

Security Rules Applicable to Major Suppliers

These security rules are aimed at reducing of risks occurring in the information and communication system and at taking requirements into consideration which arise from the security measures protecting the assets of Tomas Bata University in Zlín (hereinafter referred to as “TBU”) to which suppliers have access in accordance with provisions of § 4 Paragraph 4 of Act No. 181/2014 Coll., on Cyber Security and on Amendments to Related Acts (Cyber Security Act), as amended (hereinafter referred to as the “Cyber Security Act”), in conjunction with Annex 7 to the Decree No. 82/2018 Coll., on Security Measures, Cyber Security Incidents, Reactive Measures, Requirements for Submissions in the Field of Cyber Security and Data Destruction (Cyber Security Decree), as amended (hereinafter referred to as the “Cyber Security Decree”).

For this purpose, a major supplier, in accordance with § 2 Letter n) of the Cyber Security Decree, is any operator of an information or communication system and anyone who enters into a legal relationship with TBU which is significant from the point of view of the security of the information and communication system.

Basic Responsibilities of a Major Supplier

A Non-Disclosure Agreement (NDA) must be concluded with each major supplier, ensuring compliance with the confidentiality and security of the information, documents and equipment provided. In the event of a breach of this Agreement, the supplier is obliged to bear the consequences arising from the Agreement (contractual penalty, compensation for damage).

A Service Level Agreement (SLA) must be concluded with each major supplier, ensuring compliance with the level of services provided. In the event of a breach of this Agreement, the supplier is obliged to bear the consequences arising from the Agreement (contractual penalty, compensation for damage).

Rules aimed to ensure the integrity of information must be adjusted for each major supplier. The rules must contain requirements for data encryption to be used when the data are being transferred; electronic signatures to be used in order to unambiguously identify the person who has modified the data; restriction of write access rights and data change rights related to selected roles; data access control, etc.

Each major supplier must have an information security management system introduced (no certification is required).

Major Suppliers

1. Major suppliers are obliged to proceed in accordance with legal regulations in force and effect, in particular in accordance with the requirements applying to TBU as the administrator and operator of a major information system (hereinafter referred to as the “MIS”), in compliance with the Cyber Security Act and the Cyber Security Decree, and to reflect any amendments to the above-mentioned legal regulations or to any new legislation.
2. Major suppliers are responsible for the applied solution/delivery/administration (hereinafter referred to as the “Solution”), which is to be used in such a manner as to

comply with TBU security requirements, and to prevent security incidents and crisis situations.

3. Major suppliers are responsible for the delivery and implementation of solutions in the required quality as regards information security, in particular for a correct implementation of security procedures arising from these security rules.
4. Major suppliers are obliged to ensure that the subject matter of the performance does not contain technologies/key elements produced by manufacturers against whom the competent administrative authority has issued measures in accordance with the Cyber Security Act or who, according to the risk analysis, pose a high risk.
5. Major suppliers are obliged to create and approve a security policy that will cover the security of data and information that may be created and processed on the part of the supplier when providing the subject matter of performance. The security policy must contain the main principles, objectives, security needs, rights and obligations related to information security management.
6. Major suppliers are obliged to carry out an analysis and assessment of information infrastructure risks that may affect the provision of the subject matter of performance of the contract (the Solution to be delivered) and, depending on security needs and results, to propose and submit to TBU for approval the relevant security measures corresponding to the extent of the provided subject matter of performance and aimed to minimize or eliminate the identified risks, to monitor the measures and assess their efficiency.
7. Major suppliers are also obliged to carry out their own risk analysis/assessment on a regular basis, and to check the security measures implemented. Such inspections shall take place at regular intervals set by the supplier, at TBU's request. The supplier shall submit a written inspection report on the result of the inspection to TBU without undue delay.
8. Major suppliers are obliged to inform TBU about the methods of risk management, as well as about residual risks related to the performance of the subject matter of the contract.
9. Major suppliers are obliged to set security measures and keep the measures up-to-date, and that in the form of processes and technologies ensuring the fulfilment of the security policy.
10. Major suppliers are obliged to secure the entire data and information transfer in order to comply with security requirements as regards the confidentiality, integrity and availability of data/information during the provision of services to TBU.
11. Major suppliers are obliged to keep records on the creation and processing of data and information within the scope of the subject matter of the performance provided, to record all essential circumstances related to the assurance of security of such data and information, and to provide access to these records to TBU upon request.
12. Major suppliers are responsible for maintaining of confidentiality by all of their

employees involved in the Solution, and that as regards information, documents and equipment provided, also after the termination of the contractual relationship with TBU.

