Univerzita Karlova

Ref. No. UKRUK/21058/2026-18

Rector's Directive No. 18/2026

Cybersecurity rules at Charles University

To implement:	Art. 11 (4) and Art. 22 of Rector's Directive No. 35/2024, Information Security Management System Policy
Guarantor:	RNDr. Jan Pačes, Ph.D., Member of the Rector's Board for Institutional Resilience and Knowledge and Technology Transfer
Responsible office:	Cybersecurity Department of the Rectorate
Date of force:	20 May 2026
Date of effect:	1 June 2026

Cybersecurity Rules at Charles University

PART ONE
INTRODUCTORY PROVISIONS

Article 1
Introductory provisions

1. The present directive has been adopted to implement Art. 11 (4) and Art. 22 of Rector's Directive No. 35/2024, Information Security Management System Policy, and sets out rules, procedures, and security measures in the area of the secure handling of information and of information and communication technology (ICT) resources, which are binding on all employees of Charles University ("University"), including employees who work for the University on the basis of an agreement to complete a job ("DPP Agreement") or an agreement to perform work ("DPČ Agreement").
2. This directive also applies by analogy to persons other than employees who must comply with these rules on other legal grounds.

Article 2
Definitions

For the purposes of the present directive:

a) 'technical asset' means hardware and software equipment;
b) 'hardware (HW)' means the physical components of the system (devices) or a part thereof;
c) 'software (SW)' means a collection of programs and related instructions designed for processing data and performing specific tasks using different types of devices;
d) 'supplier' means an entity engaged in the operation, development, administration, or security of the University's information systems;
e) 'availability of information' means ensuring that information is available to the authorised employees when necessary;
f) 'confidentiality of information' means maintaining the confidentiality of information by making it accessible only to the persons who are authorised to access and handle such information;
g) 'integrity of information' means ensuring that information has not been unlawfully modified by protecting its accuracy and completeness;
h) 'protected information' means information which is essential for the running of the University and the disclosure, misuse, destruction, loss, unauthorised modification, or unavailability thereof could cause harm to the University or threaten the due performance of the University's mission;
i) 'internal information' means information which is not publicly accessible and serves the University's internal purposes;
j) 'confidential information' means protected information or internal information;
k) 'information system (IS)' is a functional set ensuring targeted and systematic collection, processing, storage, and accessibility of information and data that comprises data and information sources, carriers, and technical, program, and working resources and procedures, and the related rules;

l) ‘cybersecurity’ means the legislative, organisational, technical, and educational resources designed for ensuring the protection of cyberspace with the aim of ensuring the confidentiality, integrity, and availability of information in the University’s cyberspace;
m) ‘security event’ means an event which may result in a security incident;
n) ‘security incident’ means a breach of the security of information in information systems, a breach of the security of services or the security and integrity of electronic communication networks, a violation of security policies, security principles, or the standard security rules for the operation of information and communication technology;
o) ‘medium’ means an external memory device, such as a USB flash drive, external drive, CD, DVD, and similar devices;
p) ‘mobile device’ means a portable electronic device with an operating system, such as a mobile phone, laptop, tablet, and similar devices;
q) ‘computer network of Charles University’ means a set of technical information and communication technology resources including, but not limited to, cabling, network elements, servers, computers, mobile devices, and other specialised computer technology giving employees access to the services provided at the University;
r) ‘multi-factor authentication (MFA)’ means an authentication mechanism using two or more authentication factors;
s) ‘user account’ means the employee’s account for accessing the information system, which corresponds to the employee’s work position and is defined by unique log-in credentials;
t) ‘virtual private network (VPN)’ is a network which allows an internet connection between remote users and the destination LAN, secured by an encrypted tunnel between two points;
u) ‘device’ means a technical ICT device, such as a desktop computer, laptop, smartphone, tablet, thin client, printer, or other specialised hardware, including SoC-based smart meters, and IoT devices;
v) ‘ICT department’ means the Computer Science Centre of the University and the departments at faculties and other units of CU in charge of the administration of ICT resources.

