

Implementation of Cybersecurity

How It Runs and How It Changes

Cyril Klimeš, Tomáš Pitner

Module Contents

1. Module Summary . . . 2
2. Secure Operation and Communication Network Security . . . 3
3. The Provider of a Regulated Service Shall Ensure . . . 4
   3.1. Rules . . . 4
   3.2. Procedures . . . 4
   3.3. Essential requirement . . . 5
4. Change Management . . . 6
5. Duties of the Provider of a Regulated Service . . . 7
6. Significant Change is . . . 8
   6.1. Testing and Rollback . . . 8
7. Change in Information Security . . . 9
   7.1. Change in Confidentiality . . . 9
   7.2. Change in availability . . . 9
   7.3. Change in Integrity . . . 9
8. Examples of Potentially Significant Changes . . . 11
   8.1. Application security . . . 11
   8.2. Infrastructure Change . . . 11
   8.3. Change in Availability Level Assurance . . . 11
   8.4. Human Resources Security . . . 12
   8.5. Change in Cybersecurity Organization . . . 12
   8.6. Supplier security . . . 13
   8.7. Physical security . . . 13
   8.8. Communication network security . . . 13
   8.9. Protection against malicious code . . . 14
   8.10. Cloud Services . . . 14
   8.11. Event Logging and Correlation . . . 14
   8.12. Cryptographic means . . . 14
9. Document Policy for managing significant changes in ICT . . . 16
10. Acquisition, Development, and Maintenance . . . 17
   10.1. Acquisition of Assets . . . 17
   10.2. Development . . . 17
   10.3. Maintenance . . . 17
   10.4. Ongoing Activities . . . 17
   10.5. Ongoing Activities (2) . . . 18
   10.6. Ongoing Activities (3) . . . 18
11. Managing Cybersecurity Events and Incidents . . . 19
   11.1. Cybersecurity Event (CSE) . . . 19
   11.2. Cybersecurity Incident (CSI) . . . 19

11.3. What does a CSE that escalates into a CSI look like? . . . 19
11.4. Responsibilities . . . 19
11.5. Responsibilities (2) . . . 20
12. Business Continuity Management . . . 21
12.1. Business Continuity Management Life Cycle . . . 21
12.2. Scheme of a Cybersecurity Incident and Business Continuity . . . 21
12.3. From Rating to Targets . . . 22
12.4. Steps for business continuity management . . . 22
13. Access Control . . . 23
14. Obligated Entity . . . 24
15. Obligations . . . 25
15.1. Access Privileges . . . 25
15.2. Access Privileges Review . . . 25
15.3. User Procedure Compliance . . . 25
16. Accounts for Access Control . . . 26
16.1. Privileged Accounts . . . 26
17. Access Control . . . 27
17.1. Access Control (2) . . . 27
18. Bring Your Own Device (BYOD) . . . 28
18.1. Bring Your Own Device (2) . . . 28
18.2. Privileged Accounts . . . 28
18.3. Privileged Accounts (2) . . . 28
19. Physical Security . . . 30
19.1. Physical Security Measures . . . 30
19.2. Perimeter Protection . . . 30
19.3. Key Functions . . . 30
19.4. Access Control . . . 30
19.5. Internal Security . . . 31
19.6. Protection of Computer Systems . . . 31
19.7. Protection Against Adverse Natural Influences . . . 31
19.8. Protection Against Adverse Natural Influences (2) . . . 31
19.9. Compliance with Electrical and Fire Regulations . . . 32
19.10. Compliance with Electrical and Fire Regulations (2) . . . 32
19.11. Ensuring a Suitable Environment for Equipment Operation . . . 32
19.12. Ensuring a Suitable Environment for Equipment Operation (2) . . . 33
19.13. Ensuring Redundancy . . . 33

- Expected lecture date WS 2026: **Nov 3**

Chapter 1. Module Summary

- **Secure operation and communication networks**: rules for the whole life cycle of information, start, stop, and restore, regular backups and their verification, network service security.
- **Change management**: significant change, testing and rollback, changes in confidentiality, availability, and integrity, policy for managing them.
- **Acquisition, development, maintenance**: supplier assessment, security requirements, SDLC, security testing, patches, protection of test data.
- **Events and incidents**: cybersecurity event vs. cybersecurity incident, escalation, responsibilities of the provider.
- **Business continuity**: key elements of the organization, MTPD, RTO, RPO, continuity policy, testing, resilience.
- **Access control**: obligations of the obligated entity, access privileges and their review, privileged accounts, BYOD.
- **Physical security**: perimeter, access control, internal security, natural influences, electrical and fire regulations, redundancy.