13. Major suppliers are obliged to provide TBU with contact details of the monitoring centre (helpdesk) including the recorded activity/contact details of all their employees involved in the Solution.
14. If using the services of subsuppliers (of major suppliers) when providing the fulfilment of the subject matter of performance, major suppliers shall ensure adequate compliance with the above-mentioned security rules also as regards contractual relations entered into with their subsuppliers.

Subsuppliers

1. Suppliers shall not involve any other subsupplier in the provision of the subject matter of performance under this contract without a prior specific or general permission given by TBU.
2. Each supplier is obliged to provide TBU with the contact details of all persons who, on the part of a subsupplier, participate in the Solution, in particular those persons who provide system and technical support for the Solution.
3. Each supplier is obliged to ensure that a subsupplier complies with the requirements set out in these Security Rules.
4. Suppliers shall be responsible for ensuring that their subsuppliers do not act in contradiction with the security measures arising from these security rules. In the event that a subsupplier of a supplier fails to comply with these requirements, any such failure to comply with the requirements shall be considered a breach of the supplier's obligations set out in the contract.

1. INFORMATION AND CYBER SECURITY MANAGEMENT

- 1.1. All major suppliers as well as their subsuppliers are obliged to implement the following measures in their internal processes:
 - 1.1.1. Have a security awareness development plan in place in order to ensure adequate education and an improvement in security awareness in the following form, content and scope:
 - a) Instructions given to users, administrators, security role holders and suppliers, including their subsuppliers, regarding their obligations and security policy.
 - b) Theoretical and practical training required for users, administrators and security role holders.
 - 1.1.2. Appoint persons responsible for the implementation of the individual activities listed in the plan.
 - 1.1.3. In accordance with the security awareness development plan, instruct users, administrators, the security role holders and suppliers (subsuppliers) as regards their obligations and security policy, and that through initial and regular training sessions.

- 1.1.4. Provide regular professional training for security role holders in accordance with the security awareness development plan, depending on current cybersecurity needs.
- 1.1.5. In compliance with the security awareness development plan, provide regular staff training and testing of safety awareness of employees in accordance with their job positions.
- 1.1.6. Ensure that users, administrators and security role holders comply with the security policy and have an established procedure regarding labour law sanctions to be imposed on their employees.
- 1.1.7. In the event of termination of the contractual relationship with administrators and security role holders, ensure delegation of responsibilities.
- 1.1.8. Assess the effectiveness of the security awareness development plan, of the staff training provided and of other activities related to improvements in security awareness.
- 1.1.9. Set out rules and procedures for dealing with breaches of the established security rules by users, administrators and security role holders.
- 1.1.10. Keep records on staff training sessions provided, which shall include the topic of the staff training and a list of persons who attended the staff training sessions.
- 1.1.11. No less than once per year provide TBU with information concerning persons related to the provided subject matter of the contract, about the staff training provided and about the content of the staff training.
- 1.2. The suppliers have agreed all essential requirements regarding information security with each of their suppliers who may access, process, store, transmit or provide ICT infrastructure components both as regards the supplier's information and information of the supplier's clients.
- 1.3. TBU reserves the right to keep records on/review the supplier's activities, to keep records on incidents and unusual activities of employees and of other persons hired to work on the supplier's behalf (hereinafter referred to as the "supplier's employees"). Based on such records, TBU is authorized to check the credibility and reliability of the supplier's employees. In the event of an identified risk, TBU shall notify the supplier of the non-compliance, and both parties shall enter into negotiations in order to deal with the situation.

2. HUMAN RESOURCE MANAGEMENT

- 2.1. The supplier shall ensure that all persons participating in the performance of the contract concluded with TBU are acquainted with these security rules and with other detailed security information demonstrably provided by TBU. These persons shall confirm in writing that they have been acquainted with the rules.
- 2.2. Persons participating in the performance of the contract concluded with TBU must have demonstrable qualifications, experience and knowledge.

- 2.3. The supplier must ensure that all persons involved in the performance of subject matter of the contract concluded with TBU have undergone a vetting process, and that conditions and responsibilities for their activities have been set for them.

