Code:	SR/41/2023	
Ref. No.:	UTB/23/025921	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Asset Management Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	27 November 2023	Version: 01
Effective from:	1 December 2023	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Information Technology Centre, Legal Services	
Pages:	7	
Appendices:	1	
Distribution list:	TBU employees	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) The Asset Management Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* sets out procedures and protocols to support effective asset management 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 outline the strategic objectives and procedures of asset management with a focus on the primary and supporting assets of important information systems (hereinafter referred to as "IIS") at TBU.

(3) This policy shall apply to all TBU employees, information assets created or used within the IIS, and to users of these assets.

(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
Identification of primary assets

(1) The Cyber Security Manager (hereinafter referred to as the "CS Manager") shall identify the primary assets in the TBU's administration systems in cooperation with TBU senior executives.

(2) Primary assets are unique, based on key processes and activities important for the operation of IIS at TBU. Their identification is based on the following documents, e.g.:

a) TBU Statute,
b) Organizational Regulations of TBU Rectorate,
c) Internal rules and regulations,
d) Legislative resources,
e) Documents and publications of the National Cyber and Information Security Agency,
f) Internal acts of organizational management, etc.

(3) A primary asset is one of the following three types:

a) System,
b) Information/administration system,
c) Service.

(4) Based on the identification of primary assets, the CS Manager shall suggest for each asset whether it belongs to the ISMS.

(5) Each individual primary asset must be assigned an Asset Administrator and a Primary Asset Guarantor, both of whom must be listed in the Asset and Risk Assessment, which is a confidential document. Access to the Asset and Risk Assessment is usually limited to members of the Committee for Cyber Security Management (hereinafter referred to as the "Committee for CS"), asset administrators, guarantors and their superiors.

(6) Individual Primary Asset Administrators and Primary Asset Guarantors shall be appointed by the CS Manager in cooperation with TBU senior executives.

(7) The CS Manager shall submit for approval to the Committee for CS a proposal for the appointment of Asset Administrators and Primary Asset Guarantors.

Article 3
Assessment of primary assets

(1) The assessment of identified primary assets is managed and documented in the Asset and Risk Assessment, which is a confidential document with limited access.

(2) The assessment of primary assets shall be conducted by the Asset Administrator and the Primary Asset Guarantor in cooperation with the CS Manager.

(3) The assessment of the importance of primary assets in terms of confidentiality, integrity and availability is conducted by means of scales according to the tables listed in the Methodology for the Identification and Assessment of Assets and for Risk Management.

Article 4
Register of primary assets

(1) Primary assets must be recorded in an appropriate asset registration system and the register must contain detailed data, in particular:

a) ID,
b) Type of primary asset,
c) Name,
d) Category,
e) Specific details,
f) Asset Administrator,
g) Primary Asset Guarantor,
h) Personal details,
i) Legislation,
j) Assessment of the asset in terms of importance (availability, confidentiality, integrity),
k) Asset value,
l) Additional information about the asset – e.g. designated information system and the scope of the ISMS.

(2) The CS Manager and the Primary Asset Guarantor are responsible for keeping a central register of primary assets in electronic form.

(3) Records of primary assets are kept in the Asset and Risk Assessment.

Article 5
Identification of supporting assets

(1) The CS Manager shall identify supporting assets in the TBU's administration systems in cooperation with the Primary Asset Guarantor and the senior executives at TBU.

(2) Supporting assets ensure the existence of primary assets and can be common to multiple primary assets.

(3) When identifying supporting assets, it is necessary to take into account the architecture of the system and the need for the functionality of the primary asset.

(4) A supporting asset is one of the following six types:

a) Hardware,
b) Software,
c) Facilities – premises, buildings,
d) Means of communication - infrastructure,
e) Human resources,
f) Suppliers,
g) External systems and services.

(5) Each individual supporting asset must be assigned a Supporting Asset Guarantor, who must be listed in the Asset and Risk Assessment.

(6) The role of the Supporting Asset Guarantor may be identical to that of the supporting asset manager.

(7) Individual Supporting Asset Guarantors shall be appointed by the Director of the Information Technology Centre in cooperation with the CS Manager, Primary Asset Guarantors and Heads of offices/departments whose employees are responsible for the supporting assets.

(8) The CS Manager shall submit for approval to the Committee for CS a proposal for the appointment of Supporting Asset Guarantors.

Article 6
Assessment of supporting assets

(1) The assessment of identified supporting assets is managed and documented in the Asset and Risk Assessment.

(2) The assessment shall be conducted by the Primary Asset Guarantor and the Supporting Asset Guarantor in cooperation with the CS Manager.

(3) The assessment of supporting assets shall take into account the links between supporting and primary assets as follows:

a) Option A: Supporting assets inherit the values of primary assets.
b) Option B: Supporting assets are assessed on a case-by-case basis with respect to the value of the primary assets.
c) Option C: A formula is used to transfer the values of primary assets to supporting assets.

(4) The assessment of supporting assets must be conducted in accordance with the assessment of primary assets and shall be carried out at least in terms of confidentiality, integrity and availability by means of scales according to the tables listed in the Methodology for the Identification and Assessment of Assets and for Risk Management.