Chapter 2. Secure Operation and Communication Network Security

Chapter 3. The Provider of a Regulated Service Shall Ensure

Decree No. 409/2025 Coll., Section 12 (acquisition, development and maintenance), Section 18 (security of communication networks) and Section 11 (change management); Act No. 264/2025 Coll., Section 14

- **rules and procedures** for the protection of information and data throughout the entire life cycle,
  - procedures for **starting and stopping** the system,
  - for **restarting or restoring** the system after a failure,
  - and for **handling error states** or **exceptional events**,
- performing **regular backups** and **checking the usability** of the backups,
- rules and procedures for ensuring the **security of network services**.

3.1. Rules

- Documentation of the **rights and obligations** of administrators, users, and persons holding security roles,
- documentation of procedures for the **secure operation** of **ICT equipment** (e.g., turning PCs on/off, backup, installation/configuration of systems, maintenance of equipment, handling of media, PC room management, work safety, etc.),
- detection of cyber security incidents and regular evaluation of the information obtained (creation of audit records, IS monitoring, record protection, failure logging, clock synchronization),
- rules and procedures for protection **against malicious code** (antivirus strategy),
- technical **vulnerability management** (vulnerability scanning),
- contact **persons responsible** for providing system and technical support,

3.2. Procedures

- procedures for **managing changes** in processes, systems, and equipment for processing information that affect information security,
- procedures for monitoring, planning, and managing the capacity of **human and technical resources**,
- rules and procedures for **protecting information and data** throughout the entire life cycle,
- procedures for managing and controlling **software installation** and rules restricting software installation by users,
- performing **regular backups and testing** the usability of the backups made (backup plan,

compliance with the plan, testing the readability of backups, proper storage of backups),

- rules and procedures for ensuring the **security of network services**.

3.3. Essential requirement

Ensure the **separation of the development, testing, and operational** environments.



The testing environment should simulate the operational environment, but testing data must be anonymized.

Chapter 4. Change Management

Chapter 5. Duties of the Provider of a Regulated Service

Decree No. 409/2025 Coll., Section 11 (change management)

- reviews the possible **impacts of changes**,
- identifies **significant** changes,
- documents their **management**,
- performs **risk analysis**,
- takes measures to **reduce all adverse impacts** associated with significant changes,
- updates the **security policy** and security **documentation**,
- ensures their **testing**, and
- ensures the possibility of **returning** to the original state.

Chapter 6. Significant Change is

- Acquisition of a **new system or module**,
- change of a **significant supplier** with whom the administrator has no previous experience,
- **NÚKIB warning** of a cyber security threat,
- change in **organizational structure**,
- modification of **network topology**,
- replacement or acquisition of new **security tools** such as firewalls, SIEM, antivirus, DDoS washers, network probes, or replacement or acquisition of new hardware such as servers, switches, etc.

6.1. Testing and Rollback

- **Document** the management of the change,
- perform **risk analysis**,
- take measures to **reduce all adverse effects** associated with the change,
- update relevant **security policies** and security **documentation**,
- ensure **testing** of the change,
- ensure the possibility of **rollback** to the original state,
- decide, based on the above-mentioned risk analysis, to perform **penetration testing** or **vulnerability testing** (within the scope of assets affected by the significant change).

Chapter 7. Change in Information Security

Almost any change affects *data* or *security measures*, and both are assessed along the *CIA triad* defined in the first module.