3. OCCUPATIONAL HEALTH AND SAFETY AND FIRE PREVENTION (OHS AND FIRE PREVENTION), PHYSICAL SECURITY

- 3.1 The suppliers, as employers, are responsible for the following activities to be carried during the performance of the subject matter of the contract:
- a) Compliance with OHS and FP regulations by the supplier's employees or by other natural persons hired to work on their behalf
 - b) Prevention of unauthorized access to TBU buildings where TBU provides services (or fulfils an obligation in compliance with a contract concluded)
 - c) Prevention of damage and of unauthorized interventions in TBU buildings

4. OPERATION MANAGEMENT

- 4.1. The supplier undertakes to:
- 4.1.1. Ensure safe operation of the information system and infrastructure, if the supplier ensures their operation, used for the provision of the subject matter of performance in accordance with the requirements listed in the Cyber Security Decree and with recommendations included in information security standards, e.g. technical standards of the ISO/IEC 27000 series.
 - 4.1.2. Upon request, provide TBU with an overview of the security measures which have been implemented in the supplier's information system and infrastructure and are aimed at fulfilling the subject matter of the contract.
 - 4.1.3. Ensure that only such applications and technologies that are in accordance with the valid Czech and European legislation will be used for the provision of the subject matter of performance of the contract, in particular with regard to the licence conditions, copyright and rights related to copyright, and in accordance with amendments to selected acts (Copyright Act), as amended.

5. ACCESS CONTROL

- 5.1. Identification
- 5.1.1. Each employee of the supplier who uses the supplier's computing equipment in order to participate in the performance of the subject matter of the contract must have his/her own unique user account registered and maintained within their infrastructure, which is assigned specific roles in all systems, modules or applications. Each employee of the supplier must be registered with valid identification and up-to-date contact information.
 - 5.1.2. Each employee of the supplier, if he/she accesses TBU internal information systems, has a unique user account registered and maintained by TBU. The account is assigned specific roles in all systems, modules or applications related exclusively to the performance of the subject matter of the contract.

5.2. Authentication (Identity verification)

- 5.2.1. Requirements related to the authentication of users, administrators and applications who use the TBU information infrastructure:
- Two-factor authentication is used, i.e. an account identifier and two factors out of the triplet <authentication object, password, biometric factor>.
 - Before the requirement set under a) has been met, authentication using an account identifier and a cryptographic key must be used, including a guaranteed similar level of security.
 - Before the requirement set under a) or b) has been met, such authentication must be used which requires an account identifier and a password, including defined rules that must be technologically enforced.
- 5.2.2. In order to be given remote access for the supplier's employees, the supplier shall submit documents necessary for the completion of a remote access request form. Parameters for secure remote access shall be set according to the remote access request form, including the access duration period.
- On behalf of the supplier, the request form shall be completed internally at TBU by the person in charge of the relevant designated TBU system (based on documents provided by the supplier's contact person).
 - After the request has been granted, the supplier's employee shall be individually acquainted with details of the remote access rules and provided with authentication data.
- 5.2.3. The suppliers are responsible for the activities of their employees or of other natural persons hired to work on the supplier's behalf; such activities must be in accordance with the security rules and with other detailed security information demonstrably provided by TBU upon request by the supplier. Any damage caused by a breach of these and other detailed security information by the supplier's employees or by other persons hired to work on the supplier's behalf shall be charged to the debit of the supplier, who is obliged to compensate TBU for such damages to the full extent.

5.3. Authorization

- 5.3.1. The supplier's employees are obliged to use privileged authorizations in the TBU information infrastructure only to a reasonable extent and only for the period necessary to carry out activities in accordance with the performance of the subject matter of the contract. Users and administrators are not allowed to use accounts with privileged authorizations for routine operations not related to the administration of the relevant information system.
- 5.3.2. The supplier's employees shall be informed by TBU about TBU information which is considered confidential, about TBU confidential information which they have access to, and how they are expected to handle such information. The suppliers are not permitted to carry out any manipulations or other operations with TBU's confidential information that were not explicitly stated in the instructions.

