Tomas Bata University in Zlín

Cybersecurity

Basic training

Security
starts with (TB)U!

Table of contents

1. Introduction to Cyber Security

Cyber security protects our data, privacy and finances. Cyber-attacks do not only target companies and institutions – everyday users are also at risk. Just one careless click can compromise sensitive information or allow unauthorized access to systems.

According to current statistics, the number of cyber-attacks is increasing every year. The most common threats include phishing emails, ransomware attacks, and the exploitation of weak passwords. Real-life examples include companies losing data and operational capacity, or individuals having their bank accounts emptied by attackers.

Cyber security is therefore not just the responsibility of the IT department – it concerns every user. By following a few basic rules, the risk of an attack can be significantly reduced.

For more information about cyber security at Tomas Bata University in Zlín, please visit the website of the Information Technology Centre: www.utb.cz/kyberneticka-bezpecnost/zaklady-kyberneticke-bezpecnosti/.

The TBU computer network operating rules are available at www.utb.cz/cvt/net-utb-rules/.

2. Safe User Behaviour

Safe user behaviour is a key element in protecting information, systems and devices within an organisation. Everyday activities such as password management, handling emails, browsing websites or sharing information on social media can pose potential risks if not carried out with cybersecurity best practices in mind.

This part of the training focuses on practical guidelines and principles that will help you minimise risks and protect not only your organisation's sensitive data, but also your own personal information. You will learn how to create and manage strong passwords, recognise phishing emails, use web services securely, and share personal data responsibly.

Adhering to these principles is the foundation of responsible and safe behaviour in the digital environment.

2.1. Password management

Secure passwords

A strong password should be at least 12 characters long and include a mix of uppercase and lowercase letters, numbers and special symbols. Avoid predictable patterns (e.g. capital letter at the beginning, number at the end). Nowadays, password length is considered the most important factor for security.

Passphrases

Passphrases are easier to remember and consist of a phrase or sentence, with characters selected according to a chosen pattern. They offer higher security while remaining user-friendly.

Password managers

A password manager is an application that can generate, securely store, manage and autofill your passwords. This eliminates the need to write down or memorise every password. Users only need to remember one "master" password. Although many people do so, it is generally recommended not to store access credentials for email or online banking in password managers.

Two-factor authentication (2FA/MFA)

Two-factor authentication is an effective safeguard in case someone obtains your password. In addition to your password, a second factor (such as a code from a mobile app like Authenticator) is required. This means an attacker needs access to both your password and your phone. Enabling two-factor authentication significantly reduces the risk of account compromise.

Password practices

Never share your passwords, write them down on sticky notes, attach them to your monitor, or send them via email or chat. Use a unique password for each account to ensure that a breach in one service does not compromise others. Always log out when using public or shared computers and avoid saving passwords in browsers. If you suspect that your account has been compromised, change your password immediately. Safe password usage is just as important as having a strong password.

Screen lock

Always lock your screen when stepping away from your device to prevent misuse of open accounts. On Windows, you can quickly lock your screen using the shortcut Win + L. Be cautious of “shoulder surfing” – someone watching you type your password, especially in public spaces. If you work outside of the office, protect your screen from prying eyes – ideally using a privacy filter.

2.2. Email safety principles

Recognising scams

Always double-check the sender’s email address – sometimes a single altered character is enough to redirect your response to a malicious actor. When in doubt, call your colleague or superior directly using a phone number you already know, and verify the message content.

Checking attachments

Email attachments can contain malware or viruses. Never click on unknown attachments. If an attachment is not anticipated, verify the sender before opening it. Use antivirus software that scans attachments before opening them.

Links and URLs

Phishing links often lead to fake websites designed to steal your login credentials.

Never click on anything in suspicious emails. If a message claims you have won a prize, says your account is blocked (especially for a service you have never used), or threatens that your personal data will be leaked unless you pay via a Bitcoin wallet – do not believe it and never pay. These messages are fraudulent, even if they appear convincing.

Useful tips and advice: Hover your mouse over a link to check the actual address before clicking. Avoid clicking on links in suspicious emails – instead, go directly to the official website. Never enter your password on a website you have opened via a link in an email.

General guidelines

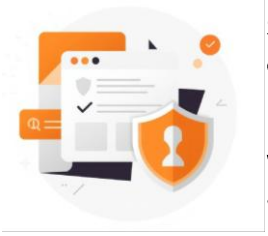
- If unsure, verify the content of the email via a phone call or a different communication method.
- Never send sensitive data in the body of an email – use encrypted attachments instead.
- Keep your email client and antivirus software up to date.

