Code:	SR/28/2024	
Ref. No.:	UTB/24/022963	
Category:	INTERNAL	
Type of document:	RECTOR'S DIRECTIVE	
Title:	Human Resources Security Policy	
Liability:	Tomas Bata University in Zlín	
Issue date:	27 September 2024	Version: 01
Effective from:	1 October 2024	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Information Technology Centre, Legal Services	
Pages:	6	
Appendices:	2	
Distribution list:	TBU employees	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D., m. p.	

Article 1
Introductory provisions

(1) The Human Resources Security Policy as part of the *Declaration of Cyber Security at Tomas Bata University in Zlín* establishes 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 the policy is to set out the principles and requirements that apply to TBU employees throughout their lifecycle with the employer, starting with the commencement of their employment, through their performance at work and any changes, and ending with the termination of their employment at TBU.

(3) This policy applies to all TBU employees, information assets created or used within an important information system (hereinafter referred to as "IIS"), and to users of those 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
Roles and responsibilities

(1) The information security roles and responsibilities are defined in the job descriptions of the staff by their immediate superior in accordance with the established model job description

of the supporting asset guarantors approved by the Cyber Security Management Committee. Information security staff roles and responsibilities are defined and documented in accordance with the *Information Security Management System Policy*.

(2) Information security roles and responsibilities include:

a) the requirement to implement and comply with policies in accordance with the information security policy,
b) a requirement to protect assets from unauthorised access, disclosure, modification, destruction or disruption,
c) a requirement to perform specific security processes or activities, legal means,
d) a requirement to establish clear accountability for activities undertaken,
e) a requirement to report security incidents or other security risks.

(3) As part of the interview process, candidates shall be clearly informed by their immediate superior or by the interviewer about the roles and responsibilities associated with the position for which they are applying.

(4) Job descriptions are used to document information security roles and responsibilities.

(5) Chief executives continuously monitor user compliance with information security in accordance with established policies and procedures.

Article 3
Employee vetting

(1) All applicants for employment shall be screened in accordance with applicable laws, internal regulations and ethical principles. The screening shall take into account the requirements established by the classification of the information to which the recruit will have access, as well as his/her reliability and potential risks.

(2) The screening shall take into account compliance with privacy and personal data protection and related regulatory requirements.

(3) When an applicant for employment is hired for a position with access to confidential information, the Human Resources will conduct a background check based on:

a) the availability of sufficient references, such as professional and personal references,
b) verification of claimed educational and professional qualifications,
c) verification of identity,
d) where appropriate, a more detailed check (e.g. lustration certificate, extract from the criminal record, for positions with material responsibility a check of the debtors register, etc.).

Article 4
Rules for the development of security awareness and manners to assess it

I Manners and forms of briefing the users

(1) In addition to the initial staff training, employees who are given access to sensitive information and information processing facilities shall be informed by their immediate superior about the information security rules and shall sign a document containing the following information:

a) the rights and legal responsibilities of staff in user roles,
b) the responsibilities of staff for handling information received from other organisations and parties involved,
c) TBU's responsibilities for handling personal data, including data created in the course of an employment relationship,
d) the extension of responsibilities beyond the TBU premises and outside normal working hours (e.g. in the case of telework, during a business trip, etc.),
e) a description of the steps to be taken in the event of non-compliance with safety requirements by employees, as set out in the *Work Regulations of TBU*, as amended.

The signed document, a template of which is attached as *Annex 1* to this Directive, shall be kept in the employee's personnel file.

II Manners and forms of briefing the asset guarantors

(2) Asset guarantors shall be briefed by the IT Security Specialist on the rules for ensuring information security and on the rules for the performance of duties related to the job position of the primary/secondary asset guarantor, or they shall be briefed on specific issues relating to a particular group of assets. A record of the briefing shall be made, a template of which is attached as *Annex 2* to this Directive, and signed by the asset guarantor.

III Manners and forms of briefing the administrators

(3) Administrators shall be briefed by their immediate superior on the rules for ensuring information security and on the rules for the performance of duties related to the job position of the administrator, or shall be briefed on specific issues related to the managed equipment before specific systems or equipment are entrusted to their management. A record of the briefing shall be made, a template of which is attached as *Annex 2* to this Directive, and the record signed by the administrator shall be kept in the employee's personnel file.

IV Manners and forms of briefing the persons in security roles

(4) Persons performing other security roles as defined in Appendix 6 to the Decree on Cyber Security shall be briefed by the Cyber Security Manager (hereinafter referred to as the "CS Manager") as part of their appointment to the role on the rules for ensuring information security and the rules for performing the given role, or will be briefed on specific issues related to the given role. A record of the briefing shall be made and signed by the person performing the security role and the form of the record shall be defined by the CS Manager.

