Code:	SR/36/2024	
Ref. No.:	UTB/24/026133	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Access Control Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	29 October 2024	Version: 01
Effective from:	1 November 2024	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Information Technology Centre, Legal Services, Data Protection Officer	
Pages:	4	
Appendices:	0	
Distribution list:	TBU employees	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D. m. p.	

Article 1
Introductory provisions

(1) The Access Control Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* sets out and specifies the requirements for cyber security (hereinafter referred to as "CS") 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 establish rules for user access to TBU important information system (hereinafter referred to as "IIS"), specifying procedures for authorizing, establishing, changing and revoking of access rights.

(3) This policy applies to all TBU employees, information assets created or used within the IIS, and 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
Basic access control rules

(1) The Cyber Security Manager (hereinafter referred to as the "CS Manager") is responsible for establishing the basic rules in the area of access control, and the Primary Asset Guarantor is responsible for access control.

(2) The Primary Asset Guarantor shall keep a record of all user accounts, which can be used to uniquely identify the person using a given user account.

(3) Access and attempted access shall be automatically recorded and monitored. Records shall be retained for a minimum of 6 months.

(4) Authentication data must not be shared by more than one person.

(5) The allocation of access rights to users and administrators shall be governed by the following rules:

a) For primary assets, the allocation process is managed and documented.
b) Access rights are granted only to the extent necessary for the performance of the user's professional duties and are defined according to the principle of the minimum necessary for the user's activities.
c) Changes to the scope of access rights shall be managed and approved on the basis of a *Request for Allocation/Change of Access Rights*.
d) An up-to-date list of all user accounts for primary assets shall be maintained, and a system of user roles and authorizations shall be defined and approved by the relevant chief executive or asset administrator.
e) A record shall be kept of accesses and attempts to access the primary asset.
f) The fundamental tool for user management is identity management.
g) Primary assets are accessed through the use of a Virtual Private Network (VPN) or HTTPS protocol.
h) Multi-factor authentication is used if the technical conditions of the individual primary assets allow it.
i) The roles of users and administrators are separated.
j) The emergency access control procedure is documented by the Primary Asset Guarantor.

Article 3
Requirements for access control

(1) The access control system consists of:

a) a description of the scope of each user role,
b) a description of the training requirement for each user role,
c) a definition of the critical combination of roles,
d) a description of the process for allocating user roles,
e) a description of the user identity verification technology,
f) a description of secure user behaviour,
g) a definition of the user access lifecycle,
h) enforcing of user identity authentication rules.

Article 4
Principle of minimum authorizations/need to know

(1) Each user has access to only those assets that he/she absolutely needs to do his/her job.

(2) The basic scope of authorization for each primary asset is defined as the minimum required for the activities needed by the user. Authorizations are broken down into user roles.

Article 5
Access control life cycle

(1) Primary assets have documented access control, which includes the following phases:

a) request for access rights,
b) approval and granting of access rights,
c) periodic review of access rights,
d) changing of access rights,
e) revocation of access rights.

(2) The request for a right of access shall specify at least the following information:

a) the person entitled to make the request,
b) the user,
c) the scope of the authorization and, where appropriate, the substantiation.

(3) The authorization and access rights allocation process shall define at least the following information:

a) the persons authorized to approve the request,
b) the persons in charge of setting the relevant authorizations.

(4) The process of changing of access rights shall define at least the following information:

a) the persons authorized to approve the request,
b) the persons in charge of setting the relevant authorizations.

(5) Access rights to information and primary assets shall be revoked:

a) upon change of job position or user role reported by the authorized chief executive,
b) upon termination of the employment or similar relationship automatically.

(6) The access control system and established access control rules are regularly reviewed by the Primary Asset Administrator.

Article 6
Privileged access management

(1) Privileged access refers to an access authorization to an account that allows the user to perform any of the following activities in the IIS beyond that of a normal user:

a) make changes to the setting,
b) change the scope of authorizations assigned to individual roles and users,
c) perform service activities without the user being present.

(2) Privileged access is assigned a different user identifier from the commonly used user account.

(3) Normal activities are not performed using privileged access.

(4) Regardless of the type of user account authorization, the login session must be set to a time limit, followed by an automatic logout from the system when it expires.

Article 7
Access control in emergency situations

(1) In order to ensure operational continuity at TBU during a cyber security incident and cyber security breach or other emergency situations, access authorizations may be set on a one-time basis beyond the standard mode of operation.

(2) Processes for handling cybersecurity incidents and cybersecurity breaches or other emergency situations are defined in the emergency plan and developed for each IIS.

Article 8
Regular review of access authorizations, including the distribution of individual users in access groups

(1) The process for reviewing access authorizations is defined in the security documentation prepared for the primary asset.

(2) Access authorizations are controlled by the Primary Asset Guarantor across the full range of user rights.

(3) The documentation for reviewing of access authorizations shall include, as a minimum:

a) definition of the control cycle,
b) the persons carrying out the inspection,
c) a record of the inspection carried out,
d) the procedure for correcting any deficiencies found.

(4) The CS Manager shall prepare a report on the review of access authorizations, which shall be approved by the TBU Cyber Security Management Committee and submitted to the TBU Management Board.

Document version			
Date	Version	Changed	Description of change
29 October 2024	01	CS Manager	Creation of document

This English version of the internal regulation is not legally binding; it is for informational purposes only and does not have to correspond to the Czech version of the document.