PART TWO
CYBERSECURITY RULES

Article 3
Cybersecurity rules

1. For the purpose of ensuring cybersecurity, all employees must comply with the rules hereunder for handling information in paper and digital form and using ICT resources and information systems securely.
2. Employees have, in particular, the following obligations:
   a) to report cybersecurity events and incidents which could breach the University’s cybersecurity via the reporting channels in accordance with Art. 19;
   b) to cooperate with supervisory bodies and other persons according to the instructions given by the cybersecurity manager.
3. Employees are also responsible for securing information and services within the scope of their competences and they are therefore involved in ensuring the confidentiality, availability, and integrity of the information processed and the services provided.

Article 4

Secure handling of assets

1. Employees aim to secure ICT devices, information, and data against loss, misuse, damage, theft, and other threats ("threats") as appropriate both during their working hours and within a reasonable scope also after they leave their workplace.
2. Before leaving, employees must secure, as appropriate, all written documents and media, including removable media, which contain confidential information, with regard to the circumstances at the workplace, against breaches and being easily accessible by unauthorised persons.
3. In the case of closed workplaces without external employees and with secure physical access, these rules may be modified in justified cases with regard to the nature of the activities performed at the workplace to avoid excessive burden and delays in everyday operation.
4. Employees working remotely must log off from the University's information systems, including remote access via virtual private network (VPN), after finishing their work.
5. It is prohibited to take devices out of the University's premises unless it is directly related to the employee's work tasks.

Article 5

Passwords and multi-factor authentication

1. Where a given system enables log-in via multi-factor authentication (MFA), the ICT department which administers the system ensures that employees use such log-in method together with a password as the primary authentication method.
2. Employees may use their own devices for multi-factor authentication under paragraph 1 in accordance with the conditions under Art. 9. If an employee does not use his or her own device for this purpose, a device provided by the employer is used.
3. Employees must comply with the rules for creating and handling passwords, and are responsible for keeping their passwords confidential.
4. Employees must comply with the following rules for creating and handling passwords:
   a) have a unique password for each individual device, information system, and application;
   b) not use an identical password for private services and for the University's user accounts;
   c) not use, in their passwords, their name or surname, the name or surname of a close person, date of birth, and other information which is directly linked to the employee's person and is generally available;
   d) not store passwords in locations where they might be stolen or revealed;
   e) not store passwords in web browsers if they might be accessed by another person;
   f) change the password in the following cases:
      i. after the first log-in to the system unless the password was created directly by the employee; or
      ii. if there is a justified reason to believe that the password has been compromised; and
   g) comply with the rule that a password must have at least 8 characters and meet at least 3 of the following complexity requirements unless the use thereof is precluded by the given system:
      i. at least one upper-case letter (e.g., AKZSD);
      ii. at least one lower-case letter (e.g., bsdijsd);
      iii. at least one digit (e.g., 7291); or
      iv. at least one special character (e.g., '.'; ','; '@'; '#'; '%'; '!'; '$'; '&'; '+'; '-').

5. If an employee is not able to use multi-factor authentication (MFA) for a specific system, he or she creates the password according to the rules under paragraph 4 and, in addition to that:
   a) does not use the previous 12 passwords;
   b) changes the password no later than every 18 months;
   c) complies with the rule that a password must have at least 22 characters for a password for a technical asset, 17 characters for an administrator account, and 12 characters for a user account, and, at the same time, the password meets all of the following 4 complexity requirements:
      i. at least one upper-case letter (e.g., AKZSD);
      ii. at least one lower-case letter (e.g., bsdijsd);
      iii. at least one digit (e.g., 7291); and
      iv. at least one special character (e.g., '.'; ','; '@'; '#'; '%'; '!'; '$'; '&'; '+'; '-').
6. The ICT department which administers the given system must ensure that employees are not able to set a password which does not meet the requirements for a user account password under paragraphs 4 (g) and 5.