7.1. Change in Confidentiality

Changes in Data

- There is a change in the data kept (extension, addition of personal data or special categories of personal data).
- There is a change in data recipients (new type of recipients, disclosure of part or all of the data, sharing of data with third parties, etc.).
- There is a change in the confidentiality of the services provided.

Changes in Security Measures

- Change in access control;
- Changes in user permissions;
- Change in access logging;
- Changes in data encryption;
- Changes in external and internal perimeter security features.

7.2. Change in availability

Changes in Data

- There is a change in the availability of stored data. The required availability is increased or decreased.
- There is a change in the availability of services provided.

Changes in Security Measures

- Change in the scope of backup and recovery.
- Change in the backup system concept.
- Change in system redundancy.

7.3. Change in Integrity

Changes in Data

- There is a change in data integrity. The impact on primary assets in the event of a breach of integrity is assessed differently from the perspective of the authorized person; the impact may be more or less significant.
- There is a change in the integrity of the services provided.

Changes in Security Measures

- Changes in change logging.
- Changes in the area of authentication elements.
- Changes in the security elements of the external and internal perimeter.

Chapter 8. Examples of Potentially Significant Changes

- Almost any change in IT can affect cybersecurity and infosecurity.
- However, not all changes are considered *significant*.

8.1. Application security

Simple change

- Change in user interface
- Change in settings made by the asset guarantor
- Change in system administration procedures
- Use of new libraries or frameworks

Potentially significant change

- Any change that affects existing application and communication security assets.
- Fundamental new system functionality used by most end users.
- Fundamental changes to system functionality (changes to approval processes and procedures).
- New services provided to the public.

8.2. Infrastructure Change

Simple change

- Replacement of disks in a disk array
- Replacement of a server or part of a server
- Replacement of active elements except those named
- Service replacement of components with capacity, performance, or communication capacity

Potentially significant change

- Any change that alters, expands, or otherwise modifies the volume, performance, or communication capacity, except for routine maintenance and replacement.
- New disk array.
- New server farm or part thereof.
- New core switches, firewall.
- Change of operating system or hypervisor or database manufacturer.

8.3. Change in Availability Level Assurance

Simple change

- Change in OS, DB, or hypervisor version
- Change in certificate
- Change in backup settings.
- Change in D/R scheme

Potentially significant change

- Conceptual change in administrator permission configuration
- Conceptual change in method of connection to central services
- Change in backup method
- Change in backup storage method
- Replacement of D/R system
- Change in D/R processes

8.4. Human Resources Security

Simple change

- Change of user
- Change of key user
- Change of asset guarantor
- Change in the frequency of security and/or application awareness training

Potentially significant change

- Change of IDM version or configuration,
- Conceptual change in password policy,
- Deployment of multi-factor authentication

8.5. Change in Cybersecurity Organization

Simple change

- Process change in incident reporting
- Process change in external access approval
- Change in implementation and operation rules

Potentially significant change

- Change of the obligations regime of the regulated service (higher / lower obligations regime)
- Change of the classification of the information system or of the **primary assets**
- Any change that affects the processes of the Information Security Management System

8.6. Supplier security

Simple change

- Change of supplier of a sub-activity or component
- Change of consultant or advisor
- Change of internet connection provider

Potentially significant change

- Change of Significant Supplier
- Change of operator
- Change in the conditions for ensuring the cyber security of a - Significant Supplier

8.7. Physical security

Simple change

- Repair of UPS, diesel generator, cooling, sensors
- Changes to cabling, relocation of racks
- Installation of new equipment in the rack

Potentially significant change

- Change of server room location
- Change of central UPS
- Change of diesel generator
- Fundamental change to server room security
- Change of technical infrastructure or IS operation location*#

8.8. Communication network security

Simple change

- Switch and router replacement
- Device firmware change
- Network configuration change
- Internet connection settings change
- Monitoring change
- Internal network routing settings change
- 1:1 network hardware replacement

Potentially significant change

- Conceptual change in VLAN, DMZ configuration
- Security change in firewall rules

- Conceptual change in the method of connecting data centers or connecting branches
- Change in external communication routing rules or change in IPS/IDS rules.

