

SECURITY RULES FOR MAJOR CONTRACTORS

PURSUANT TO ACT NO. 181/2014 COLL., ON CYBER SECURITY AND ON AMENDMENTS TO RELATED ACTS (CYBER SECURITY ACT, AS AMENDED)

1 INFORMATION AND CYBER SECURITY MANAGEMENT

- 1.1 The supplier is obliged to implement these measures in its internal processes
 - 1.1.1 shall have a Security Awareness Development Plan in place, the aim of which is to ensure adequate training and security awareness development and which contains:
 - a) instructions for users, administrators, persons performing security functions and subcontractors concerning their obligations and the security policy;
 - b) required theoretical and practical training of users, administrators and persons performing security functions;
 - 1.1.2 shall have appointed persons responsible for realization of the individual activities listed in the plan;
 - 1.1.3 shall instruct, in compliance with the Security Awareness Development Plan, users, administrators and persons holding security roles and subcontractors on their obligations and on the security policy by means of initial and recurrent training;
 - 1.1.4 in compliance with the Security Awareness Development Plan, ensure for persons holding security roles regular professional training based on the current needs as regards cybersecurity;
 - 1.1.5 shall ensure, in compliance with the Security Awareness Development Plan, regular training and verification of the employees' security awareness according to their job responsibilities;
 - 1.1.6 shall ensure inspections of compliance with the security policy by users, administrators and persons holding security roles and has set up a disciplinary procedures for its employees;
 - 1.1.7 shall ensure handover of responsibilities if the contractual relationship with the administrators and persons holding security roles is terminated;
 - 1.1.8 shall evaluate the efficacy of the Security Awareness Development Plan, of the training having been realized as well as of other activities related to development of the security awareness;
 - 1.1.9 shall determine rules and procedures to deal with cases of breaches of the established security rules by users, administrators and persons holding security roles;
 - 1.1.10 shall keep records of training containing the subject matter of the training and a list of persons who attended it.
 - 1.1.11 transmits to ANS CR, s. p. information concerning persons related to the provided subject of performance of the contract, about the performed training and its content at least once a year.
- 1.2 Shall ensure adequate compliance with these security rules also in contractual relations with his subcontractors, if the supplier uses them.
- 1.3 ANS CR, s. p. reserves the right to keep records of and check the Contractor's activities, keep records of incidents and unusual activities of the employees and other persons operating in favour or on behalf of the Contractor (hereinafter referred to as "Contractor's Staff"). Based on those records, ANS CR shall be entitled to evaluate the trustworthiness and reliability of the Contractor's Staff. In the event of any identified risk, the ANS CR shall inform the Contractor of a non-conformity and both parties shall enter into dealings to solve the situation.

2 PERSONAL SECURITY

- 2.1 The Supplier shall ensure that all persons participating in the performance according to the concluded contract with ANS CR, s. p. are acquainted with these safety rules and other specifying safety information demonstrably provided by ANS CR, s. p.
- 2.2 Persons participating in the performance according to the concluded contract with ANS CR, s. p. 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, s. p. have undergone a screening process and conditions and responsibilities have been set for their activities.

3 PHYSICAL SAFETY, FIRE PROTECTION, AND HEALTH AND SAFETY

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

4 OPERATIONAL MANAGEMENT

- 4.1 The supplier undertakes
- 4.1.1 to ensure the secure operation of the information system and infrastructure used for the provision of the subject of performance in accordance with the requirements of Decree No. 82/2018 Coll., on security measures, cyber security incidents, reactive measures on cyber security), as amended (hereinafter "VoKB") and the recommendations of the ISO / IEC 27000 series of technical standards;
- 4.1.2 upon request provide ANS CR, s. p. with an overview of security measures, implemented on its information system and infrastructure, which fulfill the subject of the contract.

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 Autentication
- 5.2.1 Conditions for authentication when using the ICT infrastructure of ANS CR, s. p.:
- multi-factor authentication is used to uniquely identify privileged users on designated systems;
 - 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, s. p. to which ANS CR, s. p. protected information they have access and how they can handle it. Any manipulation and other operations with protected information of ANS CR, s. p., 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, s. p. through VPN (Virtual Private Network) must have:
- advanced functional anti-virus protection (with realtime protection mod), certified according to AV-TEST APPROVED (av-test.org) or VB100 (virusbulletin.com) – valid for MS Windows and Android environments;
 - working personal firewall;
 - 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, s. p. must be provided. Access to storage media and decryption of protected data and information of ANS CR, s. p. 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 Conditions

- 6.1.1 changes on the part of the supplier must be managed with regard to the criticality of information, systems, processes and risk reassessment.

