security of a nuclear facility” present the general requirements in terms of resource management. The resources shall include personnel resources, the necessary expertise and tools. [2021-02-12 ]

320a. The licensee shall ensure the availability of adequate resources and competences for the planning, implementation, evaluation and continuous improvement of information security management [2021-02-12 ]

321. The key personnel and other resources related to information security management shall be employed or owned by the licensee. [2021-02-12 ]

321a. 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. [2021-02-12 ]

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. **[**2021-02-12 **]**

322a. The entire personnel of the nuclear facility and external resources shall be aware of issues related to information security to the extent required for the performance of their tasks. **[**2021-02-12 **]**

322b. A participant register shall be kept for information security training. **[**2021-02-12 **]**

323. When using external resources, the licensee shall ensure that the level of information security and assignment of responsibilities are at a level that at least corresponds to the licensee's standards for similar activities. **[**2021-02-12 **]**

323a. The licensee shall have procedures in place to supervise the information security of external resources. The monitoring shall take into account subcontracting chains. Guides YVL A.3 "Leadership and management for safety" and YVL A.5 "Construction and commissioning of a nuclear facility" present requirements for the monitoring of suppliers. **[**2021-02-12 **]**

### 3.4 Assessments, audits and reviews of the information security management system

324. The licensee shall arrange an annual self-assessment of the information security management system. The scope of the assessment shall ensure that all areas are assessed at least once every three years. Changes to the risk assessment and the envisioned threats and the information security events during the period shall also be taken into account in the assessment of the suitability and adequacy of the management system. **[**2021-02-12 **]**

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. **[**2021-02-12 **]**

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. **[**2013-11-22 **]**

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. **[**2013-11-22 **]**

328. Removed. **[**2021-02-12 **]**

329. The audits, assessments and reviews and their results shall be documented. **[**2021-02-12 **]**

### 3.5 Improving the information security management system

330. Continuous improvement shall take into account the results of the assessments, audits, reviews and exercises and the operating experience from information security management in the licensee's own field of business and other fields of business. **[**2021-02-12 **]**

331. The management shall promote ways by which the entire personnel can participate in the implementation and continuous improvement of the information security management system. **[**2021-02-12 **]**

332. The licensee's management shall ensure that any improvements made to the information security management system are aligned with the set goals. **[**2021-02-12 **]**

# 4 Protecting systems that are important to safety and security

401. Removed. [2021-02-12 ]

## 4.1 General requirements

402. The information security and architecture of any equipment and systems that directly or indirectly affect the safety or security of a nuclear facility shall be designed in a manner that employs information security controls and security arrangements to prevent unauthorised access as well as is reasonably achievable. [2021-02-12 ]

402a. Information security shall be taken into account throughout the entire life cycle of a nuclear facility, also later on during renovations and modifications. The specified controls shall be in place, and they shall be monitored, reviewed and, if necessary, improved. [2021-02-12 ]

403. The installation of unauthorised devices shall be prevented throughout the entire life cycle. [2021-02-12 ]

403a. The installation of unauthorised software shall be prevented throughout the entire life cycle. [2021-02-12 ]

403b. Accesses to the electrical and I&C systems and components, and any modifications made to the software and parameters during such accesses, shall be traceable. [2021-02-12 ]

404. 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 shall be protected. [2021-02-12 ]

404a. The documents and information pertaining to information systems, communications systems, electrical and I&C systems, networked equipment and standalone systems, security surveillance systems and communications systems for emergency preparedness shall be protected to a degree necessitated by their security significance and in a manner where they can only be accessed by authorised persons. [2021-02-12 ]

404b. In connection with system changes as referred to section 6.2 of Guide YVL B.1 and plant modifications as referred to in Guide YVL A.5, the plant- and system-level information security requirements shall be reassessed. The assessment shall also cover systems and interfaces in connection with the system to be replaced. [2021-02-12 ]