8.9. Protection against malicious code

Simple change

- Reinstallation of antivirus software on workstations/devices
- Ensuring access for suppliers
- Updating the version of the antivirus/antispam system

Potentially significant change

- Replacement of the antivirus/antispam system
- Conceptual change in the area of protection against malicious code
- Change in antivirus/antispam system settings

8.10. Cloud Services

Simple change

- Change in the scope and settings of cloud services

Potentially significant change

- Change in cloud service provider

8.11. Event Logging and Correlation

Simple change

- Change in logging structure
- Storage of logs on a different infrastructure, including migration
- Change in correlation rules
- Integration of new IS or technical assets into the monitoring and logging system

Potentially significant change

- Conceptual change in acquired logs
- Conceptual change in the protection of acquired logs
- Conceptual change in at least 10 correlation rules
- Replacement or expansion of the capacity of the monitoring and logging system
- Change in the logging and log storage scheme, change in escalation processes

8.12. Cryptographic means

Simple change

- Change in hash or encryption algorithm
- Expansion of the scope or type of encrypted data

Potentially significant change

- Conceptual change in the security of all devices (e.g., laptops)
- Change in key elements of the internal CA
- Change in hash or change in encryption algorithms

Chapter 9. Document Policy for managing significant changes in ICT

- General principles of change management
- Roles and responsibilities — Asset guarantor, CS manager, CS architect, Head of IT department responsible for operations, CS committee, User
- Types and areas of change — Significant change
- Change management process

Chapter 10. Acquisition, Development, and Maintenance

Decree No. 409/2025 Coll., Section 12 (acquisition, development, and maintenance); Act No. 264/2025 Coll., Section 14

10.1. Acquisition of Assets

Supplier assessment	When selecting suppliers, it is important to assess their security procedures and ability to protect data.
Security requirements	Define clear security requirements that the supplier must meet, including data encryption, access control, and malware protection.
Contractual obligations	Include specific security obligations and regular audits in contracts with suppliers.

10.2. Development

Secure development lifecycle (SDLC)	Implement security measures in all phases of the development lifecycle, from design to testing.
Security testing	Perform regular security tests, such as penetration tests and vulnerability analyses.
Developer training	Ensure that developers are trained in security practices and are aware of current threats.

10.3. Maintenance

Regular updates	Ensure regular updates and patches to software to fix known vulnerabilities.
Monitoring and detection	Implement systems for monitoring and detecting security incidents.
Data backup	Back up data regularly and verify that backups are secure and functional.

10.4. Ongoing Activities

Manage risks and significant changes

- These requirements include conducting risk assessments to identify potential negative impacts and proposing measures to mitigate these impacts.

10.5. Ongoing Activities (2)

- If a significant change is the subject of acquisition, development, and maintenance then:



- it is necessary to perform security testing before deployment,
- establish security requirements, include security requirements in the acquisition, development, and maintenance project (and in the contract with the supplier, if an external entity is involved in the process),

10.6. Ongoing Activities (3)

Ensure, perform,...

- ensure the security of the development and testing environment and ensure the protection of the test data used, i.e., for example, preventing work with real data, separating and preventing communication between the production and development environments, restricting access to the development environment only from specific and protected stations,
- perform security testing of significant changes before they are put into operation,
- if the goal is to acquire or develop an identity management and verification tool, the minimum level requirement for identity verification management must be met, such as multi-factor authentication with at least two different types of factors.

Chapter 11. Managing Cybersecurity Events and Incidents

11.1. Cybersecurity Event (CSE)

> událost, která může vyústit v kybernetický bezpečnostní incident
>
> — Act No. 264/2025 Coll., Section 2(2)(e)

An **event** that has not yet caused damage, but may lead to it: a failed firewall, a stolen password, an infected attachment, a user leaving an unlocked workstation.