2.3. Safe web browsing

Using the web

Today, most online activities – such as email, video streaming, music or online banking – are carried out directly in a web browser. All that is needed is an internet connection and a valid web address. Some services require users to log in and verify their identity.

HTTPS and website certificates



Secure communication is encrypted using the HTTPS protocol. Certificates are issued by trusted certificate authorities and confirm that you are communicating with the intended server.

Modern browsers automatically check the validity of website certificates and alert you if something is wrong – for example, an expired certificate or unsecured login over plain HTTP. If you see such a warning, it is safest not to proceed to the site.

Verifying information sources

When browsing the internet, it is important to verify the credibility of the information you encounter. Not all websites and articles are reliable. When evaluating sources, consider the following:

- **Website trustworthiness** – look for reputable organisations, established news outlets, or official institutions.
- **Author and contact details** – check who created the content and whether they can be contacted.
- **Date of publication** – some information becomes outdated quickly.
- **References and citations** – reliable sources provide verifiable links and references to support their claims.

Never share or rely on information from questionable websites, especially when it involves financial transactions or sensitive data. Use critical thinking and cross-check information with multiple reputable sources.

Summary

- The web consists of servers, your browser acts as the client.
- Each URL specifies the content and the server delivering it.
- Always transmit sensitive data over HTTPS.
- Website certificates verify the server's identity.
- Pay attention to browser warnings – they help you identify suspicious sites.

2.4. Sharing personal data and social media use

Most of us use social media to share moments from our personal or professional lives. However, from an attacker's perspective, this can be a valuable source of information used in social engineering attacks. Always consider your privacy when posting online and be mindful of what you share. This includes: Your full name, date of birth, addresses and contact details, photos and videos, information about your job, school, hobbies, your online activity (comments, likes, followed pages or groups).

An attacker may steal your identity by creating a fake profile and contacting your friends or colleagues to extract further information. Stolen accounts can be used to:

- Spread malicious links and messages
- Conduct disinformation campaigns
- Build a password dictionary (for "dictionary attacks") using publicly available personal details

Other common social media tricks

Security questions: Answers to common password recovery questions (like mother's maiden name) are often easy to find on social media.

Fake surveys and competitions: These are used by attackers to collect personal data, sometimes including your answers to security questions.

Stay vigilant when sharing personal data online. Regularly review your privacy settings, limit the visibility of sensitive content, and avoid disclosing details that could be exploited.

3. Device Protection

The devices we use for both work and personal life – computers, laptops, tablets and mobile phones – serve as primary gateways to the digital environment. Proper protection of these devices is essential for safeguarding data, maintaining privacy and minimising the risk of cyber-attacks.

This section of the training focuses on the principles and tools that help protect devices from malware, unauthorized access and misuse. You will learn how to use antivirus software and firewalls effectively, why it is important to keep systems and applications up to date, and how to secure mobile devices using PINs, biometrics or data encryption.

Diligent device protection is a cornerstone of safe working practices in the digital world and significantly reduces the risk of data loss or compromise.

3.1. Antivirus software and firewalls

Our devices are protected by various security tools that monitor both incoming and outgoing traffic and detect suspicious activity. The most essential of these are **antivirus software and firewalls**.

Think **of antivirus software** as an internal guard – it continuously scans your system for dangerous files, malware and viruses, and works to block them. It uses a regularly updated threat library to respond effectively to the latest attacks. While the core protective function is the same across all antivirus tools, different products may offer additional features.

A **firewall** acts like a castle gate – it monitors which internet requests are allowed to enter or leave your device. It prevents unauthorized access and protects your system from external attacks. Note that a firewall is not the same as antivirus software – it provides complementary protection and should never be disabled, even on home computers.

Properly configured security tools significantly reduce the risk of attack and are a key component of data and device protection.

3.2. System and application updates

Regular updates of your operating system and applications are a key element of cyber security. Updates fix security vulnerabilities, improve system stability, and protect against newly emerging threats.

Failing to install updates can allow attackers to exploit known weaknesses in the system or software to gain access to your device. Most modern systems support automatic updates, which greatly simplifies the process of staying secure.