5.4. Remote access

- 5.4.1. To access TBU information systems, the suppliers can use their own equipment (HW, SW).
- 5.4.2. The supplier's workstations accessing the TBU infrastructure via VPN (Virtual Private Network) must have:
 - a) Advanced functional antivirus protection (with real time protection mode enabled), including a component for active collection of logs and of cyber security incidents (e.g. SIEM) in accordance with requirements set in the Cyber Security Act
 - b) A functional personal firewall
 - c) A fully updated operating system and automatic updates of the operating system set up
 - d) An operating system that is not excluded from the manufacturer's service support (unless explicitly agreed otherwise in a contractual arrangement)
 - e) Updated third-party applications without infringing the third-party copyright
 - f) Ensured encryption of all storage media used for storage of TBU confidential data and information. Access to storage media and to the decryption of TBU confidential data and information must be provided only to persons authorized by the supplier.
 - g) An installed VPN client according to instructions given by TBU.
 - h) A second authentication factor, if required by TBU for access to the VPN or if available (e.g. HW, a mobile app or a SMS token), which will be provided by the appointed TBU employee upon signing of the takeover record.

6. CHANGE MANAGEMENT

- 6.1. 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 to:
 - 6.2.1. Manage and register contractual changes.
 - 6.2.2. Manage and register changes in the services provided in accordance with the requirements set in the Cyber Security Decree as well as the recommendations included in information security standards, e.g. technical standards of the ISO/IEC 27000 series.
 - 6.2.3. Provide TBU with all necessary assistance when analyses of the associated risks are being carried out, when measures aimed to reduce all adverse impacts associated with changes are being adopted, also when security documentation is being updated, when the related testing is being made, as well as with assistance aimed to ensure the possibility of return to the original state.
 - 6.2.4. In the event that penetration testing or vulnerability testing of the Solution is carried out, the supplier shall provide TBU with all necessary cooperation and adopt additional, effective corrective measures in order to eliminate vulnerabilities that have been detected during the penetration testing carried out.

7. ACQUISITION, DEVELOPMENT AND MAINTENANCE

- 7.1. The supplier undertakes to:

- 7.1.1. Ensure a secure implementation, innovation, updating, testing of the technologies referred to as the subject matter of performance of the Contract.
- 7.1.2. Submit to TBU documentation regarding the subject matter of performance to at least the following extent:
 - a) As-built documentation
 - b) Documentation regarding all security settings, functions and mechanisms
 - c) Documentation containing a description of the authorization concept and entitlements
 - d) Documentation containing backup and archiving procedures
 - e) Documentation containing installation and configuration procedures
 - f) Documentation containing vulnerability tests and compliance with TBU security requirements
 - g) Documentation aimed to ensure operational continuity and disaster recovery documentation
- 7.2. In the event of the development of a Solution, the supplier undertakes to:
 - 7.2.1. Adhere to and implement best practices for a secure software development in accordance with recommendations given in information security standards, e.g. technical standards included in the ISO/IEC 27000 series.
 - 7.2.2. If software audit activities and the handover of the source code to the Solution are part of the performance under the contract, an audit of the implementation in progress or of the completed implementation shall be enabled and, upon written request, the source code which is being developed for the Solution shall be submitted for a code review (automatically, using a security tool, or manually), and that in particular for the purpose of verifying whether the implementation has been performed in accordance with the contract.
 - 7.2.3. Ensure that the performance contains only such components that are objectively necessary for a proper operation of the Solution and/or that are explicitly specified in the contract (in particular, the Solution shall not contain any unnecessary components, any program samples, etc.).
 - 7.2.4. If the implementation also includes the installation of an operating system or of third-party software, ensure, during their installation, that the required versions of such products are used that are compatible and functional in the TBU environment.
 - 7.2.5. Ensure the security of the test environment on the part of the Supplier and ensure protection of the TBU test data provided.
 - 7.2.6. Ensure that only the compiled/executable code specified in the subject matter of performance of the contract and other data necessary for the operation of the subject matter of the performance will be implemented in the TBU production environment.
 - 7.2.7. Ensure that the delivered Solution complies with the recommendations given by information security standards, e.g. technical standards included in the ISO/IEC 27000 series.

