Code:	SR/29/2024	
Reference number:	UTB/24/022964	
Type of document:	INTERNAL	
Category:	RECTOR'S DIRECTIVE	
Title:	Policy for Safe Use of Mobile Devices	
Liability:	Tomas Bata University in Zlín	
Issue date:	27 September 2024	Version: 02
Effective from:	1 October 2024	
Issued by:	Rector	
Prepared by:	Cyber Security Manager	
In cooperation with:	Information Technology Centre, Legal Services	
Pages:	4	
Appendices:	0	
Distribution list:	All TBU employees	
Signature of authorized person:	Prof. Mgr. Milan Adámek, Ph.D. m .p.	

Article 1
Introductory provisions

(1) The Policy for Safe Use of Mobile Devices as part of the *Cyber Security Declaration of Tomas Bata University in Zlín* sets out the rules for the use of mobile devices in compliance with Act No. 264/2025 Coll., on Cyber Security, as amended (hereinafter referred to as the "Cyber Security Act") and related legal regulations at Tomas Bata University in Zlín (hereinafter referred to as "TBU".

(2) The purpose of this policy is to set out binding rules and requirements related to the setup of mobile devices used to perform work, study-related and other activities (hereinafter referred to as "activities") by users at TBU. The term "user" refers to:

a) TBU students and employees who have been assigned an user account in order to access the TBU Computer Network (hereinafter referred to as the "TBU Network").
b) Guests and other users using the TBU network in accordance with the relevant roaming or other contracts.
c) Appropriately, also employees of suppliers and of third parties in accordance with concluded contracts on provision of services or on supply of products.

(3) The individual terms used in this Policy are, in particular, defined in the Cyber Security Act and in related legal regulations. An overview of the individual terms is included in the document *Basic Terms of Cyber Security*, which is available on the TBU website in the *Cyber Security* section.

Article 2
Rules and procedures for safe use of mobile devices

(1) The term "mobile devices" refers to all mobile devices enabling displaying, editing, storage, transmission or printing of data, i.e. in particular:

a) Laptop
b) Tablet, iPad and similar portable devices

c) Smartphone
d) Removable disk and memory card used in such devices
e) Flash memory, digital camera, MP3 player, etc.

(2) The use of mobile devices purchased by TBU and registered as TBU property is governed by the following security rules:

a) Users are required to use such mobile devices for the performance of their activities which have been assigned to them by TBU and which meet TBU safety requirements.
b) Users are not allowed to make own modifications and installations of applications on a mobile device; all installations of applications must be made only by an authorized employee, usually by the IT administrator of the relevant component part, in accordance with the *Organizational Security Policy*.
c) Users are required to protect a mobile device against theft and misuse.
d) Users are required to report the loss of a mobile device without delay.
e) Users must not enable an unauthorized person to access a mobile device.
f) Users are required to connect a mobile device specified in Paragraph 1, Letters a) to c) to the TBU Network at fixed intervals for the purpose of updating and checks.
g) Users are not allowed to change the safety rules set on a mobile device.
h) Users are not allowed to use software that has been identified by the National Cyber and Information Security Agency as a security threat or vulnerability.
i) Removable disks, memory cards and flash memories must be encrypted.
j) Users are required to protect a mobile device referred to in Paragraph 1, Letters a) to c) by a password (including a PIN) or by a gesture.
k) Users are required to use only the Virtual Private Network (VPN) for remote access to selected information systems and services, databases and applications.

(3) The use of all other mobile devices is governed by the following security rules:

a) Installation of applications on mobile devices must not harm the information acquired and processed within the TBU regulated services in accordance with the *Information Security Management System Policy*.
b) Users are required to protect their mobile device against theft and misuse.
c) Users are required to immediately report the loss of a mobile device containing information as defined in Letter a).
d) Users must not allow another person to access a mobile device containing information as defined in Letter a).
e) Users are required to protect a mobile device referred to in Paragraph 1, Letters a) to c) by a password (including a PIN) or by a gesture.
f) Users are required to use only the Virtual Private Network (VPN) for remote access to selected information systems and services, databases and applications.

Article 3
Rules for connection of mobile devices to the TBU network and responsibilities of users

(1) The following rules apply to mobile devices listed in Article 2, Paragraph 1, Letters a) to c) of this Directive, i.e. usually devices equipped with a wireless network communication interface.

(2) In the TBU buildings, users are provided with wireless connectivity to the TBU computer

network by means of their mobile devices.

(3) The TBU network has been involved in the **eduroam** (www.eduroam.cz) international project. It is the **eduroam** network that is primarily intended for the connection of users' mobile devices.

(4) Users can connect to the **eduroam** network using valid access details provided to them by their home organization involved in the **eduroam** project.

(5) Up-to-date information on availability at particular locations, on the mode of/on the configuration for connecting are specified at eduroam.utb.cz.

(6) Wireless networks of various names may be set up within the TBU network for special purposes. The TBU Information Technology Centre (hereinafter referred to as "ITC") bears the responsibility for the setting up of such networks.

(7) The users of the ***eduroam*** network are obliged to:
   a) Adhere to the rules for ***eduroam*** network use defined by the Roaming Policy of the eduroam.cz federation, as amended (www.eduroam.cz).
   b) Observe the Access Policy (AP) for the CESNET e-infrastructure, as amended (www.cesnet.cz).
   c) Adhere to the provisions of the *Safety Policy of the Communication Network.*
   d) Use only the assigned access details; the users bear full responsibility for any misuse of the access details assigned.
   e) Use the DHCP protocol for assignment of an IP address. The assignment of a static IP address is a serious breach of these rules.
   f) React to requests and instructions received from the network administrators of the host as well as of the home network and also to those received from the roaming centre of the CESNET association without delay.

(8) Users' mobile devices must comply with valid standards and with the homologation sheet in accordance with the IEEE 802.11 standards for wireless access and must have a suitable system configuration, applied security upgrades, etc. in order to be protected in an appropriate manner.

(9) Users are not permitted to run any such server applications and applications on their mobile devices which may have a negative impact on the network operation or on the network services, overload the network and/or waste the network's capacity.

(10) The operation of other wireless networks than those approved in writing by the TBU Information Technology Centre is forbidden.

(11) In the event that a user fails to observe these rules and/or uses an insufficiently protected or a virus-infected mobile device, the network administrator may temporarily withdraw the user's right to access the TBU network. Any other sanctions imposed in compliance with other regulations are not affected thereby.

Article 4
Final provisions

(1) This Directive abrogates and replaces the Rector's Directive No. 4/2016.

Version of document			
Date	Version	Changed	Description
27 September 2024	01	Cyber Security Manager	Creation of document
15 May 2026	02	Legal Services, ITC	Amendment No. 1

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