405. Networked equipment means all devices that are connected to other devices in a way that they can be used for communication. The related physical cabling and communications shall be protected against unauthorised actions. [2021-02-12 ]

405a. The physical and logical separation of the networks shall be implemented as well as is practically achievable, while taking the security significance of the networks into consideration. **[**2021-02-12 **]**

405b. 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. **[**2021-02-12 **]**

405c. No physical possibility shall exist for the establishment, from outside the system inwards, of a data transfer connection not included in the system to the software-based systems important to the safety of a nuclear facility as referred to in Guide YVL E.7. **[**2021-02-12 **]**

405d. The protection I&C system referred to in section 5.2.5 of Guide YVL B.1 shall be functionally separated from the other I&C systems so that networked data transfer towards the protection I&C system is prevented through unidirectional separation at the physical level. **[**2021-02-12 **]**

405e. The interface between the I&C architecture and the administrative computer systems shall be implemented by making the transmission of data unidirectional in such a way that any transmission of data towards the I&C architecture is prevented through separation at the physical level. **[**2021-02-12 **]**

405f. A software-based arrangement of unidirectional data transfer shall not be considered a sufficient means of protection to meet the requirement laid down of requirements 405c, 405d and 405e. **[**2021-02-12 **]**

405g. 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. **[**2021-02-12 **]**

405h. 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. **[**2021-02-12 **]**

406. The possibility that an individual person could install a malicious functionality in several redundant devices or systems that perform the same safety function shall be restricted. **[**2021-02-12 **]**

406a. The effect of a single device or a piece of software on the reduction of the nuclear facility’s overall safety or security shall be as low as is reasonably achievable. **[**2021-02-12 **]**

406b. A system shall be in place to reliably detect the installation of any malicious functionalities or the deactivation of any protection functions **[**2021-02-12 **]**

407. Moved to para. 404a. **[**2021-02-12 **]**

408. Removed. **[**2021-02-12 **]**

409. Removed. **[**2021-02-12 **]**

410. Removed. **[**2021-02-12 **]**

411. Removed. **[**2021-02-12 **]**

412. Removed. **[**2021-02-12 **]**

413. Moved to para. 405g. **[**2021-02-12 **]**

414. Moved to para. 405h. **[**2021-02-12 **]**

### 4.2 Information security event management

415. In the information security management system, there shall be procedures in place for the detection, identification and processing of information security deviations. In the management system, there shall be procedures in place for the prevention and limitation of negative consequences. **[**2021-02-12 **]**

415a. The detection and management of information security deviations shall be practised. STUK shall be informed of the exercises in advance. **[**2021-02-12 **]**

416. Removed. **[**2021-02-12 **]**

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. **[**2021-02-12 **]**

417a. STUK shall be informed as soon as possible of all identified threats, events and phenomena at the plant concerning or related to information security that may be significant in terms of nuclear safety or be newsworthy nationally or internationally. **[**2021-02-12 **]**

### 4.3 Access control

418. The licensee shall draw up, document and review the principles for access control. **[**2021-02-12 **]**

418a. The users' access rights shall be reviewed regularly and whenever work tasks are changed. **[**2021-02-12 **]**

418b. A password policy shall be defined and implemented, and its implementation shall be monitored. **[**2021-02-12 **]**

419. Administrator rights shall be limited system-specifically. Access shall only be granted when it is required to perform work tasks. **[**2021-02-12 **]**

419a. Access to the protected items shall be controlled and monitored using access control and log procedures. The log entries shall include the necessary information that is required to trace the event and the user. **[**2021-02-12 **]**

419b. The log files shall be protected against unauthorised modifications. **[**2021-02-12 **]**

420. Moved to para. 418a. **[**2021-02-12 **]**

421. Moved to para. 418b. **[**2021-02-12 **]**

422. Removed. **[**2021-02-12 **]**

### 4.4 Security testing of systems

423. The information security of security surveillance systems shall be tested. Security testing can also be performed during the drills arranged to demonstrate the effectiveness of security arrangements pursuant to Guide YVL A.11. **[**2021-02-12 **]**

