**Security Operational Requirements for suppliers and service providers for maintenance contracts**

# Introductory provisions

For the purpose of this attachment to the Agreement, the following abbreviations and terms are used:

|  |  |
| --- | --- |
| **Act or** **CSA** | Act No. 181/2014 Coll., concerning Cyber security and change of related laws (Cyber Security Act), in the wording of later regulations |
| **CSD** | Decree No. 82/2018 Coll. on security measures, cybersecurity incidents, reactive measures, particulars of filings concerning cybersecurity, and disposal of data (Cybersecurity Decree), as amended. |
| **Regulation** | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation) |
| **Personal information** | All information about an identified or identifiable physical person (such as name, identification number, location data, network identifier, or one or more specific physical, physiological, genetic, economic, cultural or social identity of that individual). |
| **Personal information processing** | Any operation or set of operations that is performed with personal data or personal data files, such as collecting, recording, organizing, structuring, storing, customizing or modifying, retrieving, viewing, using, making available through transmission, dissemination or any other disclosure, alignment or combination, restriction, erasure or destruction. |
| **Date of the agreement conclusion** | Date of the conclusion of this agreement or the date of integration of said Security requirements into the agreement through the appendix of this agreement. |
| **Individual prom the Provider’s party** | A physical individual participating in the fulfillment of the contract and having a labor or similar contract relationship with the Provider or their sub-providers |
| **Classification scheme** | Classification scheme specifying handling data and information of UJV Group in paper and electronic form. |
| **Consumer’s environment** | Physical perimeter specified by the physical space in rent or property of the Consumer or a logical perimeter defined by the network elements in the administration or the property of the Consumer. |

# Purpose

The purpose of this Annex is to define binding Security Operational Requirements and their level for providers whose subject of performance for the Client is maintenance and service support of systems, HW elements or software service (hereinafter also referred to as "SW"). Furthermore, the purpose of this Annex is to define binding Security Operational Requirements also for providers who, in connection with the performance under the Contract for the Client, access services and, in this context, information and control communication systems, and/or who process and/or transmit and/or store and/or archive any data and information of the Client within the scope of the performance for the Client (hereinafter also referred to as "Security Operational Requirements").

1. Furthermore, the purpose of this document is to define the requirements for suppliers according to ISO/IEC 27001 and applicable legislation, especially according to the provisions of Section 5(2)(e) of Act No. 181/2014 Coll., on Cyber Security and on Amendments to Related Acts (Cyber Security Act), as amended, and Section 8 of Decree No. 82/2018 Sb. on Security Measures, Cyber Security Incidents, Reactive Measures, Submission Requirements in the Field of Cyber Security and Data Disposal (Cyber Security Decree), as amended, while also taking into account other related applicable legislation on the subject.
2. The Provider undertakes to implement the Security Operational Requirements in accordance with the applicable legislation, in particular the aforementioned legal regulations, and is fully responsible for their implementation to the Client.

# 2. Security Operational Requirements and measures

### 2.1 System of Management of Information Security

The Provider acknowledges, that the Consumer has established the Information Security Management System according to ISO/IEC 27001 and is a person according to § 3 paragraph c) and d), eventually e) or f) of the Act 181/2018 Coll. and is bound to fulfill the requirements of the related legislation.

Information security requirements are part of the binding terms of cooperation with the external entity, binding on third parties. An authorized employee of a company belonging to the ÚJV Group (Person authorized to act on behalf of the Client in technical and implementation matters, maintenance unit, department managers (heads) as owners of information (information assets), CISO (Chief Information Security Officer), CSO (Chief Security Officer)), authorized to act in the area of information security, must ensure the information security requirements of the ÚJV Group in relation to the external entity (supplier) and with binding effect on third parties, in accordance with the requirements of the owner of the information assets

When performing for the Client, the Provider undertakes to meet the following obligations:

