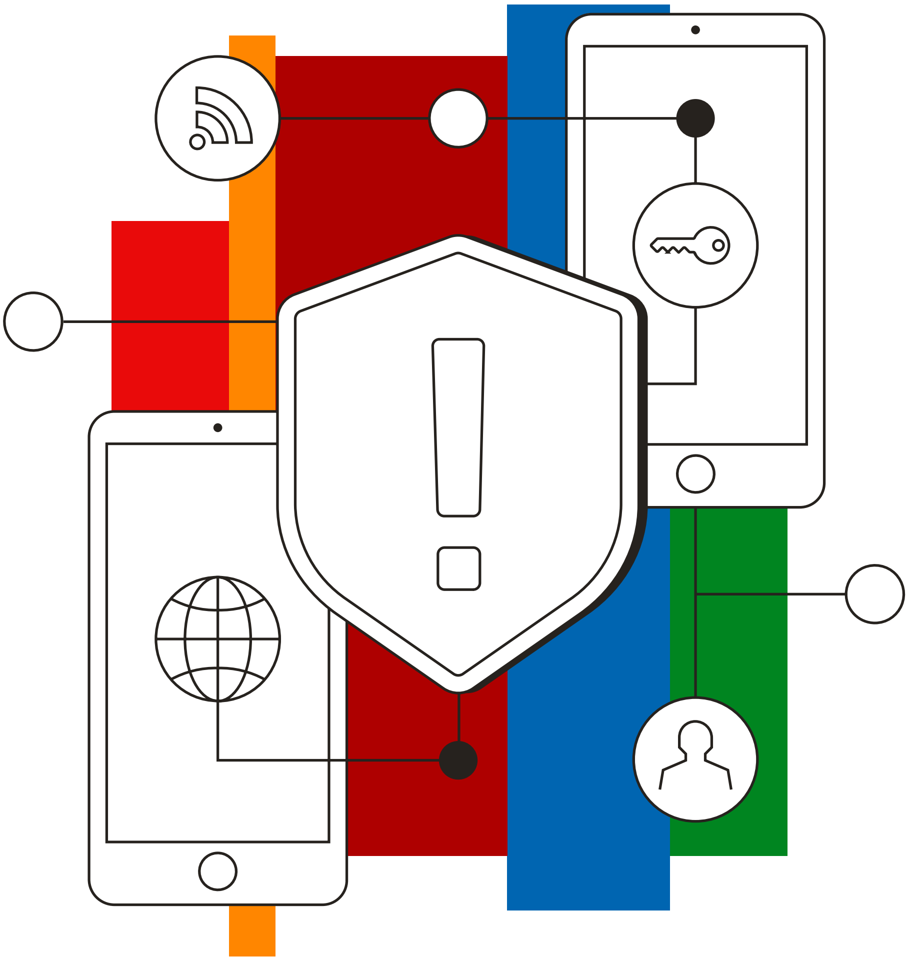

Good Security Practices

for Companies
prepared by mBank

Introduction

Cyber attacks pose a major challenge to companies' IT security.
They may lead to data leaks, compromise confidential information and cause IT system downtime.

Appropriate safeguards and security hygiene are therefore essential to protect against such incidents. They help you avoid serious legal and financial consequences, damage to reputation and loss of confidence among clients and business partners.

Stay safe – follow security guidelines!

most frequent causes of cyber attacks

phishing

Phishing involves scammers sending messages (e.g. emails, text messages) containing links to fake websites or dangerous attachments. This way they trick people into sharing their confidential details, e.g. the login and password to a bank account or personal data.

What you should keep in mind:

- always check senders' email addresses, e.g. for typos,
- if you are not sure whether a message is genuine, contact the sender using a different channel (e.g. by phone),
- pay attention to the format of attachments in a message – be extremely careful with files that have several extensions in their names (e.g. faktura_10.pdf.exe, przelew.pdf.zip, wyplata.jar.doc.), as they can easily infect your device with malware,
- before clicking a link provided in an email, hover your mouse over it to see where it leads and make sure that the URL address is correct.

malware

In order to mitigate the risk of malware infection:

- use only trusted sources – do not download software or apps from suspicious websites and always check the reputation of a source,
- before installing new software, scan it using an updated antivirus,
- regularly use an antivirus on your device to detect and remove any potential threats; regularly perform full system scans on your device and set up a scan schedule,
- use advanced solutions to protect your workstations; in addition to antivirus software, consider using Endpoint Protection software, which allows you to detect more advanced methods of infecting your computers,

unsecured network services

Secure network services:

- check if your devices are exposing unnecessary network services to the internet, such as Remote Desktop – if it is not absolutely necessary, restrict such exposure,
- make sure that the Wi-Fi network you are using is protected by a strong encryption algorithm and a strong password; do not share the network you are using for work with third parties,
- make sure that all connections to critical apps use secure protocols such as HTTPS, which provide encryption for data transmission, protecting it from eavesdropping and tampering.

exploitation of software vulnerabilities

- download apps and software from official stores only; do not download them from untrusted sources,
- always keep your device's operating system up to date in order to eliminate security vulnerabilities,
- keep abreast of information about the latest vulnerabilities and threats published by software producers and trusted industry sources; this will enable you to quickly react to potential threats,
- check if the software provided to you by external firms is secure; security vulnerabilities in such software may expose your network to ransomware.

