ME/PSO

HANDBOOK

Information Security Handbook

Fundamentals, principles and everyday practices for protecting information

Companion material for the training course:
“Raising Information Security Awareness”

Document No. MEPSO-PRI-IB-001 · Classification: Internal Use
Information and Cyber Security Department · MEPSO AD Skopje

Contents

1. Introduction

Information is one of the most valuable assets of any organization. At MEPSO, as an operator of critical infrastructure, protecting information is not merely a technical matter — it is the responsibility of every employee.

This handbook explains the fundamental concepts of information security in an accessible way and offers practical guidance you can apply every day. The goal is not to turn you into an expert, but to give you the knowledge and awareness to recognize risks and act safely.

Every day we work with sensitive data — operational data about the electricity transmission system, personal data of employees, business information and technical documentation. Compromising this information can cause serious consequences: from financial damage and disruption of operations to endangering the security of critical infrastructure.

> **Why this matters to you.** Most security incidents do not happen because of sophisticated technical attacks, but because of simple human errors — a weak password, clicking a suspicious link, or leaving a computer unlocked. That is exactly why your awareness is the first and most important line of defense.

2. What is information security

Information security is the practice of protecting information from unauthorized access, use, disclosure, disruption, modification or destruction. It covers not only digital data, but also information on paper, verbal communication and the knowledge held by employees.

2.1 Types of information we protect

- **Operational data** — information about the state and control of the electricity transmission system;
- **Personal data** — information about employees, associates and third parties;
- **Business information** — contracts, financial data, strategic plans;
- **Technical documentation** — diagrams, configurations, security procedures;
- **Access credentials** — passwords, keys, certificates.

2.2 What we protect it from

Threats can come from various sources:

Threat source	Example
External attackers	Hackers, organized cybercrime groups
Malicious software	Viruses, ransomware, spyware
Insider threats	Disgruntled or careless employees
Human error	Accidental deletion, sending data to the wrong recipient
Physical threats	Theft of devices, unauthorized access to premises
Natural disasters	Fire, flood, power outage

3. Principles: confidentiality, integrity, availability

Information security rests on three fundamental principles, known as the “CIA triad” (Confidentiality, Integrity, Availability).

3.1 Confidentiality

Information is accessible only to those who are authorized to access it. This is achieved through access control, encryption and the principle of least privilege — each user receives only the rights necessary for their work.

> **Example.** Financial reports should be accessible only to the finance department and management, not to all employees. If everyone has access to everything, the risk of misuse or leakage grows dramatically.

3.2 Integrity

The accuracy and completeness of information are protected from unauthorized or accidental modification. Every change to critical data must be recorded and traceable, so that we can trust that the information is accurate and unaltered.

> **Example.** If someone modifies the configuration parameters of a system without authorization, it can cause the system to malfunction. Integrity mechanisms (logging, checksums, versioning) allow us to detect and roll back such a change.

3.3 Availability

Information and systems are available to authorized users when needed. This is ensured through backups, business continuity plans, redundant systems and protection against attacks aimed at denying access.

> **Balance.** The three principles are sometimes in tension — overly strict control (confidentiality) can reduce availability. The goal is to strike the right balance according to the importance of the information.

4. Information classification

Not all information is equally sensitive. Classification helps us know how to handle each type of information.

Level	Description	Example
Public	May be freely published	Press releases, public reports
Internal use	Employees only	Internal procedures, organizational charts
Confidential	Restricted circle of people	Contracts, financial data
Strictly confidential	Most strictly protected	Security configurations, strategic plans

4.1 Handling rules

- ✓ Label documents according to their classification level
- ✓ Do not share confidential information over unprotected channels
- ✓ Dispose of sensitive documents securely (not in a regular waste bin)
- ✓ When in doubt about the level, treat the information as higher classified

5. Password management

Passwords are the keys to the digital world. A weak password is like leaving your door unlocked — an invitation for unauthorized access.