1. if the Provider uses subcontractors in the provision of the performance, the Provider undertakes to ensure compliance with the Security Operational Requirements also in contractual relations with its subcontractors;
2. designate, no later than 5 days after demonstrable receipt of these Security Operational Requirements, a responsible contact person for the purposes of ensuring compliance with these Security Operational Requirements and related communication between the Parties (hereinafter also referred to as "Contact Person for Security on the Provider's side[[1]](#footnote-2)"). inform the Client of the Contact Person for Security on the Provider's side in writing by the same deadline. the Client stipulates that the appointment of the Contact Person for Security on the Provider's side does not affect provisions relating to the Parties’ Authorized Persons if said provision(s) is/are applied in the maintenance contract;
3. ensure that the Contact Person for Security on the Provider's side, immediately after their appointment, determines the scope and describes the relevant assets needed to fulfil these Security Operational Requirements on the Client's ICT systems (assets are understood as e.g. data and information, ICT systems, modules, HW elements, applications , databases, servers, storage, end devices – workstations such as a personal computer or laptop, etc. used for the maintenance of the Client's ICT systems);
4. if personal data is processed in the performance of these Security Operating Requirements or in the performance of the concluded contract, the Security Contact Person on the Provider's side undertakes to inform in the sense of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter referred to as "the Regulation") its subcontractors about the processing of their personal data and the personal data of their employees and, where applicable, to ensure that separate contracts are concluded for the processing of personal data within the meaning of the relevant provisions of the Regulation
5. comply with all provisions of the Regulation. The Provider must apply all necessary measures in order to eliminate illegal or accidental access to personal information, modification, damage or loss of such information, illegal transfers, other unauthorized processing and misuse of such information
6. the Provider undertakes not to provide data from ICT systems to a third party
7. ensure that the Provider's Security Contact on the Provider’s side has made all persons involved in the provision of performance on the Client's ICT systems on behalf of the Provider and/or its subcontractors aware of these Security Requirements.
8. provide regular reporting - i.e. produce and provide asset assessment reports and undertake risk identification and risk management planning in relation to the performance provided. The Provider undertakes to submit the Asset Valuation Report and the Risk Management Plan to the Client once a year, always by the end of January for the previous calendar year. The Asset Valuation Report will always consist of the following chapters:
9. Management Summary
10. Cyber Security Status Report for the year under review
11. Implemented Security Measures
12. Assessment of security events and incidents
13. Uncovered security risks and proposal of measures to be taken
14. Status of compliance with security legislation
15. Conclusions and recommendations

The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at least, bound to:

1. Procure security principles and processes, which will cover the security of data and information, that can be created and processed on by the Consumer party under the terms and conditions of the contract.
2. Manage their own risks that can affect the provision of the terms and conditions of the contract.
3. Based on the security requirements and results of risk evaluation, implement appropriate security measures according to the terms and conditions of the contract, monitor them, and evaluate their efficiency.
4. Keep a record of the security policy covering security of data and information, which can be created and processed by the Consumer’s party under the terms and conditions of the contract. The security policy must include the general principles, objectives, security requirements, rights and obligations concerning the management of information security.
5. Set up and maintain the current security measure in the form of processes and technologies, ensuring fulfillment of the security policy.
6. Keep a record of the creation and processing of data and information according to the provided terms and conditions of the contract, record all significant circumstances concerning the assurance of the security of the data and information and grant access to them upon the request of the Consumer.
7. In case of using a sub-contractor, ensure inclusion of adequate compliance to Security requirements in contract relationships with their sub-contractors.
8. After the contract performance termination, without undue delay, shred all information and data of the Consumer, which were handed over during the performance of the contract.