Recommendations for safe update practices:

- Enable automatic updates wherever possible.
- Install updates as soon as they are released – especially critical security patches.
- Regularly check applications that do not update automatically and download updates only from trusted sources.
- If you are unsure about updating your system, contact the IT administrator at your component part.

Keeping your system up to date is a simple but powerful way to protect your device from attacks and data loss.

3.3. Mobile device security

Mobile devices are always often with us and contain sensitive personal and work-related data, making their protection crucial.

Screen lock

Your device should always be secured with a screen lock.

Traditional methods: A PIN (at least 6 digits, avoiding simple or predictable combinations) or a pattern. Note: Patterns are easier to observe and generally less secure.

Modern methods: Fingerprint or facial recognition. These technologies are reliable, but their effectiveness also depends on the strength of your backup PIN or pattern.

Data protection

- SIM card – It should be protected with a PIN code to prevent misuse if the phone is lost or stolen.
- Memory cards – Ideally encrypted. Sensitive data should not be stored on unencrypted external storage.
- Backups – Regularly back up your contacts, photos, and other important data to avoid loss in case of theft or device failure.

Geolocation

Mobile devices often use GPS or other location services. Be cautious when granting apps access to your location, especially if data might be shared publicly.

Two-factor authentication

Mobile authenticators (e.g. Microsoft Authenticator) generate codes used together a with your password. To ensure their security, your phone should be protected with a strong PIN or biometric lock — otherwise, an attacker who obtains your device could abuse the authenticator.

4. Threats and Attacks

The digital environment is full of risks and potential attacks that can compromise your devices, data or privacy. These threats may originate from external sources – such as cybercriminals – but can also stem from internal vulnerabilities, especially if safe behaviour principles are not followed.

In this part of the training, you will be introduced to the most common types of cyberattacks encountered today. You will learn how to identify fraudulent emails, SMS messages or enticing attachments, which are often used in phishing, spear phishing, baiting or smishing campaigns. We will also explain how malicious files and ransomware can damage your devices or block access to your data, and how to protect yourself from password attacks, including brute-force methods and keyloggers.

Understanding these threats is the first step towards actively protecting your devices, accounts and sensitive information.

4.1. Social engineering - phishing, spear-phishing, baiting and smishing

Phishing

A social engineering attack aimed at obtaining confidential information, such as login credentials. The attacker poses as a trusted email sender – for example, a notification about a full mailbox or a required account update. The stolen data can then be misused for further attacks.

How to recognise phishing:

- Suspicious or misspelled sender address, or unusual domain (.ru instead of .cz).
- Poor grammar or translation errors.
- Links directing you away from known websites.
- Urgency to act quickly or use of familiar branding to appear legitimate.

Vishing

Vishing (voice phishing) is a scam involving fraudulent phone calls using social engineering techniques. Attackers impersonate bank employees, government officials or the police to extract sensitive information or convince victims to transfer money. These calls often rely on creating a sense of fear and urgency.

How to recognise vishing:

- Suspicious phone numbers (short, unfamiliar area codes) — though numbers may also be spoofed.
- The caller remains vague and uses general information and a false identity to extract real data.
- Sense of urgency — pressure to respond immediately (e.g. threat of losing savings).
- Request for sensitive information (passwords, card numbers, ID details).

Spear-phishing

Spear phishing is a targeted form of phishing aimed at a specific individual or organisation. Attackers gather personal or professional information about the victim (e.g. role, interests, contacts) to make their messages appear more credible. Identifying such emails requires increased vigilance, even if the sender seems familiar.

How to recognise spear-phishing:

- Unusual requests from known contacts – even a colleague's email may be spoofed.
- Personalised content – the attacker may know your name, job title, projects or interests.
- Pressure to act quickly – urging immediate link clicks or disclosure of information.
- Links and attachments – may contain hidden URLs or malicious files, even if they appear legitimate.
- Inconsistencies with internal procedures – such as requests for sensitive data through unofficial channels.

Baiting

A technique exploiting curiosity — for example, a USB stick labelled "Employee Rewards". Connecting such a device may automatically launch malicious software. Baiting can also occur digitally, such as through "free" downloads of music or software.

How to recognise baiting:

- Suspicious external media – USB drives, CDs or memory cards found in hallways, meeting rooms or public places.
- Tempting labels – documents titled "Salary Plan" or "Confidential Internal Information".
- Unknown source – media or files from unknown or unauthorised individuals.

Smishing

Phishing via SMS messages, often containing links to fraudulent websites or requesting calls to fake numbers.

