

Code:	SR/3/2024	
Ref. No.:	UTB/24/001485	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Supplier Management Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	30 January 2024	Version: 01
Effective from:	1 February 2024	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Information Technology Centre, Legal Services	
Pages:	4	
Appendices:	1	
Distribution list:	TBU employees	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1

Introductory Provisions

- (1) The Supplier Management Policy sets out the rules for suppliers in accordance with the Act No. 181/2014 Coll., on Cyber Security, and on Amendments to Related Acts, as amended (hereinafter referred to as the “Cyber Security Act”) and Decree No. 82/2018 Coll. on Security Measures, Cyber Security Incidents, Reactive Measures, Requirements on Documents Submitted in the Area of Cyber Security and Data Destruction (hereinafter referred to as the “Decree on Cyber Security”) at Tomas Bata University in Zlín (hereinafter referred to as “TBU”).
- (2) The purpose of this policy is to lay down specifications and requirements related to public tenders, including small-scale tenders for potential major suppliers, which refers to every operator of an information or communication system and anyone who enters into a legal relationship with TBU, that is important in terms of the security of the information and communication system (hereinafter referred to as the “supplier”) at TBU.
- (3) This policy shall apply to all suppliers who have access to the assets of TBU. The scope of contractual arrangements of individual public tenders shall be determined according to the type and importance of the asset.
- (4) The individual terms used in this Directive are defined particularly by the Cyber Security Act and the Decree on Cyber Security. The individual terms are listed in the document entitled ‘*Glossary of Cyber Security Terms*’, which is available on the TBU website in the *Cyber Security* section.

Article 2

Rules and principles for the selection of suppliers

- (1) TBU shall lay down rules for suppliers that take into account the requirements of the TBU information security management system (hereinafter referred to as the “ISMS”), inform its suppliers about these rules and require their compliance.
- (2) TBU shall manage the risks associated with the suppliers and keep records of its suppliers.
- (3) TBU shall demonstrably inform its suppliers in writing about their records, and the requirements for demonstrable provision of the afore-mentioned information shall include:
 - a) identification of the controller or operator,
 - b) identification of the information and communication system,
 - c) identification of the supplier,
 - d) notification that the supplier is a major supplier for the controller, or that the major supplier is also an operator,
 - e) the content of the security rules for major suppliers taking into account the requirements of the ISMS, whose template forms Annex 1 to this Directive.
- (4) TBU shall ensure, in connection with the management of risks associated with suppliers, that contracts concluded with the suppliers contain relevant measures in order to ensure the security of the important information systems (hereinafter referred to as the “IIS”).
- (5) TBU shall regularly review the performance of the subject matter of the contracts concluded with the suppliers from the point of view of the ISMS.

Article 3

Rules for the assessment of the risks associated with suppliers

- (1) The Committee for Cyber Security (hereinafter referred to as the “Committee for CS”) shall determine the manners and levels of the implementation of security measures within all concluded contractual relationships and, in cooperation with the offices/departments in charge of legal duties related to the contractual relationships shall determine the content of mutual contractual liability for the implementation and control of security measures.
- (2) The Committee for CS shall carry out a regular risk assessment and regular checks of the security measures implemented for the services provided using its own resources or through a third party, and in response to risks and identified deficiencies, the Committee for CS shall ensure that they are dealt with in cooperation with the offices/departments and employees in charge.
- (3) A confidential document entitled ‘*Checklist for Supplier Audit and Inspection*’ has been created and is used for the assessment of the risks associated with suppliers.

Article 4

Requirements for contracts concluded with suppliers

- (1) Contracts concluded with suppliers must contain the following or a similar text:

The supplier takes into cognizance the fact that TBU is the controller of important information systems in compliance with § 3 Letter e) of the Cyber Security Act, and other information systems necessary to ensure proper operation of TBU as a public higher education institution established by the Act No. 404/2000 Coll. on the Establishment of Tomas Bata University in Zlín.

- (2) Contracts concluded with suppliers must also contain the following essentials, based on Annex 1, relevant to the specific supplier and the specific content of the supply or service:
- a) provisions on information security (in terms of confidentiality, availability and integrity),
 - b) provisions on the right to use the data,
 - c) provisions on the authorship of the program code or on program licenses,
 - d) provisions on supplier control and audit (customer audit rules),
 - e) provisions governing the supply chaining, while ensuring that subcontractors undertake to comply fully with the arrangements between TBU and the supplier and do not conflict with TBU's requirements applicable to the suppliers,
 - f) provision on the supplier's obligation to comply with the security policy of TBU or provisions on the approval of the security policies of the supplier by the obliged entity,
 - g) change management provisions,
 - h) provisions on the conformity of contracts with generally binding legal regulations,
 - i) provisions on the supplier's obligation to inform TBU about:
 - cyber security incidents related to the performance of the subject matter of the contract,
 - the manner in which risks are managed by the supplier and the residual risks related to the performance of the subject matter of the contract,
 - a significant change in the control of this supplier in accordance with the Business Corporations Act or a change in the ownership of essential assets, or a change in the authorization to handle these assets used by this supplier for performance under the contract concluded with the controller,
 - j) specification of requirements from the point of view of security to be complied with upon termination of the contract (for example, a transition period when cooperation is terminated, when it is still necessary to maintain the service before introducing a new solution, data migration, etc.),
 - k) specification of requirements for business continuity management in relation to suppliers (e.g. inclusion of suppliers in emergency plans, tasks of suppliers in the activation of business continuity management),
 - l) specification of requirements for the format of the transfer of data, operational data and information provided upon request by the controller,
 - m) data destruction policy,
 - n) provisions on the right to unilaterally withdraw from the contract in the event of a significant change in control of the supplier or a change in the control over the essential assets used by the supplier for the performance under the contract,
 - o) provision on penalties for breaches of obligations.

- (3) In the event of personal data processing, it is necessary to clarify the relationships between contractual partners (independent controllers, joint controllers and the relationship between the controller and the processor). In the case of joint controllers, it is necessary to determine the means and the purposes of the processing.

Article 5

Rules for conducting an audit

- (1) Customer audit rights must be enshrined in the contract.
- (2) Customer audit refers to a regular review of security measures by controlling the performance of contracts to the extent of compliance with the requirements for security measures, at least once per year. Details are specified in the *Supplier Evaluation Methodology*, which is a confidential document.

Article 6

Rules for the evaluation of suppliers

- (1) Supplier evaluation will be conducted on the basis of a fixed procedure defined in the *Supplier Evaluation Methodology*. The basis for the evaluation of suppliers will be the assessment of the degree of fulfilment of the requirements defined in the contract aimed primarily at ensuring information security and cyber security at TBU.
- (2) The result of the evaluation shall be used both for obtaining feedback within the ISMS, as well as for possible evaluation of the supplier in other public tenders.
- (3) The person in charge of performance of the subject matter of the contract (usually an applicant for the acquisition of a service or a good) is obliged to conduct supplier evaluation in cooperation with the CS Manager and with the use of counselling services provided by the staff of the Information Technology Centre always no later than upon termination of the contractual relationship with the supplier, and in the case of long-term cooperation, always at the end of each calendar year throughout the duration of the contractual relationship with the given supplier.
- (4) The results of the evaluation of suppliers conducted shall be submitted to the Committee for CS and shall have the character of a confidential document.

Document version			
Date	Version	Changed	Description of change
30 January 2024	01	CS Manager	Creation of document