424. The system qualification and testing of I&C system platforms and electrical and I&C equipment and systems referred to in Guide YVL E.7 shall take information security into consideration. **[**2021-02-12 **]**

425. The testing of networks related to I&C architecture, especially plant networks, shall utilise advanced methods. **[**2021-02-12 **]**

426. Removed. **[**2021-02-12 **]**

# 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. **[**2021-02-12 **]**

## 5.2 Construction licence stage

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

1. The licence applicant's information security management policy in accordance with requirement 308 and description of the information security management system in accordance with section 3.1, providing comprehensive idea of the management of information security and information security risks.
2. The information security requirements of plant-level design.
3. The architecture-level information security plans including a description of connections between systems.

**[**2021-02-12 **]**

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

1. The procedures related to the classification and processing of documents and information.
2. The system-specific information security requirements.
3. A description of the information security organisation during construction in accordance with requirement 310.
4. A plan concerning the information security supervision activities that are applied to suppliers during the construction of the nuclear facility in accordance with requirement 323a.

**[**2021-02-12 **]**

504. Removed. **[**2021-02-12 **]**

505. Removed. **[**2021-02-12 **]**

### 5.3 Construction stage

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

1. Significant changes to the documents referred to in requirement 502.
2. System platform-, system- or device-specific security test plans in accordance with section 4.4.

**[**2021-02-12 **]**

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

1. Significant changes to the documents referred to in requirement 503.
2. Security test reports in accordance with section 4.4.

**[**2021-02-12 **]**

508. Removed. **[**2021-02-12 **]**

509. Removed. **[**2021-02-12 **]**

### 5.4 Operating licence stage

510. Removed. **[**2021-02-12 **]**

511. For the processing of the operating licence application, the documents from the construction licence and construction phase shall be submitted to STUK in their final form, along with other documents and clarifications required by STUK, to verify the sufficient level of information security. The documents needed for the processing of the operating licence application are the following:

1. A description of the information security management system during the operation phase.
2. An analysis of the fulfilment of information security requirements at the plant, architecture and system levels.
3. A description of the information security organisation during the operation phase.

**[**2021-02-12 **]**

### 5.5 Operation stage

512. During the operation phase, the following shall be submitted to STUK for information:

1. In connection with a plant or system change, the assessment referred to in requirement 404b and the updated requirements.
2. Updates of documents in accordance with requirement 511.

**[**2021-02-12 **]**

513. Removed. **[**2021-02-12 **]**

514. Removed. **[**2021-02-12 **]**

### 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. **[**2013-11-22 **]**

# 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), 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. **[**2021-02-12 **]**

## 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(1) of the Nuclear Energy Decree concerning the nuclear security and emergency arrangements. **[**2021-02-12 **]**

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 un-announced. **[**2021-02-12 **]**

604. The inspections on the information security and security culture of construction license phase may be integrated with STUK's other inspection activities. **[**2013-11-22 **]**

605. At its discretion, STUK may participate in the information security audits and reviews performed during the construction licence phase.
STUK shall be notified of any audits or reviews sufficiently early. **[**2021-02-12 **]**

605a. At a location indicated by the license applicant, STUK shall inspect the results of the threat and risk analysis in accordance with requirement 314. **[**2021-02-12 **]**

## 6.3 Construction stage

606. 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. **[**2021-02-12 **]**

607. The inspections on the information security and security culture of construction phase may be integrated with STUK's other inspection activities. **[**2013-11-22 **]**

608. At its discretion, STUK may participate in the information security audits and reviews performed during the construction phase. STUK shall be notified of any audits or reviews sufficiently early. **[**2021-02-12 **]**

608a. At a location indicated by the construction licence holder, STUK shall inspect the reports on supervision activities in accordance with requirement 323a, assessment reports in accordance with requirement 324 and assessment reports in accordance with requirement 325. **[**2021-02-12 **]**