General guidelines for protection against phishing, vishing, spear-phishing, smishing and baiting:

- Never click on suspicious links or share personal or confidential information.
- Verify the sender and contact known institutions through official channels.
- Report suspicious messages to your IT department.
- Do not connect unknown USB devices or other external media (see Baiting above).

4.2. Malicious files and ransomware

Malicious files

Malicious files are programs or documents that, once opened, can damage your device, steal data or install unwanted software. The most common types include:

- Executable files (.exe, .bat, .msi) – can install harmful programs.
- Compressed archives (.zip, .rar) – may hide executable files.
- Office documents with macros (.docm, .xlsm, .pptm) – contain automated scripts that can download and run malicious content.

These files are often spread via email, external media (such as USB drives or CDs), or downloads from untrusted websites. Attackers frequently disguise them as legitimate documents like invoices or reports.

Ransomware

Ransomware is a type of malicious software that encrypts your files or entire system, making them inaccessible. Attackers then demand a ransom in exchange for decryption. It is most spread through email attachments, infected files or USB drives.

Recommended prevention measures

- Do not open suspicious attachments or download files from untrusted sources.
- Only enable macros in verified, trusted documents.
- Regularly back up important data to a location separate from your main device.
- Keep your antivirus software and operating system up to date.
- If infected with ransomware, immediately disconnect the device from the network.
- It is generally not recommended to pay the ransom – it encourages further attacks and does not guarantee data recovery.

4.3. Password attacks (brute force, keyloggers)

Passwords are a fundamental element in protecting our accounts and data. Attackers use various methods to try to obtain them to gain access to sensitive information, ranging from emails to bank accounts.

Brute force attacks

A brute force attack involves systematically trying every possible combination of characters until the correct password is found. The effectiveness of this method depends on the length and complexity of the password – the longer and more random it is, the harder it becomes to crack.

Keyloggers

A keylogger is a malicious programme or device that monitors and records keystrokes. This enables attackers to capture login credentials without needing to crack the password using brute force. Keyloggers are often spread via infected files, email attachments, or compromised websites.

Dictionary attacks

Dictionary attacks rely on lists of commonly used passwords and words from natural language. The attacker's software goes through these options one by one. This method is faster than pure brute force but is only effective against weak or common passwords.

Social engineering attacks

Attackers often try to trick users into revealing their passwords voluntarily – for example, through phishing emails, fake websites, or phone calls (known as "vishing"). These techniques can be highly effective because they bypass technical security measures and exploit human error or carelessness.

Prevention:

- Use strong, random, and unique passwords for each account.
- Enable two-factor authentication (2FA), which requires a second independent factor in addition to the password.
- Never reuse passwords across different websites.
- Be cautious of suspicious emails, links and attachments – they may contain keyloggers or lead to phishing sites.
- Change your passwords regularly and use a password manager to store them securely.

5. Legal and Organizational Framework

Cybersecurity is not only a matter of technology and user habits – it is also governed by legal regulations and organisational policies. These frameworks define the responsibilities of both individuals and organisations, setting out how data, systems and information must be handled to avoid breaching the law or internal rules.

In this section of the training, you will be introduced to key legal standards, including both Czech and European legislation, with a particular focus on the Cybersecurity Act, which outlines obligations for protecting information systems. We will also explore the importance of internal security policies and guidelines implemented by organisations to ensure data protection and the secure operation of IT systems.

Understanding the legal and organisational framework will help you act in compliance with regulations and minimise the risks associated with improper or careless handling of information.

5.1. Legislation

In the Czech legal system, the Constitution represents the highest legal authority, followed by other laws and regulations. These legal norms define the boundaries within which we must operate and crossing them may lead to legal consequences. The internet must not be regarded as a "lawless space" – the same legal principles that apply in the physical world also apply in cyberspace. For example, fraud committed online is just as criminal as fraud committed offline. Moreover, due to the digital footprints left behind, it is often possible to identify and prosecute cybercriminals.

In the Czech Republic – as in all European Union member states – cybersecurity is governed not only by national legislation but also by international and European directives. One of the key European instruments is the NIS Directive (Network and Information Security Directive), which sets out basic requirements for the security of networks and information systems. The NIS Directive obliges member states to develop national cybersecurity strategies, ensure coordination between public authorities, and implement mechanisms for reporting security incidents by providers of essential and digital services.