5.1 Characteristics of a strong password

- ✓ At least 12 characters — the longer, the more secure
- ✓ A mix of upper and lower case letters, numbers and symbols
- ✓ No personal details (name, date of birth, pet's name)
- ✓ No common words or predictable sequences (123456, password)
- ✓ Unique for every account — do not reuse the same password

5.2 The passphrase technique

> **Tip.** Instead of a hard-to-remember string, use a phrase only you know and replace some letters with symbols. For example, a sentence that means something to you personally, turned into a combination of letters, numbers and symbols — long, complex, yet easy to remember.

5.3 Common mistakes

Do	Avoid
Use a password manager	Writing passwords on a note at your desk
A different password for every account	The same password everywhere
Change it when compromise is suspected	Sharing it with colleagues
Enable two-factor authentication	Sending passwords by email

6. Two-factor authentication

Even the strongest password can be compromised. Two-factor authentication (2FA) adds a second layer of protection — in addition to something you know (a password), it requires something you have (a code from your phone, an app or a physical key).

6.1 How it works

When you log in, after entering your password, the system asks for additional confirmation — most often a code generated on your phone. Even if someone learns your password, they cannot get in without the second factor.

> **Recommendation.** Whenever it is available, enable two-factor authentication — especially for business accounts, email and administrative access to systems.

7. Protecting your workstation

Your computer is the gateway to the organization's information. Protecting it is your daily responsibility.

7.1 Daily habits

- ✓ Lock your screen whenever you step away (even briefly)
- ✓ Do not install unapproved software
- ✓ Regularly update the operating system and applications
- ✓ Do not disable security software (antivirus, firewall)
- ✓ Do not plug in unknown USB devices

> **Warning.** USB devices are a common way of spreading malware. A USB stick found in the parking lot or given to you by a stranger — never plug it into your work computer.

8. Security when working remotely

Working from home or on a business trip brings additional risks. The same rules apply, but with greater care.

- ✓ Back up important data
- ✓ Access internal systems only through VPN
- ✓ Use a trusted internet connection; avoid open public Wi-Fi
- ✓ Do not leave your device unattended in public places
- ✓ Be aware of who can see your screen (shoulder surfing)
- ✓ Keep work and personal devices separate where possible

9. Physical security

Information security is not only digital. Physical access to premises, devices and documents is just as important.

- ✓ Carry your ID badge and do not lend it to anyone
- ✓ Do not let unknown people follow you in through the door (tailgating)
- ✓ Keep sensitive documents locked away
- ✓ Apply a “clean desk” policy — do not leave confidential documents in plain sight
- ✓ Report unknown persons in protected areas

10. Incident management

No matter how careful we are, incidents happen. What matters is knowing how to respond.

10.1 What is an incident

Any event that could endanger the security of information — a suspicious email, a lost device, a compromised password, unusual system behavior.

10.2 How to respond

1. Do not panic — a quick, calm reaction is key
2. Do not try to “fix” the problem yourself
3. Immediately report to the Information Security Department
4. Document what you noticed and what you did
5. Cooperate with the security team

> **Reporting is not a punishment.** Reporting an incident promptly is responsible behavior that protects the entire company. It is better to report a false alarm than to miss a real attack.

11. Employee responsibilities

Every employee has a role in protecting information:

- ✓ Following security policies and procedures
- ✓ Protecting access credentials (passwords, badges)
- ✓ Reporting suspicious activities and incidents
- ✓ Participating in security awareness training
- ✓ Handling sensitive information with care
- ✓ Notifying when changing job position or leaving the company

Practical scenarios

The best way to learn security is through real situations. Review the following scenarios and think about how you would act.

Scenario 1: A suspicious email

You receive an email that appears to be from the IT Department, urgently asking you to confirm your password via a link, otherwise your account will be blocked within 24 hours.

Wrong reaction: You click the link and enter your password so you do not lose your account.

Correct reaction: You stop. No legitimate IT Department asks for your password by email. You check the sender's address, do not click the link, and report it to the Security Department through an official channel.