### 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(1) of the Nuclear Energy Decree concerning the nuclear security and emergency arrangements. **[**2021-02-12 **]**

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. **[**2013-11-22 **]**

611. The inspections on the information security and security culture of operation license phase may be integrated with STUK's other inspection activities. **[**2013-11-22 **]**

611a. At a location indicated by the licence applicant, STUK shall inspect the results of the operation-phase threat and risk analysis in accordance with requirement 314. **[**2021-02-12 **]**

### 6.5 Operation stage

612. 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. **[**2021-02-12 **]**

613. The inspections on the information security and security culture of the operation phase may be integrated with STUK's other inspection activities. **[**2021-02-12 **]**

614. At its discretion, STUK may participate in the information security audits and reviews performed during the operation phase. STUK shall be notified of any audits or reviews in good time. **[**2021-02-12 **]**

615. STUK supervises the functions of the information security management system as part of the operation stage inspection program. In addition, STUK makes other inspections 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 unannounced. **[**2021-02-12 **]**

615a. At a location indicated by the licensee, STUK shall inspect the reports on supervision activities in accordance with requirement 323a, assessment reports in accordance with requirement 324, assessment reports in accordance with requirement 325 and up-to-date results of the threat and risk analysis in accordance with requirement 314. **[**2021-02-12 **]**

### 6.6 Decommissioning stage

616. In the decommissioning stage, STUK supervises the processing of information to be protected at its discretion. **[**2021-02-12 **]**

617. Removed. **[**2021-02-12 **]**

618. Removed. **[**2021-02-12 **]**

## 7 References

1. Nuclear Energy Act (990/1987). **[**2013-11-22 **]**

2. Radiation and Nuclear Safety Authority Regulation on Security in the Use of Nuclear Energy (STUK Y/3/2020). **[**2021-02-12 **]**

3. Radiation and Nuclear Safety Authority Regulation on the Safety of a Nuclear Power Plant (STUK Y/1/2018). **[**2021-02-12 **]**

4. Act on the Openness of Government Activities (621/1999). **[**2013-11-22 **]**

5. Removed. **[**2021-02-12 **]**

6. Removed. **[**2021-02-12 **]**

7. Removed. **[**2021-02-12 **]**

8. Removed. **[**2021-02-12 **]**

9. Vahti, www.vahtiohje.fi. **[**2021-02-12 **]**

10. Removed. **[**2021-02-12 **]**

11. Removed. **[**2021-02-12 **]**

12. Removed. **[**2021-02-12 **]**

13. KATAKRI, National Security Auditing Criteria (2020). **[**2021-02-12 **]**

14. Removed. **[**2021-02-12 **]**

15. Nuclear Energy Decree (161/1988). **[**2013-11-22 **]**

16. Removed. **[**2021-02-12 **]**

17. Removed. **[**2021-02-12 **]**

18. Removed. **[**2021-02-12 **]**

19. SFS-EN ISO/IEC 27000. Information technology. Security techniques. Information security management systems. Overview and vocabulary. **[**2021-02-12 **]**

20. Government Decree on Security Classification of Documents in Central Government (1101/2019). **[**2021-02-12 **]**

21. Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU). **[**2021-02-12 **]**

# Definitions

**System (information security)**

System in the context of information security shall refer to a system consisting of 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.

**Risk analysis**

Risk analysis shall refer to examinations, performed using systematic measures, in order to 1) identify threats, problems and vulnerabilities, 2) identify the reasons for them, and 3) assess and classify the consequences and related risks of undesirable situations. (STUK Y/3/2020)

**Information security management system**

An information security management system consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets.

**Nuclear security**

Nuclear security shall refer to the measures needed to protect the use of nuclear energy against activity that could endanger nuclear or radiation safety in the nuclear facility, its precincts other places or vehicles where nuclear energy is used. (Nuclear Energy Act 990/1987)