### 2.2 Human Resources Security

The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at least, bound to:

1. Ensure the person responsible in contract terms, within 10 days of entering the contract, confirms, in written form, to the Consumer, that all individuals participating in the fulfillment of the terms and conditions of the contract for the Provider’s party are provably introduced to the security requirements and rules of CYBEX (Cyber security rules for external employees).
2. Provide the terms and conditions of the contract employing only Authorized individuals, which have been properly introduced to the rules of CYBEX and possess verified qualification, knowledge and experience according to the terms and conditions of the contract.
3. Adhere to relative provisions control Acts of UJV Group and CEZ Group in the extent in which they have been introduced to said Acts. The provable introduction is deemed as the Provider’s employee training provided by the Consumer, electronic transfer or transfer by protocol of the relative documentation or access to a shared repository, provided by the Consumer, containing relative internal control Act.
4. In case a supervision over the terms and conditions of the contract service is part of the terms and conditions of the contract, define and fulfill roles and accountability for monitoring networks and devices according to the terms and conditions of the contract.
5. Ensure, that individuals participating in fulfillment of the terms and conditions of the contract for the Consumer in Consumer’s environment or with Consumer’s assets, including the case the Consumer’s assets are used outside of Consumers environment:
   1. For saving and sharing data and information of the Consumer using only approved media;
   2. Not saving or sharing data and information with ethically inappropriate content conflicting with good behavior or damaging the name of the Consumer;
   3. Not downloading, sharing, saving, archiving, or installing data files and executable files conflicting with the terms and conditions of the license or copyright;
   4. Not visiting web pages with ethically inappropriate content;[[2]](#footnote-3)
   5. Not attempting unauthorized access to the resources of the Consumer or other subjects;
   6. Not attempting unauthorized modification or other unauthorized interference with resources of the Consumer, not even in the case, that the resource of the Consumer is managed by them;
   7. Not participating with the resources of the Consumer in spreading spam or malicious software.
   8. The Provider agrees to ensure that any persons involved in the provision of services to the Customer on the Customer’s ICT systems perform only activities in accordance with the project and operational documentation.

The provider acknowledges that part of the conditions, in order to gain access to Consumer’s resources, is processing of Provider’s employees’ personal information, of those who participate in the fulfillment of the terms and conditions of the contract, by the Consumer. In case the Consumer is not enabled to process personal information of the affected employees, said employees will not be granted access to the resources of the Consumer.

### 2.3 Management of Operation and Communications

The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at least, bound to:

1. Ensure safe operation of the information system and the infrastructure used for fulfillment the terms and conditions of the contract.
2. On request, provide a summary, report, or other adequate information concerning the security measures implemented in their information system and infrastructure.
3. Ensure that, for fulfillment of the terms and conditions of the contract only applications and technologies are used that are in accordance with valid Czech and European legislation and, in particular, with the license conditions of the Act No. 121/2000 Coll., concerning copyright, as well as those concerning the laws related to copyright and related amendments.

### 2.4 Management of Approach and Secure User Behavior

The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at least, bound to:

1. Assign authorization to their individual employees to carry out actions in such a way that the risk of undesired access to the Consumer’s assets is minimized.
2. Ensure, that granted access is not shared by several individuals in the Producer’s party.
3. State in the request for access the extent of data/information, service, purpose, for which is the access to the ICT system of the Consumer requested and a time specification of the duration of the validity of the access (e.g.: for an indefinite period / 1 year / 1 month / 1 day).
4. Ensure that individuals participating in the fulfillment of the terms and conditions of the contract, who have access to the information asset of UJV Group or CEZ Group, keep the authentication media and information safe, and under no circumstances provide unauthorized access to other individuals.
5. Continuously control and evaluate the validity and necessity of access, both physical and logical, of all individuals from the Provider’s party that enter the Consumer’s environment.