6.2 The supplier undertakes

- 6.2.1 manage and record contractual changes;
- 6.2.2 manage and record changes in the services provided in accordance with the requirements of VoKB and the recommendations of the technical standards of the ISO / IEC 27000 series.

7 ACQUISITION, DEVELOPMENT AND MAINTENANCE

7.1 The supplier undertakes

- 7.1.1 ensure safe implementation, innovation, updating, testing of technologies that are the subject of performance;
- 7.1.2 submit to ANS CR, s. p. the documentation of the subject of performance at least to the following extent:
 - a) documentation of the actual design;
 - b) documentation of all safety settings, functions and mechanisms;
 - c) documentation containing a description of the authorization concept and authorization;
 - d) documentation containing backup and archiving procedures;
 - e) documentation containing installation and configuration procedures;
 - f) documentation including vulnerability tests and compliance with the safety requirements of ANS CR, s. p.;
 - g) documentation to ensure continuity of operation and disaster recovery.

7.2 In the case of solution development, the supplier undertakes

- 7.2.1 adhere to and implement best practices for secure software development according to the recommendations of the ISO / IEC 27000 series of technical standards;
- 7.2.2 if the software audit activities and handover of the source code for solution are part of the performance under the contract, the audit of the performed or performed performance will be enabled and the developed source code for solution for code review will be submitted upon written request (automatically by security tool and manually), in particular in order to verify whether the performance has been carried out in accordance with the contract;
- 7.2.3 ensure that the performance contains only those components that are objectively necessary for the proper operation of the solution and / or that are explicitly specified in the contract (in particular, that the solution does not contain any unnecessary components, no program samples, etc.);
- 7.2.4 if the performance also includes the installation of the operating system or software of third parties, ensure during its installation that the prescribed versions of these products are compatible and functional in the environment of ANS CR, s. p.;
- 7.2.5 ensure the safety of the test environment at the supplier and the protection of the provided test data ANS CR, s. p.;

- 7.2.6 ensure that in the production environment of ANS CR only compiled or executable code specified by the subject of the contract and other necessary data for the operation of the subject of performance will be delivered;
- 7.2.7 ensure that the delivered solution will be in accordance with the recommendations of the ISO / IEC 27000 series of technical standards within the scope of the provided performance;
- 7.2.8 provide ANS CR with the necessary cooperation in the event that ANS CR requires / implements the performance of safety tests related to the subject of performance. In the event that the customer requires the supplier to perform security tests, it will be agreed in a separate contractual agreement;
- 7.2.9 submit the source code of ANS CR, if stipulated in the contract, in a secure form ensuring its integrity and in that case:
 - a) ensure source code version control;
 - b) ensure that source code is backed up and stored outside of the production environment;
 - c) ensure that the source code distribution includes a file from the development environment for a controlled compilation of that source code;
- 7.2.10 do not develop, compile and disseminate in the environment of ANS CR program code that aims to illegally control, violate availability, confidentiality or integrity, or unauthorized or illegally obtain data and information.

8 USING CRYPTOGRAPHIC MEANS

- 8.1 If the use of cryptographic means is required within the subject of performance, the technical conditions are as follows:
 - 8.1.1 encryption with a standardized symmetric password using at least AES 256, the password must be passed through another communication channel;
 - 8.1.2 encryption using digital certificates issued by a generally recognized CA or a CA that is explicitly trusted by both parties;
 - 8.1.3 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;
 - 8.1.4 encryption using PGP keys agreed by both parties or verified by an independent trusted third party;
 - 8.1.5 for VPN access to designated systems is used a standardized defined cipher AES256/SHA256 or stronger;
 - 8.1.6 for web servers presenting data originating from designated information systems outside the system itself, they use the HTTPS protocol with a least TLS 1.1 cipher;
 - 8.1.7 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.