USB devices

Use only devices from trusted sources:

- make sure that the USB devices you plug in to your computer or laptop come from trusted sources,
- scan the USB device before opening any file saved on it; use antivirus or Endpoint Protection software,
- disable the AutoPlay feature for files on your computer – this way, malicious software will not run automatically,
- do not leave your device unattended, especially in public places or where it can be accessed by unauthorised third parties,
- limit the use of pen drives and portable storage devices; consider if all employees of your company need to use them.

computer sharing

Sharing a computer may increase the risk level.
In order to prevent it:

- do not make your work devices accessible to your children or other family members,
- use separate devices for personal purposes.

use secure devices

Make sure that the devices (e.g. laptops, phones) used by you and your employees or associates to process confidential information are secure.

Use network devices with an active firewall system.	Configure your firewall so as to limit network traffic to the necessary minimum, which will reduce the risk of unauthorised access.
Regularly instal security patches.	Regularly update the operating system and software on your devices to protect them against the latest threats. The same applies to network edge devices such as firewalls, routers and VPN concentrators.
Limit user privileges	Restrict user privileges on devices to prevent users from changing configurations, installing or uninstalling software and running unauthorised software. Do not allow unauthorised exchange of data with other devices if the employee’s duties do not require it.
Lock devices automatically.	Set the operating system to automatically lock access after a maximum of 15 minutes of user inactivity. This will help prevent unauthorised access.
Secure remote access to the internal network using an encrypted VPN connection.	This adds another layer of security by concealing network traffic and making it more difficult for unauthorised third parties to access the network. Remember that VPN is only one of many layers of security; although it enhances privacy, it does not protect you against all threats.
Secure devices against theft and unauthorised interference.	
Enable event log.	This will allow you to clearly identify the users who made changes in IT systems.
Set individual access passwords.	Make sure that every device user has their own individual access password. Restrict access to systems and data to the minimum necessary to perform work.
Introduce strong password policies.	Make sure that passwords protecting devices are created in line with the best market practices. Use long (at least 12 characters) random passwords that are difficult to guess.
Do not allow account sharing.	Impose a ban on account sharing for your employees. This way you will prevent unauthorised access and ensure user accountability.

Make sure that the devices (e.g. laptops, phones) used by you and your employees or associates to process confidential information are secure.

Restrict access to network resources.	Restrict access to your network resources to specific devices or users only. This way you will minimise the risk of unauthorised access.
Restrict access to admin accounts.	Do not use admin accounts (also on workstations) for everyday work. Make sure that your employees use admin accounts only if it is necessary for task completion.
Disable built-in and unused accounts.	Disable accounts that are not used for work (e.g. guest accounts).
Two-factor authentication (2FA).	Enable two-factor authentication on accounts and services whenever possible. 2FA requires an additional identity verification step, which significantly hinders unauthorised third parties from taking over accounts. Use solutions provided by renowned providers to limit the risk of unauthorised access to processed information.
Use password managers.	They help you generate, store and use strong passwords. At the same time, however, remember to adequately protect access to the password manager.

create secure backups

Backups allow for quick data recovery if malicious software encrypts your devices.

Decide what needs to be secured.

Backups should cover the most important data or a full system image to enable quick restoration of full functionality if needed.

Create backups regularly.

This way you will reduce the risk of data loss. Think about how long your company can operate without the latest data. What would happen if you lost data from the past few days? On this basis, determine the optimal backup frequency.

Store backups on external media that are disconnected from the network, power supply and the main system.

This will allow you to minimise the risk of backups being infected with malware that may spread to all available drives and network resources. By isolating backups, you will secure access to a clean, uncorrupted data version.

Ensure secure access to backups.

Make sure that only authorised users have access to backups.

Regularly test backup recovery.

Regularly check if your backups are complete and can be recovered without issues. This way you will ensure that your backups are useful in crisis situations.

Encrypt your backups.