11.2. Cybersecurity Incident (CSI)

> narušení bezpečnosti informací v kybernetickém prostoru
>
> — Act No. 264/2025 Coll., Section 2(2)(f)

An **event that has actually resulted in a breach** of confidentiality, integrity, or availability. Act No. 264/2025 Coll., Section 2(2)(b) — security of information means protection of its confidentiality, integrity, and availability

11.3. What does a CSE that escalates into a CSI look like?

- An employee leaves their workplace and *does not lock their computer* (CSE). The computer is **misused** (CSI).
- The perimeter *firewall fails* (CSE). As a result, the organization will **not have access** to the Internet (CSI).
- There is an *intrusion into the network* (CSE). **Malware is deployed** within the network (CSI).
- Login credentials are *stolen* (CSE). This is followed by **access to the network** using these credentials (CSI).
- A user downloads an attachment from a *virus-infected website* (CSE). Their end station is **attacked** by a virus or malware (CSI).

11.4. Responsibilities

Act No. 264/2025 Coll., Section 14 (list of security measures), Section 15 (reporting duty); Decree No. 409/2025 Coll., Section 14 (handling of events and incidents) and Sections 21-23 (detection, recording, evaluation)

- Establish a process for **detecting and evaluating** cyber security events and managing cyber

security incidents.

- Assign responsibilities and establish procedures for:
- detect and **evaluate cyber security events and incidents**,
- **coordinate and manage cyber security incidents**,
- **report cyber security incidents** to the regulator,
- **keep records** of cyber security incidents and their management.
- Define and apply procedures for identifying, collecting, obtaining, and preserving credible **evidence** needed to analyze a cyber security incident,
- **Ensure the detection** of cyber security events,
- Ensure that users, administrators, persons holding security roles, other employees and suppliers **report unusual behavior** of the information and communication system and any suspected vulnerabilities,

11.5. Responsibilities (2)

- **investigate and determine the causes** of the cyber security **incident**,
- **evaluate the effectiveness** of the incident solution and, based on the evaluation, determine the necessary security measures or update existing security measures to prevent a recurrence,
- **notify** the affected users and the regulator within the statutory deadlines,

Chapter 12. Business Continuity Management

Decree No. 409/2025 Coll., Section 15 (business continuity management)

- Identification of key elements (**systems and processes**) in the organization and subsequent setting of processes and procedures to **ensure continuity or restoration** of these elements at a predefined level at which it will still be possible to perform the basic tasks of the organization.
- It is necessary to perform a **risk assessment and analysis** of existing information and communication systems and services.

12.1. Business Continuity Management Life Cycle

It is necessary to determine:

the minimum level of services provided

that is acceptable for the use, operation, and management of the information and communication system — the **maximum tolerable period of disruption** (MTPD) for each key process,

recovery time

during which the minimum level of services provided by the information and communication system will be restored after a cyber security incident — the **Recovery Time Objective** (RTO),

data recovery point

as the time period for which data must be restored after a cyber security incident or failure — the **Recovery Point Objective** (RPO).

12.2. Scheme of a Cybersecurity Incident and Business Continuity

- **time to restore operation** — the **Recovery Time Objective** (RTO),
- **data recovery point** — the **Recovery Point Objective** (RPO).

12.3. From Rating to Targets

The targets are derived from the business impact analysis: the impact of the unavailability of a process on the organization, expressed in financial and non-financial terms. The **availability rating** assigned to the asset in the first module (*Asset Management*) sets the permitted unavailability; RTO and RPO make that rating operational.

The incident and continuity relationship: an incident is the trigger for the continuity plan, and the continuity plan defines the maximum time the incident is allowed to interrupt the service. The plan is tested through exercises that simulate the incident scenarios handled in *Managing Cybersecurity Events and Incidents*.

12.4. Steps for business continuity management

- Establishing a **business continuity management policy** includes rules and procedures for senior management, suppliers, etc.,
- assessing the potential risks and impacts of cyber security **incidents threatening business continuity**, based on risk assessment and impact analysis,
- Establishing the **rights and responsibilities of administrators** and persons holding security roles,
- Conducting regular testing, updating, and distribution of **business continuity plans** and contingency plans,
- Implementing measures to **increase the resilience** of the information system.