5.2. Cybersecurity Act

In the Czech Republic, cybersecurity is mainly governed by Act No. 264/2025 Coll., on Cybersecurity, which has applied since 1 November 2025. The law covers organisations that provide important or essential services, for example in energy, transport, healthcare or digital services. Depending on their importance, they must follow either a higher or lower set of security duties. These duties include protecting systems, managing risks, reporting serious incidents to NÚKIB and making sure management takes responsibility.

The details are set out in implementing regulations. Decree No. 408/2025 Coll. says which services are covered. Decrees Nos. 409/2025 and 410/2025 Coll. describe the security measures for the higher and lower regimes. These include access control, backups, supplier checks, incident handling and recovery plans. Together, these rules help organisations reduce cyber risks and respond when an incident happens.

5.3. Internal security policies

Our university has established its own internal security policies, which define the rules and responsibilities of employees when working with information systems and data.

These policies and directives cover areas such as:

- User access rights and authentication.
- Use of university devices and network resources.
- Rules for data backup and retention.
- Procedures for reporting security incidents.
- Measures to prevent data leaks and misuse of sensitive information.

The directives provide specific instructions within each area and establish mandatory employee behaviour to minimise the risk of cyber threats. Failure to comply with these rules may result in disciplinary action, including restricted access to systems, workplace sanctions, or other measures in accordance with employment regulations.

Internal policies and directives complement the legislative framework, such as the Cybersecurity Act, and ensure that the university can effectively implement security measures and enforce compliance across all staff members.

The cybersecurity policies issued by TBU are available at the following link:
https://www.utb.cz/univerzita/o-univerzite/struktura/poradni-sbory/vybor-pro-rizeni-kyberneticke-bezpecnosti/vydane-politiky/

6. Incident Response

Cyber incidents can affect any user and organization – from data loss to malware attacks to attempts to disrupt the system. The key is a quick and correct response that minimizes damage and allows for the restoration of safe operation.

In this part of the training, you will learn how to recognize incidents, what first steps to take when an attack is suspected, and who to report a security problem to. Understanding these procedures is essential for protecting data, devices, and information systems.

The goal is to teach you to react in a timely manner, proceed correctly, and cooperate with responsible individuals or departments in the organization so that each incident is handled effectively and safely.

6.1. How to recognise a cybersecurity incident

A cybersecurity incident is any unwanted event that threatens the integrity, availability or confidentiality of an organisation's information or systems. The key first step is timely detection – the sooner an incident is identified, the less damage it is likely to cause.

Possible signs of an incident include:

- Unusual system behaviour – computers, servers or applications fail to start, slow down, freeze or restart without an apparent reason.
- Unauthorised access – alerts about logins from unknown devices, unusual geographic locations, or outside of working hours; or an inability to log into applications or accounts.
- Suspicious communication – unexpected emails with links or attachments, often urging immediate action.
- File or data changes – unexpected deletion, encryption, or movement of files not initiated by users.
- Security tool alerts – antivirus software, firewalls, or intrusion detection systems reporting suspicious activity.
- Unusual network activity – sudden spikes in incoming or outgoing traffic or attempts to connect to unknown servers.

6.2. Initial steps when suspecting an attack

If a user notice signs of a potential cybersecurity incident, it is crucial to act quickly but systematically. Taking the right steps can significantly reduce damage and shorten system recovery time.

(1) Stay calm and avoid interfering with the system

Do not panic or attempt unqualified interventions. Actions such as deleting files, trying to "fix" the system, or interacting with suspicious emails may worsen the situation. They can also destroy important evidence needed for investigation.

(2) Disconnect the device if possible

If you suspect that your computer or mobile device has been compromised, disconnect it from the internet, any external storage devices and the power supply. This helps prevent the potential spread of malicious software.

(3) Record suspicious activity

Carefully document all suspicious events, including:

- The time and location of the incident.
- A description of system or network behaviour.
- Suspicious emails, links or attachments.
- Any actions you have taken.

(4) Immediately notify your IT or the Information Technology Centre of TBU

Contact the personnel in charge at TBU and provide them with all recorded information. Do not delay – a fast response can significantly limit the impact of the incident.

6.3. Who to report a security issue to

If you encounter a security problem, attack, or suspicious activity, it is important to know whom to contact. Prompt and accurate reporting can prevent more serious damage and protect both your data and that of the entire institution.

Inform the IT administrator at the relevant component part or the Information Technology Centre about the specific issue, including what happened and when.