Article 7
Register of supporting assets

(1) Supporting assets must be recorded in an appropriate asset registration system and the register must contain detailed data, in particular:

a) ID,
b) Supporting asset category,
c) Supporting asset group,
d) Type of supporting asset,
e) Name,
f) Description of the supporting asset,
g) Asset Administrator,

h) Supporting Asset Guarantor,
i) Assessment of the asset in terms of confidentiality, integrity, availability,
j) Other relevant information about the asset – e.g. what kind of operator they have, whether it is a major supplier, whether it is a designated information system and the scope of the ISMS.

(2) The CS Manager and the Supporting Asset Guarantor are responsible for keeping a central register of supporting assets in electronic form.

(3) Records of supporting assets are kept in the Asset and Risk Assessment.

Article 8
Identification of links between primary and supporting assets

(1) The links identified between primary and supporting assets are included in the Asset and Risk Assessment.

(2) For the analysis and documentation of the properties, dependencies and composition of all assets, the interviews conducted with the Asset Administrator, Primary Asset Guarantor, Supporting Asset Guarantor and Heads of specialized offices/departments in cooperation with the CS Manager are crucial.

Article 9
Protection policy related to the individual asset levels

(1) In accordance with the Cyber Security Act, the following policy rules have been stipulated:

a) Protection policy necessary to be complied with in order to ensure the security of the individual asset levels:
   - By determining the methods to be used for identification of the individual asset levels.
   - By establishing policy rules for the handling and recording of assets according to asset levels, including rules for secure electronic sharing and physical transfer of assets, and
   - By setting the permissible uses of assets.

b) Protection policy corresponding to the asset level, and
c) Methods to be used for reliable erasure or disposal of technological data carriers depending on the level of assets.

(2) Assets shall be tagged in compliance with the policy established and according to the asset classification.

(3) The asset protection policy related to the individual asset levels is based on the level of confidentiality, integrity, and availability.

(4) In accordance with the asset assessment, allowable handling methods for the individual types of assets containing information shall be set out, and possible data destruction

methods for each of the asset levels shall be specified. The handling methods for each of the asset types must be chosen in proportion to each of the asset levels. The classification of the information must be carried out by the responsible Primary Asset Guarantor, Supporting Asset Guarantor or the author of the information. The level of the asset will have an impact on sharing of information about the relevant asset.

(5) The asset protection policy, including the methods used for determination of the individual asset levels, rules for handling and registration of assets according to asset levels, and the permissible uses of assets are set out in the documents entitled 'Asset Classification and Asset Handling', with both of them included in Annex 1.

(6) The defined policy on acceptable use of assets applies to all asset users, suppliers and third parties and must be documented.

(7) All TBU internal and external staff members are obliged to get acquainted with the classification of information and with the confidential information handling policy, and to comply with the policy when dealing with the said information.

Article 10
Data destruction methods

(1) The data erasure policy and the policy on the destruction of technological data carriers are defined in accordance with the Decree on Cyber Security and must contain adequate security measures corresponding to the value and importance of the assets.

(2) The data destruction policy shall be proportionate to the value and importance of the assets and shall take into account:

a) Value of the asset (especially in terms of confidentiality)
b) Technology (types and size of information carriers)
c) Whether the information carrier is under the control of the organization or not
d) Whether the data is part of a dedicated or multitenant environment
e) Who will carry out the data destruction (internal employee/external entity)
f) Availability of equipment and tools for disposal
g) Capacity of the carriers to be disposed of
h) Whether trained staff are available
i) Time required for the disposal
j) Price of disposal including costs related to tools, training, validation, reuse of the information carrier
k) Possible data destruction methods (e.g. destruction of the carrier, multiple overwriting of the data carrier, encrypting of the data to make it unreadable, etc.)
l) Applicable data destruction methods depending on the condition of the information carrier (e.g. if the device is damaged, it will not be possible to use the option of overwriting the information, and one of the methods of physical disposal will have to be used instead).

(3) The methods of disposal of technological information carriers, traffic data, information and copies thereof are the following:

a) Erasure:
- Data erasure resulting in the inaccessibility of the data for the system (deleting a data file, disposal of the printout in the garbage)
- It is the least secure data destruction method, as the information can be recovered.
- It is not applicable to non-rewritable media.
- Applicability of method for the confidentiality level of the asset: Low

b) Overwriting:
- Overwriting of confidential information with random values
- It is a data destruction method with a medium level of security, freely available tools do not enable information recovery.
- It can be replaced or combined by a secure destruction of cryptographic keys to encrypted information.
- It is not suitable for damaged media, non-rewritable media or large-capacity media.
- Applicability of method for the confidentiality level of the asset: Low to critical

c) Physical disposal of the information carrier:
- Destruction of the information carrier, also, if applicable, disassembly of the device and destruction of the information carriers, shredding of printouts
- The most secure data destruction method, as the information carrier cannot be reused, the original information cannot be recovered.
- Applicability of method for the confidentiality level of the asset: Medium to critical

Document version			
Date	Version	Changed	Description of change
27 November 2023	01	CS Manager	Creation of document