- 7.2.8. Provide TBU with the necessary cooperation in the event that TBU requires/implements the performance of security tests related to the subject matter of performance.
- 7.2.9. In the event that TBU requires a certificate evidencing that security tests have been performed by the supplier, this shall be agreed upon in a separate contractual agreement.
- 7.2.10. Hand over the TBU source code, if so stipulated in the contract, in a secure form ensuring its integrity, and, in such a case, do the following:
 - a) Ensure version control of the source code.
 - b) Ensure that the source code is backed up and stored outside the production environment.
 - c) Ensure that the distribution of source codes includes a file from the development environment for the purpose of a controlled compilation of the same source codes.
- 7.2.11. Avoid developing, compiling or distributing of any program codes in the TBU environment which aim to illegally control, disrupt availability, confidentiality or integrity of data/information, or acquire data/information in an unauthorized/illegal manner.

8. USE OF CRYPTOGRAPHIC TOOLS

- 8.1. If the use of cryptographic tools is required in the context of the subject matter of performance, the technical conditions are as follows:
 - 8.1.1. Encryption by a symmetric algorithm with the application of the AES method using a key length of 256 bits; the password must be transmitted over a communication channel other than the data being transmitted.
 - 8.1.2. Encryption by an asymmetric algorithm with the application of the DSA method using key lengths of 3,072 bits or more or an elliptic curve based method (EC-DSA, EC-Schnorr) using key lengths of 256 bits or more.
 - 8.1.3. Use of the hash function, with the application of the SHA-2 or SHA3 method using output lengths of 256 bits or more.
 - 8.1.4. Encryption using digital certificates issued by a generally accepted CA or a CA that is explicitly trusted by both parties.
 - 8.1.5. Encryption of disks in the XTS mode (the length of the data/sector unit must not exceed 220 cipher blocks) or EME2.
 - 8.1.6. Integrity protection by the HMAC (Approved Hash Function) or EMAC mode.

9. MONITORING

- 9.1. Access to selected confidential internal information and to TBU information and communication systems which is given to the supplier's employees is continuously logged, monitored and evaluated. If technically and operationally possible, the following events are recorded in TBU systems:
 - a) Successful and unsuccessful user logins and logouts

- b) Activities carried out by administrators
 - c) Successful and unsuccessful actions related to accounts, permissions and entitlements
 - d) Failure to carry out activities due to missing access authorizations
 - e) User activities that may affect the security of the information and communication system
 - f) Commencement and termination of activities of technical assets
 - g) Automatic warning or error messages in technical assets
 - h) Access to logs and malicious activity attempts related to logs
 - i) Changes to the settings of the activity recording tool
 - j) Changes in the use of authentication mechanisms, including changes in the data used to log in
- 9.2. If technically and operationally possible, TBU shall assign the following information to each log entry:
- a) Date and time
 - b) Type of activity
 - c) Name of the relevant technical asset
 - d) Identification of the user
 - e) Identification of the originator's network device
 - f) Success/failure of the performance of the activity
 - g) Level of severity
- 9.3. The supplier is obliged, within its ICT infrastructure, to continuously monitor published and known security vulnerabilities that may affect a smooth and secure operation of systems related to the services provided by the supplier. These include, for example, vulnerabilities in operating systems, third-party software, web components, etc.
- 10. PROTECTION OF DATA STORAGE AND OF PORTABLE MEDIA**
- 10.1. The storage of TBU confidential information in data repositories, on portable media, and any transport of media outside TBU premises is subject to an approval by TBU.
- 10.2. If TBU confidential information is stored in a data repository and on portable media, the supplier is obliged to store or require the storage of such data in encrypted form and to keep records of such media.
- 10.3. The supplier is obliged to ensure the destruction of operational data containing TBU confidential information immediately after the purpose of their processing/storage. Once the data on the electronic medium have been destroyed, it must not be possible to recover the information. The supplier must issue an official record on the data destruction.
- 11. CYBER SECURITY OCCURRENCES/INCIDENTS**
- 11.1. The supplier is obliged to report all suspicions concerning all unusual situations, security vulnerabilities and cyber security problems/incidents:
- 11.1.1. Immediately/without undue delay after becoming aware of a cyber security problem/incident.

11.1.2. By contacting the contact person acting on behalf of TBU and specified in a superior contract.

11.1.3. In writing via e-mail sent to abuse@utb.cz.

11.1.4. The following information must be reported:

- a) Date and time of the occurrence/incident detection
- b) Type of the event/incident
- c) Source of the event/incident
- d) Target/victim of the event/incident
- e) Potential impact

11.2. If a cyber security problem/incident occurs, and the cyber security incident is, subsequently, dealt with and assessed on the part of TBU, the supplier shall provide the required cooperation, in particular by providing logs and identification data (e.g. IP address, MAC address, HW type, serial number, or IMEI) of the terminal device/mobile terminal device in question, for a content analysis, and, if required, the supplier shall implement the measures required by TBU without undue delay.