The Provider acknowledges, that the access to the ICT system of UJV Group companies is possible to allow only to the physical persons identified as an employee of the Provider / Provider’s sub-contractor, verified by an identity document and with the generated unique identifier for ICT system access and registered in the registry of identities only on basis of a Provider’s request for access. In order to register in the Identity Register, it is necessary to disclose these personal data to the Provider's employee:

* + 1. Name (Identity Register)
    2. Last Name (Identity Register)
    3. Maiden name (Identity Register)
    4. Gender (only for verification purposes, without registration in the Identity Register)
    5. Birth Date (Identity Register)
    6. Personal Identification Number (only for verification purposes, without registration in the Identity Register, we do not store PIN in the system, we do not require it to be sent or recorded in the form, but it is required for the verification of physical identity to generate the unique identifier, physical identity communicates it at the moment of verification. In case of person´s disagreement, verification is carried out based on the date of birth and other personal data).
    7. Email (Identity Register)
    8. Mobile phone or landline (Identity Register)

The Provider acknowledges informing its employees and subcontractors to whom the access (physical, logical) to the ICT system will be assigned, the manner of processing their personal data, and the Provide undertakes to process personal data exclusively in accordance with the Regulation.

The Provider acknowledges that the activities of users accessing the Client’s information systems using privileged user accounts may be monitored and recorded for the purposes of security auditing, investigation of security incidents, and ensuring compliance with the Client’s internal security policies.

The user is clearly informed at the start of each session that their activity is being actively recorded.

The Provider undertakes to inform all relevant persons (e.g., employees, subcontractors, partners) who will participate in the performance of this agreement and access the aforementioned systems of the possibility of such monitoring and recording.

The Provider acknowledges that authorization assigning to the Provider’s employee must be controlled by the principle of minimum necessity and is not claimable.

The Provider acknowledges that in case of unsuccessful attempts to authorize a user (an individual from Provider’s party), the respective account can be blocked and treated as a security incident and measures for security incident management can be applied (e.g.: immediate cancellation of access to the information assets).

### 2.5 Acquisition, Development and Maintenance

Requirements on the system and operational security documentation of the Client’s ICT systems

The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at least, bound to:

1. Ensure secure implementation, innovation, update, maintenance and testing of technologies, and backup and archiving of data, if they are part of the terms and conditions of the contract.
2. Transfer the documentation of the terms and conditions of the contract to the Consumer including at least:
3. documentation of actual execution
4. documentation of all security settings, functions and mechanisms
5. documentation including a description of authorization concept and authority
6. documentation including back-up and archiving processes
7. documentation including installation and configuration processes
8. documentation for ensuring the continuity of operation and recovery after an accident i.e. the recovery strategy (for systems classified as 'A' in terms of availability)
9. The Provider undertakes that effective protection against malware is and will be provided for all ICT systems of the Provider (including storage media) that connect to the Client's environment,
10. follow the procedures for data and software (SW) backups specified in the project and operational documentation. All backups performed by the Provider, including backup media, must be protected;
11. continuously detect technical vulnerabilities and configuration inconsistencies of the subject of performance in the process of performing maintenance on the Client's ICT systems. Detected technical vulnerabilities must be evaluated with respect to the associated risk and corrective action must be taken by the Provider according to the nature of the subject matter;
12. ensure that installation of SW component updates proceeds only from credible sources (in accordance with the project documentation and according to the procedures set out in the operating regulations) and in accordance with valid contractual terms and conditions of the SW manufacturer (notably with respect to licensing terms and conditions and Act No. 121/2000 Coll., on Copyright, Rights Associated with Copyright and on Amendment of Certain Acts (The Copyright Act), as amended).

