

# SECURITY RULES FOR REGULAR CONTRACTORS

---

## 1 INFORMATION SECURITY MANAGEMENT

---

- 1.1 The supplier undertakes
    - 1.1.1 manage own risks that may affect the provision of the subject delivery;
    - 1.1.2 on the basis of security needs and the results of risk assessment, implement appropriate security measures within the scope of the provided subject of delivery, monitor them, evaluate their effectiveness;
    - 1.1.3 keep records on the creation and processing of data and information within the scope of the provided subject of delivery, record all significant circumstances related to ensuring the security of this data and information and, upon request, these records of ANS CR make available;
    - 1.1.4 if a subcontractor is in the provision of the delivery subject, ensure adequate compliance with these security requirements also in the contractual relations with its subcontractors.
- 

## 2 PERSONAL SECURITY

---

- 2.1 The supplier shall ensure that all persons participating in the performance according to the concluded contract with ANS CR are acquainted with these safety rules and other specifying safety information demonstrably provided by ANS CR.
  - 2.2 Persons participating in the performance according to the concluded contract with ANS CR must have demonstrable necessary qualification prerequisites, experience and knowledge.
  - 2.3 The supplier must ensure that the persons participating in the performance according to the concluded contract with ANS CR have undergone a screening process and conditions and responsibilities have been set for their activities.
  - 2.4 The supplier must ensure in a verifiable form an adequate awareness of the security of information of persons participating in the performance according to the concluded contract with ANS CR.
  - 2.5 The supplier must have in place a process for terminating or changing the employment of an employee participating in the performance according to the concluded contract with ANS CR.
- 

## 3 PHYSICAL SAFETY, FIRE PROTECTION, AND HEALTH AND SAFETY

---

- 3.1 Conditions and rules of physical safety, fire protection and safety and health protection at work are described in the contract with ANS CR.
- 

## 4 OPERATIONAL MANAGEMENT

---

The supplier undertakes to ensure the secure operation of the information system and infrastructure used for the provision of the subject of performance in accordance with the recommendations of the ISO / IEC 27000 series of technical standards.

---

## 5 ACCESS MANAGEMENT

---

- 5.1 Identification
    - 5.1.1 Each employee of the supplier participating in the performance of the contract by the supplier's resources must have registered and maintain its own unique user account within its IT infrastructure, to which specific roles are assigned in individual designated systems, modules or applications. Each employee of the supplier must be kept with valid identification and current contact details.
    - 5.1.2 Each employee of the supplier, if he/she has access into the internal systems of ANS CR has a unique user account with ANS CR who is assigned specific roles in individual systems, modules or applications related exclusively to the performance of the subject of the contract.
-

## 5.2 Authentication

### 5.2.1 Conditions for authentication when using the ICT infrastructure of ANS CR

- a) multi-factor authentication is used to uniquely identify privileged users on designated systems;
- b) password authentication - if it is not possible to use unambiguous identification of privileged users by multiple factors, authentication using cryptographic keys is used to guarantee a similar level of security or the use of a password with the required rules.

## 5.3 Authorization

5.3.1 The supplier's employees are obliged to use privileged rights in the ICT infrastructure of ANS only to a reasonable extent and only for the time strictly necessary for the performance of activities in accordance with the performance of the subject of the contract. Users and administrators may not use accounts with privileged privileges for routine work unrelated to the administration of the designated system.

5.3.2 The supplier's employees are informed by ANS CR to which ANS CR protected information they have access and how they can handle it. Any manipulation and other operations with protected information of ANS CR, which were not explicitly stated in the instructions, are not permitted by the supplier.

## 5.4 Remote access

5.4.1 The workstation of the supplier accessing the infrastructure of ANS CR through VPN (Virtual Private Network) must have

- a) advanced functional anti-virus protection (with real time protection mod), certified according to AV-TEST APPROVED (av-test.org) or VB100 (virusbulletin.com) – valid for MS Windows and Android environments;
- b) working personal firewall;
- c) functionally set automatic system updates;
- d) operating system that is not outside the manufacturer's service support (unless expressly stated in the contractual agreement);
- e) updated third party applications in compliance with third party copyrights;
- f) encryption of all storage media on which the protected data and information of ANS CR must be provided. Access to storage media and decryption of protected data and information of ANS CR must be allowed only to authorized persons of the supplier;
- g) VPN client installed, installed purely at the expense of the supplier;
- h) second factor (HW or SMS token) for access to the VPN, which will be provided by a designated employee of ANS CR against the signing of the handover protocol.