11.3. The supplier is obliged to analyse the causes of a cyber security problem/incident and propose measures to prevent a recurrence thereof in the event that the supplier has caused the security incident or has participated therein.

12. SUPPLIER AUDIT (CUSTOMER AUDIT)

12.1. Authorization to conduct an audit of the supplier.

12.1.1. TBU reserves the right to conduct audits of the suppliers.

12.1.2. The supplier undertakes to provide TBU with all necessary documentation, in particular with a list of technical and organizational measures, necessary in order to provide evidence of the fact that the obligations arising from these Security Rules, as well as from the Cyber Security Act and the Cyber Security Decree, have been met, and, for this purpose, the supplier undertakes to enable TBU to carry out inspections, including audits to be conducted by TBU or by an auditor authorized by TBU to conduct an audit. The supplier shall provide all necessary cooperation during such inspections and audits.

12.1.3. TBU shall notify the supplier of the intention to conduct an audit sufficiently in advance, i.e. no less than 14 calendar days in advance. Both parties agree on the content, necessary cooperation and time schedule of the audit, with TBU undertaking to proceed in such a manner as not to disrupt the operational needs of the supplier.

12.1.4. All suppliers are obliged to appoint their representative(s) who will be present during an inspection/audit.

12.1.5. TBU reserves the right, in case of serious reasons (e.g. suspicion of risky behaviour of the supplier) occurring in connection with the performance of the subject matter of this contract, to conduct an unannounced audit of the supplier, taking the supplier's operational situation into account.

12.1.6. If non-conformities are detected, the auditor/inspector shall determine corrective measures and a date for the implementation of the same. The supplier is obliged to implement corrective measures to the specified extent and within the required deadline.

12.1.7. Documentation on audits carried out by TBU shall be kept by the department responsible for conducting of audits. The same identifier shall always be used in reference to a particular audit. The individual audit records shall contain the following information:

- a) Audit plan
- b) Audit notification
- c) Audit questionnaire (a list of the auditor's questions, if the auditor deems it appropriate)
- d) Audit report
- e) Written, photographic or other records of operations, procedures or facilities related to the audit (to the extent necessary for documenting of findings)
- f) Record on findings (Corrective actions and follow-up checks)

12.1.8. The audited party (the supplier) shall receive a final audit report containing all findings made, on the basis of which:

- a) the supplier shall propose a method of implementation of measures (including binding deadlines) set by the auditor, and submit a list of such measures to TBU for approval.
- b) TBU shall, subsequently, confirm its consent to the proposed measures or return the measures including comments to the supplier for revision.

12.2. Corrective measures

12.2.1. The audited party (supplier) is obliged to ensure that the corrective measures agreed upon are implemented within the specified period of time.

12.2.2. The supplier shall announce and submit the report on the measures implemented to TBU.

13. ASSET PROTECTION AGAINST UNAUTHORIZED ACTIVITIES

13.1. The supplier shall avoid installing or using tools on TBU assets that are not part of the subject matter of performance of the contract.

14. CONTINUITY MANAGEMENT OF ACTIVITIES

14.1. TBU is entitled to involve suppliers in continuity management of activities, and that in particular in the continuity plan of activities

14.2. related to the information system and to the associated services and/or to involve suppliers in the TBU Emergency Plan.

14.3. The supplier shall submit to TBU a methodology for data backup and recovery in the form of a backup plan, a test scenario for data recovery, a registration system, including the assurance of the integrity and authenticity of the backup medium. As such, the backup must be encrypted.

15. REQUIREMENTS TO BE MET UPON TERMINATION OF THE CONTRACT

- 15.1. In the event of termination of the contractual relationship, the suppliers and their employees must be stripped of all access rights to TBU assets (VPN, systems, information) no later than on the date of termination of the contractual relationship.
- 15.2. If TBU assets have been provided to the supplier's employees, these assets must be returned no later than on the date of termination of the contractual relationship.
- 15.3. If TBU information assets (data) have been provided to the supplier, they must be returned and completely deleted, without any possibility of renewal, from all supplier's information systems and supplier's media containing such assets no later than the date of termination of the contractual relationship.