(5) The procedure for the implementation of security awareness development is described in detail in a separate document entitled *Security Awareness Development Plan*.

Article 5
Security training for new staff

(1) Every new employee receives initial security training and then regular refresher training at least once a year (taking into account any changes in documentation, procedures, etc.).

(2) All employees receive regular information security training at least once a year in accordance with the *Security Awareness Development Plan*.

(3) Only an employee who has been properly trained in information security and security measures relevant to his/her job position and has received training in the information systems he/she will use in the performance of his/her employment may use information and communication technology devices. A record shall be made of the familiarisation and training and shall be kept in the employee's personnel file.

(4) In the event of a serious cybersecurity incident, employees will receive additional training.

(5) The aim of the safety training is to learn how to prevent security incidents and breaches, how to behave in unusual situations and how to learn from them. This means that employees:

a) understand their role and are aware of their responsibilities towards their employer and their environment,
b) understand the principles of the information security management system and the resulting procedures,
c) behave in accordance with the established security measures,
d) have an understanding of the management, operational and technical mechanisms used to ensure the security of the assets for which they are responsible and/or with which they work.

(6) The CS Manager shall prepare and maintain reports on security training, which shall include, as a minimum, the date of the training, the subject of the training and a list of persons who have received the training, including their signatures in the case of training scheduled to be attended in person.

(7) The CS Manager is responsible for conducting information security training sessions.

Article 6
Rules for dealing with breaches of the information security management system policy

(1) In the event of a serious security incident caused by a violation of the TBU's security policy by an employee, proceedings shall be initiated against such employee in accordance with the relevant provisions of the Act No. 262/2006 Coll., Labour Code, as amended. The method of management shall be appropriate to the nature of the incident and its impact on TBU.

(2) In the event of such a breach, the relevant chief executive shall take into account:

a) completion of security training,
b) the nature of the security breach and its impact,
c) whether it is his/her first or repeated violation,
d) whether the breach is intentional or negligent,
e) the relevant legislation,
f) existing contracts,
g) other relevant circumstances.

(3) If a crime is suspected, TBU shall proceed in accordance with the relevant provisions of the Code of Criminal Procedure and related legislation.

Article 7
Rules for termination of employment relationship or change of job position

(1) When deciding whether to terminate or modify the employment relationship, the chief executive in charge must take into account the following risk factors:

a) the reasons for the change or termination of the employment relationship,
b) the existing responsibilities of the employee,
c) the value of the assets to which he/she may have access.

(2) Prior to the termination or modification of the employment relationship, the chief executive in charge shall remove or restrict, or issue written instructions to remove or restrict, access rights to information assets and information processing devices.

(3) If access rights are shared by more than one employee, the chief executive in charge shall decide to change the group access rights, remove those users from all group access rights lists, and prohibit all other employees from sharing information with the departing employee. The chief executive in charge shall inform the asset manager of this action.

(4) In serious cases, the employee's access rights and privileges shall be immediately revoked. If there is a threat of continued unauthorized or prohibited activity, the employee shall be immediately removed from the TBU premises and denied access to the workplace.

I Changing access rights when changing job position

(5) In the event of a change in the employment relationship, the chief executive in charge must, in addition to changing the job description, issue written instructions to change access authorizations, both in terms of physical access (access cards, keys, etc.) and, above all, authorizations for the TBU information systems, in order to reflect the employee's new job position. The chief executive in charge shall make a formal record of this.

II Return of entrusted assets and withdrawal of rights upon termination of employment

(6) In the event of termination of the employment relationship, the employee must return all loaned devices, documents and other equipment relating to the assets entrusted to him/her.

The persons responsible for the areas concerned must formally acknowledge receipt of all assets.

(7) In the event of termination of employment of key employees (users with assigned roles in the IIS, primary asset guarantors, supporting asset guarantors in the categories of technical equipment, software and communications) or employees in security roles, a handover of responsibilities shall be ensured.

(8) The procedure and formalities for terminating employment are the responsibility of the relevant chief executive, who will ensure that all security aspects and appropriate procedures are followed. In cases where this is the content of the contract, he/she must inform employees, contractors or third parties of operational and personnel changes.

(9) As part of the process of termination of employment, the chief executive in charge shall formally confirm the removal of all access rights of the departing employee, both in terms of physical access (access cards, keys, etc.) and, in particular, access rights to the TBU information systems (removal of all access rights of the employee as of the date of termination of employment).

Document version			
Date	Version	Changed	Description of change
27 September 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, therefore, does not have to correspond to the Czech version of the document.