---

## 6 CHANGE MANAGEMENT

---

6.1 The supplier undertakes

6.1.1 manage and record contractual changes;

6.1.2 manage and record changes in the services provided in accordance with the recommendations of the technical standards of the ISO / IEC 27000 series.

---

## 7 USING CRYPTOGRAPHIC MEANS

---

7.1 If the use of cryptographic means is required within the subject of performance, the technical conditions are as follows

7.1.1 encryption with a standardized symmetric password, the method of which is defined by ANS CR. The password must be passed through another communication channel;

7.1.2 encryption using digital certificates issued by a generally recognized CA or a CA that is explicitly trusted by both parties;

7.1.3 if the validity of the certificate against the CRL cannot be verified, the certificate is considered invalid and cannot be used for encryption or signing;

7.1.4 encryption using PGP keys agreed by both parties or verified by an independent trusted third party;

7.1.5 for VPN access to specified systems, a standardized defined cipher is used by ANS CR;

- 7.1.6 for web servers, presenting data originating from designated information systems outside the system itself, use the HTTPS protocol in ANS CR standardized cipher;
- 7.1.7 for web servers, presenting data originating from designated systems for users outside ANS CR, the EV certificate of a generally recognized certification authority is used.

---

## **8 MONITORING**

---

- 8.1 Access of the supplier's staff to selected internal information and to the information and telecommunication systems ANS CR is recorded, monitored and evaluated on a continuous basis. The system events are recorded in logs
  - 8.1.1 successful and unsuccessful user logins and logouts;
  - 8.1.2 activities performed by administrators;
  - 8.1.3 successful and unsuccessful manipulations of accounts, permissions and rights;
  - 8.1.4 non-performance due to lack of access rights;
  - 8.1.5 user activities, that may affect the security of the information and communication system;
  - 8.1.6 commencement and termination of technical asset activities;
  - 8.1.7 automatic warning or error messages of technical assets;
  - 8.1.8 access to logs, attempts to manipulate logs and changes the settings of the activity logging tool and the use of authentication mechanisms, including changing the data used for logging in.
- 8.2 The ANS CR assigns to each record in the log
  - 8.2.1 date and time;
  - 8.2.2 type of activity;
  - 8.2.3 the name of the relevant technical asset;
  - 8.2.4 the user identification;
  - 8.2.5 the originator's network equipment identification;
  - 8.2.6 success or failure of the activity;
  - 8.2.7 the severity level.
- 8.3 The supplier is obliged to continuously monitor within its ICT infrastructure published and known security errors that may affect the smooth and safe operation of systems related to the services provided by it. These include vulnerabilities in operating systems, third-party software, web components, etc.

---

## **9 DATA REPOSITORY AND MEDIA PROTECTION**

---

- 9.1 The storage of ANS CR protected data on data repository, portable media and transfer of thereof outside premises of ANS CR requires prior approval of ANS CR.
- 9.2 In the case of storing protected information of ANS CR on data repository and portable media, the supplier is obliged, if technically possible, to store or require storage of this data in encrypted form and keep records of these media.
- 9.3 The supplier is obliged to ensure the disposal of operational data containing protected information of ANS CR immediately after disregarding the purpose of their processing and / or storage in accordance with the [NIST 800-88](#) standard. It must not be possible to recover the information after disposal of the data on the electronic medium. The supplier must keep a report on the disposal of data.

---

## **10 CYBER SECURITY EVENTS / INCIDENTS**

---

- 10.1 The supplier is obliged to report all suspicions of cyber security events / incidents
  - 10.1.1 responsible person ANS CR;
  - 10.1.2 in the period immediately (without delay) after the detection of the cyber security event / incident;

- 10.1.3 by hand, by e-mail, by telephone with the registration of the call on both sides, or in person;
- 10.1.4 with description
- a) date and time of discovery;
  - b) the nature of the event;
  - c) event sources;
  - d) the goals / victims of the event;
  - e) potential impact.

---

## **11 PROTECTING ASSETS AGAINST UNAUTHORIZED ACTIVITIES**

---

The supplier does not install and use tools for the assets of ANS CR, which are not part of the subject of performance.

---

## **12 CONDITIONS FOR TERMINATION OF THE CONTRACT**

---

- 12.1 In the event of termination of the contractual relationship, all access of the supplier and its employees to the assets of ANS CR no later than the date of termination of the contractual relationship.
- 12.2 If the assets of ANS CR have been provided to the supplier's employees, these assets must be returned no later than the date of termination of the contractual relationship.
- 12.3 If information assets (data) of ANS CR have been provided to the supplier, they must be returned and completely deleted in accordance with [NIST 800-88](#) from all systems of the supplier and the supplier's media containing such assets by the date of termination of the contractual relationship.