Article 6

Electronic Mail

1. Employees must use the assigned email account to perform their work tasks and, at the same time, they may not use their private email accounts to perform their work tasks. The automatic forwarding of work messages to private email addresses is not allowed.
2. It is prohibited to register and use the University's email address for e-shops, sending advertising messages, newsletters, and other similar services unless they are directly related to the performance of work tasks. A user must unsubscribe from active services which are not related to the purpose for which the email address was provided unless such measure would require unreasonable effort.
3. Employees must comply with the security rules for eliminating phishing emails. For this purpose, they must:
   a) check who the actual sender of an email is in the case of non-standard syntax;
   b) pay attention to messages which contain the following:
      i. major grammatical mistakes;
      ii. requests for entering or sending log-in credentials;
      iii. requests for payments; or
      iv. requests for entering banking or personal data; and
   c) in case of any suspicions, employees must observe the following rules:
      i. not open, or respond to, emails with suspicious content;
      ii. not enable macros when opening files;
      iii. verify the authenticity of the sender's email address, where possible;
      iv. not open suspicious email attachments and not enter data in, or click on, active windows or links.

Article 7

Computers, laptops, and other devices

1. When using computers, laptops, and other devices provided by the University, employees have the following obligations:
   a) prevent unauthorised and other persons from using the devices;
   b) not service or upgrade the devices themselves or otherwise; these activities may only be carried out by an authorised employee of the ICT department or another employee who has

been given explicit approval to do so within his/her work position or authorised by the ICT department;
c) report a lost device to their superordinate without delay; and
d) connect the device to the University's computer network, in particular, for the purpose of installing updates in the case of mobile devices.

2. Devices used for performing work may only be connected a secured network using an encrypted connection via a virtual private network (VPN).

Article 8

Use of a private device for work purposes

Employees who use their private devices for work purposes must ensure or set the following:

a) regular updates of the operating system of the device and immediate updates of security updates; devices with an operating system which is not supported may not be used;
b) activated and updated firewall and a secure anti-virus software;
c) disk encryption;
d) automatic lock or log-off for the device;
e) installation of applications only from secured, verified sources;
f) locking the device with a secure alphanumeric password, fingerprint, or facial recognition; and
g) protection against modifications decreasing security.

Article 9

Copy machines, printers, and scanners

When operating and using printers, scanners, copy machines, and other similar devices, it is prohibited to leave the devices while confidential information is being processed.

Article 10

Media

1. Employees may use removable media and store information on them only if necessary to perform their work, and they are responsible for the security of the removable media and the content thereof. If an unknown removable medium is found, it is prohibited to insert the medium in a computer, laptop, or other device; employees are obliged to hand over such medium to the ICT department.
2. Employees may not take removable media out of the University's premises unless it is directly related to the employee's work tasks. If an employee must take a removable media out of the University's premises, he or she must equip the medium, as appropriate, against theft and unauthorised use of the information stored on the medium.
3. In particular, employees must encrypt media which contain confidential information or further secure such media otherwise, as appropriate.
4. If a medium which contains confidential information is lost or stolen, the employee must report such fact in accordance with Art. 19.

Article 11

Connecting devices to the University's network

1. Devices may be connected to the University's internal, non-public networks only by the employees of ICT departments at the University.
2. An employee's access to the network may be denied or restricted if the employee's device does not comply with the requirements hereunder, in particular under Art. 12.

Article 12

Software updates

1. Software updates are installed by the ICT department usually in the form of an automatic installation, or manually. Employees must provide the necessary cooperation for the installation of the updates.
2. Employees who use devices which are not under the remote administration of the ICT department are subject to the obligations regarding the use of devices under Art. 8 by analogy.

Article 13

Internet

1. Employees may not use a device to access the following services:
   a) online games;
   b) pornography and erotic websites;
   c) intentional masking of the employee's identity, in particular, via TOR;
   d) P2P networks using tools such as torrent; and
   e) public cloud storages which are not administered by the University or the University's supplier of such services.
2. Employees may not download or otherwise save the following file types:
   a) applications and Windows libraries (e.g., exe, dll);
   b) Unix applications;
   c) Unix/Linux installation packages (e.g., deb, rpm);
   d) audio files (e.g., mp3, wav);
   e) video files (e.g., avi, mp4, mpeg, mpg); and
   f) Torrent files.
3. The restrictions under paragraphs 1 and 2 do not apply to cases which are directly related to work tasks or setting devices in a way to allow the performance of work tasks.
4. In the case of an ongoing security threat, ICT employees are authorised to restrict access to a website or other ICT services which may be used to spread a threat.