Chapter 13. Access Control

Chapter 14. Obligated Entity

- controls access based on **groups and roles,**
- assigns each user and administrator accessing the information and communication system **access rights and permissions and a unique identifier,**
- implements security **measures to control device access** to information and communication system resources,
- implements security measures necessary for the safe use of **mobile devices** and other technical equipment, and, where applicable, security measures related to the use of technical equipment **that the obligated person does not administer,**

Chapter 15. Obligations

- **manage access based on groups and roles,**
- **assign each user** and administrator accessing the information and communication system **access rights and permissions and a unique identifier**,
- **manage identifiers, access rights, and permissions** for applications and technical accounts,
- **implement security measures to control access** by devices to information and communication system resources,
- **implement security measures** necessary **for the secure use of mobile devices**

15.1. Access Privileges



Limit the assignment of privileged permissions to the level **necessary** to perform the job.

- limit and control the use of software resources that may be able **to bypass system** or application controls,
- **assign and revoke access permissions** in accordance with the access control policy,

15.2. Access Privileges Review

- **conduct regular reviews of the settings** of all access permissions, including the division into access groups and roles,
- **use an identity management and verification tool and** a tool for managing **access permissions**

15.3. User Procedure Compliance

- Enforce that users **comply with established procedures** when using private authentication information,
- Ensure that **access rights are revoked or changed** when there is a change in position or classification
- **users**, administrators, or persons holding security roles,
- **ensure that access rights are revoked or changed upon termination** or change of **contractual relationship**,
- **document the granting and revocation of access rights**.

Chapter 16. Accounts for Access Control

16.1. Privileged Accounts

- the highest level of access and permissions, used for system administration, configuration, and maintenance. They pose a significant security risk if compromised. Examples: administrator accounts, root accounts.
- Limited permissions required for routine tasks. Used by regular users to access applications and data. Less risky than privileged accounts, but still vulnerable to attack. Examples: accounts for employees, students.
- For automated processes and applications. They have specific permissions needed to run a given application or service. They are often not tied to a specific user, but to a system or application. Examples: accounts for database services, accounts for backup systems.



Only the rights that the application needs are granted.

Chapter 17. Access Control

- **Discretionary access control (DAC)**: Users have access rights that are determined by the data owner. This type of control is flexible, but may be less secure because users can change access rights.
- **Mandatory access control (MAC)**: Access rights are determined by a central authority and cannot be changed by users. This type is often used in high-security environments, such as the military.

17.1. Access Control (2)

- **Role-based access control (RBAC)**: Access rights are assigned based on the roles that users hold. This type is very effective for organizations where access needs to be managed for a large number of users.
- **Attribute-based access control (ABAC)**: Access rights are determined based on user attributes such as their role, access time, or the type of device they are using. This type is very flexible and allows for detailed access control.

Chapter 18. Bring Your Own Device (BYOD)

- Applicable to: *Employees who bring, use, and connect their own mobile devices, such as smartphones, laptops, or tablets, to the workplace.*
  - **Establish a clear BYOD policy -** permitted device types, security requirements, and procedures for accessing company data.
  - **Data encryption -** all sensitive data on personal devices must be encrypted.
  - **Access control -** two-factor authentication (2FA) and strong passwords
  - **Security software -** installation of antivirus and antimalware software

18.1. Bring Your Own Device (2)

- **Remote wipe capability -** in case of loss or theft.
- **Regular updates and patches -** regularly updated operating system and applications
- **Employee training -** on security threats and best practices for protecting their devices and company data.
- **Monitoring and auditing -** regular monitoring and auditing of devices and networks

18.2. Privileged Accounts

Multi-factor authentication (MFA)

Use MFA for all privileged accounts to increase access security.

Regular monitoring and auditing

Monitor and record the activities of privileged accounts so that you can quickly identify and respond to suspicious activities.

18.3. Privileged Accounts (2)

Password management

Use strong passwords and change them regularly. Consider using password managers for secure password storage and management.

Access time restrictions

Implement a "just-in-time" access policy that allows access only for a limited time when necessary.

Employee training

Regularly train employees on security procedures and the risks associated with privileged accounts.

Securing remote access

Use encrypted channels for remote access to systems and restrict access to approved devices

only.