9 MONITORING

- 9.1 Access of the supplier's staff to selected internal information and to the information and telecommunication systems is recorded, monitored and evaluated on a continuous basis. The system events are recorded in logs
 - 9.1.1 successful and unsuccessful user logins and logouts;
 - 9.1.2 activities performed by administrators;
 - 9.1.3 successful and unsuccessful manipulations of accounts, permissions and rights;
 - 9.1.4 non-performance due to lack of access rights;
 - 9.1.5 user activities, that may affect the security of the information and communication system;
 - 9.1.6 commencement and termination of technical asset activities;
 - 9.1.7 automatic warning or error messages of technical assets;

- 9.1.8 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.
- 9.2 The ANS CR, s. p. assigns to each record in the log
- 9.2.1 date and time;
 - 9.2.2 type of activity;
 - 9.2.3 the name of the relevant technical asset;
 - 9.2.4 the user identification;
 - 9.2.5 the originator's network equipment identification;
 - 9.2.6 success or failure of the activity;
 - 9.2.7 the severity level.
- 9.3 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.

10 DATA REPOSITORY AND MEDIA PROTECTION

- 10.1 The storage of ANS CR, s. p. protected data on data repository, portable media and transfer of thereof outside premises of ANS CR, s. p. requires prior approval of ANS CR, s. p.
- 10.2 In the case of storing protected information of ANS CR, s. p. 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.
- 10.3 The supplier is obliged to ensure the disposal of operational data containing protected information of ANS CR, s. p. 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.

11 CYBER SECURITY EVENTS / INCIDENTS

- 11.1 The supplier is obliged to report all suspicions of cyber security events / incidents
- 11.1.1 responsible person ANS CR, s. p.;
 - 11.1.2 in the period immediately (without delay) after the detection of the cyber security event / incident;
 - 11.1.3 by hand, by e-mail, by telephone with the registration of the call on both sides, or in person;
 - 11.1.4 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.

12 SUPPLIER AUDIT (CUSTOMER AUDIT)

- 12.1 Authorization to perform audit of the contractor
- 12.1.1 ANS CR, s. p. reserves the right to perform audits of the supplier.
 - 12.1.2 ANS CR, s. p. shall notify the supplier of the intention to perform an audit with sufficient advance notice of at least 5 working days. Both parties agree on the content, necessary cooperation and time schedule of the audit with the proviso that ANS CR, s. p., undertakes to proceed so as not to disrupt the operational needs of the supplier.

- 12.1.3 ANS CR, s. p. reserves the right in case of serious reasons (eg. suspicion of risky behavior of the supplier) in connection with the performance of the contract to perform an unannounced audit of the supplier, taking into account the operational situation of the supplier.
- 12.1.4 When critical information infrastructure elements related to the commission implementing regulation (EU) laying down common requirements for air traffic management / air navigation service providers and other air traffic management network functions and supervision (ANS provision) are audited, the auditor / inspector sets out the corrective actions to be identified and the date of their implementation. The supplier is obliged to implement corrective measures within the scope of the specified measure and within the required deadline.
- 12.1.5 Documentation of audits performed by ANS CR, s. p. is kept in the department responsible for conducting audits. Records related to a particular audit are always identified by the same identifier. Individual audit records consist of:
- a) audit plan;
 - b) audit notification;
 - c) audit questionnaire (list of auditor's questions if the auditor deems it appropriate);
 - d) audit report;
 - e) written, photographic or other records of the operation, procedures or equipment related to the audit (if necessary to document the findings);
 - f) record of findings (corrective actions and follow-up).
- 12.1.6 The audited party (supplier) will receive a final audit report with comments, including any findings, on the basis of which
- a) the supplier proposes, on the basis of the findings stated in the final audit report, a proposal of measures and deadlines for solutions and submits their list to ANS CR, s. p. for approval.
 - b) ANS CR, s. p. subsequently confirms its agreement with the proposed measures or returns them with comments to the supplier for revision.

12.2 Corrective actions

- 12.2.1 The audited party (supplier) is obliged to ensure the implementation of the agreed corrective measures within the specified time.
- 12.2.2 The report on the implemented measures is announced by the supplier and handed over to ANS CR, s. p.

13 PROTECTING ASSETS AGAINST UNAUTHORIZED ACTIVITIES

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

14 CONDITIONS FOR TERMINATION OF THE CONTRACT

- 14.1 In the event of termination of the contractual relationship, all access of the supplier and its employees to the assets of ANS CR, s. p. no later than the date of termination of the contractual relationship.
- 14.2 If the assets of ANS CR, s. p. have been provided to the supplier's employees, these assets must be returned no later than the date of termination of the contractual relationship.
- 14.3 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.