In case the terms and conditions of the contract include software maintenance or software development, the Provider is bound to:

1. Adhere to and implement the best practices for safe software development defined in the contract relationship.
2. Allow the Consumer to carry out an audit on the fulfillment of the contract and, on written request, present the Consumer with developed sources code of software, if the audit activities and showing the source code are mentioned in the contract. The consumer will be allowed to execute code review (automated through security tools, and manual), especially in order to verify that the Provider is proceeding or proceeded in fulfilling the contract according to the terms and conditions of the contract and the Security requirements.
3. Provide the Consumer, in the terms stated by the Consumer, respectively, without unnecessary delay, the requested co-operation on execution of security testing during the development of the software or anytime after the delivery of the software.
4. Ensure that the fulfillment will include only the elements that are objectively necessary for proper operation of the software and/or that are explicitly specified in the contract (especially that the software will not include any unnecessary components, any program samples etc.).
5. In case the installation of the operating system or other third-party software is a part of the fulfillment of the contract, ensure, during its installation, that the specified versions of these products installed are compatible and functional within the Consumer’s environment.
6. Ensure the security of the Provider’s testing environment and security of the testing data provided by the Consumer.
7. Ensure that only an executable code, specified by the terms and conditions of the contract will be supplied within the production environment, and the necessary data for operation of the contract fulfillment will be compiled.
8. Ensure that, according to the terms and conditions of the contract, the provided software will be
9. in accordance with the security policies and standards of the Consumer
10. tested in accordance with the security policies of the Consumer (applies to the Provider, in case they were introduced to such security policies)
11. Install software only based on the migration processes approved by the Consumer in advance.
12. Transfer the source code to the Consumer in secure form, ensuring its integrity.
13. Ensure the management of various versions of the source code.
14. Ensure the back-up of the source code and its safe storage outside the production environment.
15. Ensure that the distribution of the source code includes a file from the development environment for directed compilation of said source codes.
16. Not develop, compile or share, in the environment of the Consumer, a program code with the purpose of illegal takeover, disruption of access, confidentiality or integrity or unauthorized and illegal acquisition of data and information.

### 2.6 Cyber Security Events and Incidents Management[[3]](#footnote-4)

The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at least, bound to:

1. Without unnecessary delay, report to the Consumer all security events and incidents with potential negative impact to the Consumer through a specified communication channel or through the Contact Person.
2. Evaluate concerning information security incidents and preserve it for future use according to the requirements of valid Czech and European legislation.
3. In case of a security event and consecutive management and evaluation of the security incident, and/or in case of suspicion of a security incident, provide the Consumer with the relevant information concerning an identified suspicious device or individual from the Provider’s party.
4. Without unnecessary delay, and after agreement with the Consumer, implement measures requested by the Consumer within the agreed terms in order to reduce the impact of a security incident or prevent the continuation of an incident, that can make an impact to the Customer.
5. Co-operate in the analysis of the causes of security incident and suggest measures with the intention to prevent its recurrence in case the security incident was cause by the Provider, or the Provider participated in its origin.

The Provider acknowledges that the process of management of security incidents, or other consequential breach of the Security Requirements, caused by the Provider will not be considered as a circumstance excluding the responsibility of the Provider for delaying the fulfillment of the terms and conditions of the contract and will not be a basis for a compensation of any kind in case of damage to the Provider or any other individual from the Consumer’s party. Other provisions concerning the accountability of the Provider for extensions included in the contract are not influenced by the provision.

### 2.7 Business Continuity Management

The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at least, bound to:

1. Ensure adequate continuity of any assets in their ownership that are necessary for the fulfillment of the terms and conditions of the contract.
2. Continuously control and test that they are capable of ensuring the continuity of assets according to the agreed level of service.

### 2.8 Physical Security

The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at least, bound to:

1. Adhere to the operational rules of the buildings (regime measures) and used spaces, especially in the area of physical safety of security areas, where the components of ICT systems or the data carriers are placed.
2. In accordance with the terms and conditions of the contract, ensure the physical safety of the installation, back-up or archiving of media and documentation in accordance with the Classification scheme, especially labeling, preservation and disposal. Physical disposal of used media will be carried out according to prescribed procedures which must guarantee that the security classification is maintained.