Chapter 19. Physical Security

19.1. Physical Security Measures

- **perimeter** protection,
- **access** control,
- **internal** security,
- **protection** of computer systems — against dismantling, modification, or
- connecting **peripherals** to input/output ports
- protection against adverse **natural influences**,
- compliance with **electrical and fire regulations**,
- ensuring a **suitable environment** for equipment operation,
- ensuring **redundancy**, etc.

19.2. Perimeter Protection

Perimeter

- is an area that directly **surrounds the space in which protected assets** (data, information, as well as ICT elements, etc.) are located
- requires a combination of technologies and human resources.

19.3. Key Functions

Deterrence

Visible elements, such as **fences, walls, or warning signs**, can deter potential intruders.

Intrusion Detection

Use of various **sensors and detectors**, such as infrared beams, vibration sensors, or cameras, which record attempts to breach the perimeter.

Entry Prevention

Physical barriers, such as gates and barriers, that prevent unauthorized access.

Notification and Response

Systems that trigger alarms upon detecting an intrusion and alert security personnel.

19.4. Access Control

To ensure that only authorized persons can pass through the perimeter:

- **Key system**

- **Tokens**
- **Biometric** identification
- **Combination** of systems

19.5. Internal Security

- **Clean desk** policy
- Server **protection**
- **Camera** system
- Intruder **alarm** system connected to a central monitoring station
- **Air conditioning**, **UPS**
- **Redundant** backup power supplies
- **Fire suppression** system
- **ID cards**

19.6. Protection of Computer Systems

- Protection against **theft**
- Protection against **dismantling** and **modification**
- Protection against connecting **unauthorized peripherals**

19.7. Protection Against Adverse Natural Influences

- Minimize damage caused by natural disasters such as floods, earthquakes, storms, landslides, and others:

Resilient Building Construction	Use of materials and construction techniques that increase building resistance to earthquakes, strong winds, and other natural influences.
Flood Protection Measures	Building levees, retention basins, and reservoirs that help regulate water flows and reduce flood risk.

19.8. Protection Against Adverse Natural Influences (2)

Evacuation Plans	Preparation and regular updates of evacuation plans for residents of at-risk areas.
Early Warning Systems	Installation of sensors and monitoring devices that detect natural threats and provide timely warnings to the population.
Meteorological Services	Regular monitoring and forecasting of weather, which helps prevent damage caused by storms and other atmospheric

phenomena.

19.9. Compliance with Electrical and Fire Regulations

Electrical Equipment Safety	Ensuring that all electrical devices and installations meet safety standards and are regularly inspected.
Surge Protection	Installation of protective devices that protect equipment against surges and power outages.
Backup Power Sources	Use of backup power sources, such as UPS (uninterruptible power supplies), to ensure continuous operation of critical systems.

19.10. Compliance with Electrical and Fire Regulations (2)

Fire Detection and Suppression	Installation of smoke detectors and automatic fire suppression systems that respond quickly to fire outbreaks.
Evacuation Plans	Development and regular updating of evacuation plans in case of fire, including employee training.
Safe Equipment Placement	Locating critical equipment in areas with low fire risk and ensuring adequate ventilation and cooling.

19.11. Ensuring a Suitable Environment for Equipment Operation

Cooling

and maintaining proper humidity levels (preventing condensation and electrostatic discharges)

Security Measures

access only for authorized personnel.

Fire Protection

installation of smoke detectors and automatic fire suppression systems.

Stable Power Supply

(UPS and backup generators to ensure continuous operation even during power outages), **surge protection**.

19.12. Ensuring a Suitable Environment for Equipment Operation (2)

Spatial Organization

proper arrangement of equipment in rack cabinets and sufficient space for maintenance and cooling. Cable management organized for easy access and to minimize risk of overheating or damage.

Monitoring and Maintenance

regular monitoring of temperature, humidity, and other critical parameters. Performing regular maintenance and equipment checks to ensure long-term reliability.

19.13. Ensuring Redundancy

- Minimization of **outages**
- Increased **reliability**
- Protection against **physical threats**
- Ensuring **operational continuity**
- Rapid **recovery** after a disaster