Do not attempt to resolve the problem yourself – incorrect actions could make the situation worse.

What to include when reporting:

- A description of the security incident.
- The type of incident (if you can identify it).
- Specify the affected system (e.g., website, computer, server), including the operating system used.
- Identify the device or service involved (domain name, IP address, MAC address, port).
- If possible, attach supporting evidence such as the original suspicious email with full headers, screenshots, links to fraudulent or infected websites, logs from firewalls, antivirus software, etc.

Never neglect reporting suspicious activity. Even minor incidents can be part of a larger attack, and your report helps protect the institution.

The preferred method of reporting is via email to the Helpdesk of the Information Technology Centre: **abuse@utb.cz**.

7. Advanced Topics

In this part of the training, we will explore modern approaches and tools that enhance the security of working with digital devices and data. We will examine the principles of Zero Trust, which challenge traditional notions of trust within a network and help to minimise the risk of unauthorised access. We will also look at the use of VPNs (Virtual Private Networks) for remote work, ensuring secure communication even outside the university network. Another essential topic is data backup, a critical step in protecting important information from loss or damage. These advanced practices help safeguard sensitive data and promote a responsible approach to cybersecurity, especially in academic and research environments.

7.1. Zero trust principles

Zero Trust is a modern security approach based on a simple principle: **"Never trust, always verify."** Unlike traditional security models that consider internal networks to be secure by default, Zero Trust assumes that even internal users or devices may pose a threat.

What it means for users:

- Authentication is always required – login and access to systems are verified not only when joining the network, but also continuously with every action.
- Strong passwords and two-factor authentication (2FA) – your credentials must always be securely protected.
- Least privilege access – users only have access to the data and applications they genuinely need for their role.
- Device compliance – your device must meet security standards, such as having an up-to-date operating system and antivirus software.

How Zero Trust improves security:

- It limits the lateral movement of attackers within the institution/organisation.
- It reduces the risk of compromised accounts being misused.
- It provides better visibility and control over who does what with systems and data.

For users, the key is to: Follow security policies, keep your device updated and never share your login credentials. Zero Trust is not just a technology – it is a mindset. It is about thinking securely every single day.

7.2. Zero trust principles

Remote work has become a common part of modern working life, making secure access to organisational systems essential. A VPN (Virtual Private Network) is one of the key tools used to protect data when connecting from outside the organisation.

What a VPN does:

- Encrypts internet traffic between your device and the corporate network, preventing attackers from easily intercepting your data.
- Masks your real IP address and can help prevent unauthorised access.
- Enables secure access to internal systems even from public Wi-Fi networks – for example, in cafés or airports.

Recommended best practices for users:

- Always use a VPN when connecting from outside the university network.
- Do not disable encryption or certificate checks – these are critical to secure communication.
- Never use public Wi-Fi without a VPN – public networks are a common source of eavesdropping and "man-in-the-middle" attacks.
- Keep your VPN client up to date and follow the university's security policies.
- Avoid storing sensitive data on your personal device – whenever possible, work directly within the protected corporate environment via VPN.

VPNs are a fundamental security tool for remote work. Even when enjoying the comfort of working from home, it is crucial to follow secure connection practices to keep both corporate data and your personal information safe.

7.3. Data backup

In a professional environment, reliable data backup is one of the cornerstones of cyber security. University data is highly valuable but constantly at risk – from hardware failures and accidental deletion to malicious software (such as ransomware) or device theft. Backup is therefore one of the most important security measures.

Why backup?

- Disaster recovery – if your hardware fails, you can quickly restore your data.
- Protection against ransomware – even if an attacker encrypts your entire device, your data can be recovered from a backup.
- Human error – accidentally deleted files can be restored from the most recent backup.

How to backup properly?

- Regularly – backups should be performed consistently (e.g. daily or weekly).
- Separate from the device – a backup stored on the same machine as the original data is not effective.
- Avoid using public cloud services (e.g. Google Drive, Dropbox) – these are not under the university's control and may pose security risks.
- Test your backups – regularly check that your data can actually be restored when needed.

Practical tips for users:

- Use external drives or NAS (Network Attached Storage).
- Use designated storage systems – such as network drives approved by the university.
- Always save important work data to an additional location, not just your local machine.

It is the user's responsibility to store work-related data in designated locations specified by the university. This is the only way to ensure that the data can be securely backed up and restored in case of a problem.