Scenario 2: A found USB device

In the parking lot in front of the building you find a USB stick. You are curious what is on it and consider plugging it into your computer to see who it belongs to.

Wrong reaction: You plug in the USB stick to view its contents and return it to its owner.

Correct reaction: You do not plug it in. Abandoned USB devices are a common way of spreading malware. You hand it to the Security Department, which will examine it safely.

Scenario 3: A colleague asks for access

A colleague from another department asks you to lend them your password to access a system, because their access “is not working” and they need it urgently.

Wrong reaction: You give them your password to help, since they are a colleague and it seems urgent.

Correct reaction: You do not share your password — ever, with anyone. You direct them to contact the IT Department to resolve their access problem. Sharing passwords is a violation of the security rules.

Scenario 4: Working from a café

You are working from a café and urgently need to access an internal MEPSO system over the venue's free Wi-Fi.

Correct reaction: You connect through VPN before accessing any internal resource. You pay attention to who can see your screen. If VPN is not available, you wait until you have a secure connection.

Frequently asked questions

Is it really important to lock my screen if I am only stepping away briefly?

Yes. Even a few minutes are enough for someone to access your computer and its information. Locking the screen is a quick habit that prevents a big risk.

What if I forget a complex password?

Use a password manager — a tool that securely stores all your passwords, so you only need to remember one master password. The IT Department can recommend an approved tool.

Is it safe to reuse the same password if it is very strong?

No. Even the strongest password, if used in multiple places and one of them is compromised, exposes all of your accounts. Every account needs a unique password.

When should I report an incident?

Whenever you are in doubt. It is better to report something that turns out to be harmless than to miss a real incident. The security team is there to help.

Do my personal devices fall under these rules?

If you use them for work or to access MEPSO systems, yes. The same security principles apply to every device that touches the organization's information.

What if I suspect a colleague is breaking security rules?

Report what you know to the Security Department. This is not “telling on someone” — it is protecting the entire company from a potential risk.

Glossary of terms

A brief explanation of the key terms used in this field.

Term	Meaning
Authentication	The process of confirming a user's identity
Authorization	Determining what a user is allowed to access
Encryption	Converting data into an unreadable form for protection
Malware	A program created to cause harm or gain unauthorized access
Phishing	Fraud via fake messages aimed at stealing data
Ransomware	Malware that locks data and demands a ransom
VPN	Virtual private network for a secure remote connection
2FA	Two-factor authentication — a second layer of protection at login
Firewall	A system that controls network communication
Backup	A copy of data used for recovery in case of loss
Social engineering	Manipulating people into disclosing information
Critical infrastructure	Systems of essential importance to society

Daily security checklist

A practical list you can follow every working day.

At the start of the working day

- ✓ Check whether there are security updates to install
- ✓ Review your emails carefully before clicking

During the day

- ✓ Lock your screen whenever you step away
- ✓ Watch out for suspicious messages and requests
- ✓ Do not share access credentials with anyone
- ✓ Report anything suspicious immediately

At the end of the working day

- ✓ Lock away sensitive documents
- ✓ Apply the “clean desk” policy
- ✓ Log out or lock your computer
- ✓ Check that you have not left confidential materials in plain sight

> **Habit above all.** Security is not a one-off activity, but a daily habit. Small, consistent actions make the biggest difference.

12. Conclusion

Information security is a joint effort. Technology provides the tools, but real protection comes from aware and responsible employees. Every choice you make — from a strong password to reporting a suspicious message — contributes to the security of MEPSO.

This handbook is a starting point. Keep learning, stay alert, and do not hesitate to ask for help when in doubt. Security is a journey, not a destination.

> **Key message.** There is no such thing as perfect security, but there is responsible behavior. You are the most important part of the organization's defense.

MEPSO AD Skopje — Electricity Transmission System Operator of North Macedonia
Document No. MEPSO-PRI-IB-001 · Classification: Internal Use