Backup encryption will protect your data in case the device or medium containing this data is stolen. Store the recovery key in a safe place that is independent from the encrypted device and the external resources containing backups.

protect confidential information

The security of your company's confidential information depends largely on the people working in the company. Make sure that your employees and associates know how to protect such information.

Ensure formal protection of confidential information.

Introduce an internal regulation setting out the key principles of secure processing of confidential data.

Make it clear in the regulation:

- which information is considered confidential, how to handle it and how to protect it,
- where to dispose of paper documents, to whom they can be handed over and how to handle them during remote work or while traveling.

Introduce a written confidentiality statement.

Protect the confidentiality of your information processed by employees and associates. Oblige them to submit a confidentiality statement. This can take the form of a separate statement or a provision in the agreement signed with an employee or associate. This way you will make sure that anyone who processes confidential information is aware of this fact.

Foster awareness among your employees and associates.

Ensure that the persons processing confidential information in your organisation know how to do it right. Organise regular training to remind your employees about the key principles, e.g. how to handle confidential information, who to share it with, how to protect such information if it needs to be sent outside the company and things to be cautious about (e.g. links and attachments in emails, installing software from unknown sources). Consider ending the training with a short knowledge test.

Introduce an incident management procedure.

Introduce an internal regulation explaining how to deal with security incidents.

Make it clear in the regulation:

- what is considered an incident in your organisation,
- where and how to report an incident,
- who is responsible for handling an incident and what measures should be taken,
- who in the company should be regularly informed about incidents.

Introduce a vulnerability management procedure.

Introduce an internal regulation explaining how vulnerabilities should be dealt with in your ICT environment.

Make it clear in the regulation:

- how to classify vulnerabilities,
- by when vulnerabilities must be resolved,
- where and how to report vulnerabilities,
- who coordinates the vulnerability resolution process,
- who in the company should be regularly informed about unresolved vulnerabilities.

use secure software

Apply the latest best practices for secure software development. Always follow security principles, regardless of whether you develop software in-house or buy it from an external provider.

Address architecture security. Use software developed in line with confidential information protection principles:

- **secure by design** – designing a system in a way that incorporates the security requirements already at the design stage to address risks the system could pose to information processed in it if those requirements were not implemented,
- **defence in depth** – designing multiple layers of security controls throughout a system to protect information processed in it,
- **secure by default** – incorporating appropriate protection of confidential information into the structure of a designed system in such a way that the system enforces it by default, without any additional actions,
- **default deny** – denying access by default – access must be granted knowingly, openly and be accounted for,
- **fail secure** – designing a system so that, in the event of a failure or error, it automatically transitions into a state that prevents any compromise of its security (e.g. by blocking access to information),
- **zero trust** – an approach assuming that no component, device or network can be trusted, regardless of whether it is located inside or outside the organisation.

Observe the best practices for secure coding

(e.g. the OWASP Top 10 Proactive Controls).

Protect personal data. Implement solutions based on the following principles:

- **privacy by design** – designing a system in a way that incorporates privacy considerations already at the design stage,
- **privacy by default** – incorporating appropriate privacy considerations into the structure of a designed system in such a way that the system enforces it by default, without any additional actions,

Avoid using immature or obsolete/unsupported technologies.

Test software before deploying it to your production environment and when introducing major changes.

Check software not only in terms of its functionality and performance, but most of all in terms of its security (pentesting).

ensure physical security

Prevent unauthorised third parties from entering your premises or causing damage (e.g. stealing confidential documents).

Implement access control.	Introduce, for example, electronic access cards to rooms where your company processes confidential or high-value business information. Control access to rooms with IT equipment (e.g. laptops, printers, servers). This will enable you to monitor who enters individual rooms and the time at which access occurred.
Monitor guest traffic.	Register individuals from outside your company who visit your premises. In particular, this applies to guests who have access to rooms with office equipment or where confidential documents are stored. Such individuals should be accompanied by an employee of your company at all times when on the company's premises.
Consider installing video surveillance.	Think about installing a video surveillance system in rooms where your company processes confidential or high-value business information. Consider placing surveillance cameras also in rooms with IT equipment (e.g. laptops, printers, servers).
Protect documents.	If employees and associates in your company use paper documents, make sure that they secure them properly after they finish work (e.g. by retrieving documents from printers and desks and storing them in locked cabinets or safes). This way you will prevent unauthorised persons (e.g. the cleaning staff) from accessing these documents.

This document is for informational purposes only. It sets out general security guidelines and good practices for companies developed to raise awareness and encourage essential prevention efforts. This document is not a comprehensive manual or a guarantee of security; its application does not release a company from the obligation to independently analyse risks, align its safeguards to the specific nature of the company's business and to use professional advisory services. mBank S.A. is not liable for any damage resulting from the observance or non-observance of the guidelines set out in this document.