### 2.9 Security Tools

The Provider will actively participate, according to the terms and conditions of the contract, in observing, operating a developing security measures. The Provider is, at least, bound to:

1. Implement security measures for removal or blockage of the network connection/connections that does/do not fulfill the requirements for the security of the integrity of the communication network.
2. Implement access from a mobile device to the environment of the Consumer only through secured connection of virtual private network (VPN).
3. Connect to the environment of the Consumer only such devices (switch, Wi-Fi access point, router, hub etc.) that have passed through an approval process, including that their connection was approved by an authorized individual in technical matters from the Consumer’s party, and who is identified in the contract.
4. Without unnecessary delay, document and deactivate all unused terminals in the network or unused ports in active network element, that is according to the terms and conditions of the contract and is in the report of the Provider.
5. Avoid installation onto any assets of the Consumer, or use in the environment of the Consumer, the following types of tools, unless they are part of the contract:
6. Keylogger – software or hardware, that can, without authorization, log keystrokes with the aim to disrupt the confidentiality of the input data and information.
7. Sniffer – software or hardware, that allows unauthorized monitoring of network traffic.
8. Weakness analyzer (Weakness scanner) – software or hardware tool allowing the search and identification of weaknesses in the ICT systems, detection of available network services and ports, running processes, running afflictions and their versions etc.
9. Backdoor – hidden software or hardware tool, allowing bypass of approved authentication procedures, installed with the aim of providing easy, unauthorized access to the ICT system.
10. Malware and other malicious software that disturbs bypasses or restricts the security measures in the Consumer environment in any way.
11. connect to the Consumer environment only ICT devices that meets the following requirements:
12. Security patches must be applied (operating system, internet browser, MS Office, Java and possibly other SW if applicable);
13. Must have anti-virus protection installed, running, and updated.
14. The mass storage media (flash drives, floppy disks, CDs, and DVDs, etc.) must be checked on a device that has updated antivirus protection before it can be used.
15. It must be connected only to dedicated secure zone as defined in the operations or project documentation. If it is not defined in the operations or project documentation, it is assumed that the connection of such devices is not permitted.
16. If a device such as a notebook/computer is used for maintenance that is not dedicated solely to the maintenance of the Customer’s ICT system, it must meet the conditions specified in this chapter.
17. Continuously record and preserve data concerning the ICT device operation (operation and localization information) according to the contract and in adherence with requirements of valid Czech and European legislation.
18. Upon request, provide the Consumer with a report including the results of monitoring of all user and administrative activities and other events according to the contract and for up to 2 years after the termination of the contract.
19. Ensure the collection of information concerning the operational and security activities according to the contract, and the security of acquired information from unauthorized reading or modification.
20. For on-line transactions completed through web technologies, implement TLS/SSL certificates with the aim of ensuring their confidentiality, integrity and identity communicating parties.
21. Secure all private information provided by the Consumer with appropriate encryption and against unauthorized access, especially on the mobile devices.

The Provider acknowledges that, if the technical connection of the UJV Group to the Provider is causing disturbance to the functioning of the UJV Group or CEZ Group, the connection can immediately be ended without prior warning, unless the contract states otherwise.

The Provider acknowledges that all activities of the Provider and their fulfillment realized in the environment of the Consumer are monitored and evaluated in accordance with the fulfillment of the contract and adheres to the internal documents of the Consumer, which have been introduced to the Provider.

1. for changes in the Contact Person for Security on the Provider's side, the provision on Parties’ Authorized Persons shall be used. The Provider is obliged to report any change in the Contact Person for Security on the Provider's side within 5 days of making the change. [↑](#footnote-ref-2)
2. Data and information containing elements of extremism, terrorism, pornography and/or incitement to hatred and social prejudices relating to a social group identified based on race, religion or faith, gender, sexual orientation, nationality and ethnic affiliation or other difference. [↑](#footnote-ref-3)
3. The terms security incident and security event are equivalent to the terms cyber security event / cyber security incident as defined by Act No. 181/2014 Coll., on Cyber Security as amended. [↑](#footnote-ref-4)