Article 14

Local area network (LAN)

Employees with access to the University's internal networks are responsible for the activities they perform using these internal networks. For security reasons, employees may not carry out, in particular, the following activities (with the exception of authorised employees who perform such activities for the purposes of their work tasks):

a) using the network elements for personal purposes and consuming a high amount of the network capacity;

b) spreading malicious code (malware);
c) changing the network configuration of network components and end stations;
d) using tools designed for intentional identity masking;
e) port scanning;
f) performing any form of monitoring of the computer network which might result in data capture;
g) circumventing the employee's authentication or the security of any device, computer network, or user account;
h) carrying out activities not related to work using the University's devices, which could lead to restricting or denying access to services provided to other employees;
i) using programs, scripts or commands, and sending messages with the intention to restrict or disable the provision of services or terminal services locally or via a computer network, internet, or intranet;
j) exploiting security gaps or creating attacks against communications in computer networks; and
k) providing information on the configuration and topology of the network to third parties, unless such activities are a part of the employee's work tasks, and interfering with the data cabling except for everyday manipulation.

Article 15

Storing, backing up, and archiving data

Employees may save files which contain confidential information only to officially supported tools used by the University in the designated folders or the University's information systems, using exclusively the account provided by the University.

Article 16

Returning assets

1. Upon terminating employment, employees return or hand over all assets provided to the authorised person. The above rule applies, in particular, to returning or handing over the following:
   a) ICT resources;
   b) identification cards, chips, and other means of identification or authentication;
   c) documents, software, software licences;
   d) data; and
   e) log-in credentials for services, accounts, and systems.
2. If an employee's work position changes, paragraph 1 applies with the necessary modifications.

Article 17

Remote communication tools

1. When communicating remotely, in particular, in the case of audiovisual or audio calls, employees must preferentially use the tools provided by the University.
2. Employees verify the identity of the persons with whom they are communicating as appropriate, in particular when sharing confidential information.
3. While calling and sharing information, employees may only share information which is necessary for work purposes and which the employees concerned are authorised to access.

Article 18

Use of artificial intelligence

Employees take a cautious approach when using AI tools and make sure to protect personal data and confidential information in accordance with the legal regulations and the University's internal rules.

PART THREE
REPORTING SECURITY EVENTS AND INCIDENTS

Article 19

Reporting security events and incidents

Employees report security events and incidents which might result in a cybersecurity breach to the Charles University computer network security team (CSIRT) at abuse@cuni.cz. Other relevant procedures for reporting security events and incidents, including the scope thereof, may be determined by the head of the University's Cybersecurity Department in accordance with Art. 21.

PART FOUR
FINAL PROVISIONS

Article 20

Dean's directives and directives of a director of another unit

A dean of a faculty or a director of another unit may adopt a directive which provides, in accordance with this Rector's directive, further details of compliance with cybersecurity rules at a faculty or other unit of the University.

Article 21

Related documents

In order to implement the technical and organisational matters under this directive and to further specify procedures in the area of cybersecurity, the head of the Cybersecurity Department of the Rectorate may adopt binding methodology guidelines and rules after discussion within the Cybersecurity Committee, and issue recommendations and awareness-raising materials of an informative nature.

Article 22

Transitional Provisions

1. The rules set out in Art. 5 apply as follows:
   a) to the employees of the Rectorate of the University as of the date of effect hereof;
   b) to the employees of other units of the University no later than as of 1 July 2026;
   c) to other employees of the University no later than as of 1 August 2026.
2. If an employee is employed at multiple workplaces within the University, the rules under Art. 5 apply to the employee as of the date on which they apply to the workplace which first applies these rules.

Article 23

Effect

This Rector’s directive comes into force on 20 May 2026 and becomes effective on 1 June 2026.

Prague, 20 May 2026

prof. RNDr. Jiří Zima, CSc.
Rector