



# Cybersecurity

## Basic level – Basic IT security

CFPA-E Guideline No 13:2024 S





**The CFPA Europe develops and publishes common guidelines about fire safety, security, and natural hazards with the aim to achieve similar interpretation and to give examples of acceptable solutions, concepts, and models. The aim is to facilitate and support fire protection, security, and protection against natural hazards across Europe, and the whole world.**

**Today fire safety, security and protection against natural hazards form an integral part of a modern strategy for survival, sustainability, and competitiveness. Therefore, the market imposes new demands for quality.**

**These Guidelines are intended for all interested parties and the public. Interested parties includes plant owners, insurers, rescue services, consultants, safety companies and the like so that, in the course of their work, they may be able to help manage risk in society.**

**The Guidelines reflect best practice developed by the national members of CFPA Europe. Where these Guidelines and national requirements conflict, national requirements shall apply.**

**This Guideline has been compiled by the Security Commission and is adopted by the members of CFPA Europe.**

**More information: [www.cfpa-e.eu](http://www.cfpa-e.eu)**



Wallisellen, March 2024  
CFPA Europe

Elisabetta Carrea  
Chairman

Cologne, March 2023  
Security Commission

Ingeborg Schlosser  
Chairman



**Contents**

Foreword..... 4

Orientation..... 4

1 Scope..... 5

2 References..... 5

3 Definitions..... 5

    3.1 user account (user)..... 5

    3.2 application..... 5

    3.3 authorization..... 5

    3.4 computer..... 6

    3.5 mobile devices..... 6

    3.6 network devices..... 6

    3.7 organization's resources..... 6

    3.8 operating system..... 6

    3.9 portable storage media..... 6

    3.10 software..... 6

    3.11 service accounts..... 6

    3.12 strong passwords..... 6

4 Requirements..... 7

    4.1 Computers and mobile devices..... 7

        4.1.1 General..... 7

        4.1.2 Creating backups..... 7

        4.1.3 Protection against malicious code..... 7

        4.1.4 Use of the organization's resources for private use..... 7

        4.1.5 Use of private equipment..... 7

    4.2 Software and applications..... 8

        4.2.1 General..... 8

        4.2.2 Security updates..... 8

        4.2.3 Automatic program launch and automatic playback..... 8

    4.3 Networks..... 8

        4.3.1 General..... 8

        4.3.2 Guest network..... 10

        4.3.3 Traffic protection..... 10

    4.4 External IT services, including cloud storage..... 10

        4.4.1 Agreement..... 10

        4.4.2 Scope of the agreement..... 10

        4.4.3 GDPR..... 11

    4.5 Access rights..... 11

        4.5.1 User accounts..... 11

        4.5.2 Service accounts..... 11

        4.5.3 Access Rights..... 11

        4.5.4 Passwords..... 11

    4.6 Information security training..... 11

5 Bibliography..... 12

European guidelines..... 13

Key words:

## **Foreword**

This document is based on SSF-standard 1101 (edition 1 from 2018).

CFPA Europe thanks SSF (the Swedish Theft Prevention Association) for the permission to publish it as a CFPA Europe Guideline.

SSF is a non-profit organization. The aim of the association is to promote safety and security for individuals and property through crime prevention measures, and to help shape opinions and disseminate information with regard to crime prevention.

SSF has been publishing standards on behalf of the Swedish Insurance Federation (formerly Försäkringsförbundet) since 2001.

Further information can be found on the SSF website at [www.stoldskyddsforeningen.se](http://www.stoldskyddsforeningen.se)

The SSF standards refer to, or wherever possible are based on, national and international standards and other applicable technical specifications or international quality standards.

Application is voluntary unless agreed otherwise.

In addition to the requirements specified in the standards, compliance with laws and official national regulations is assumed.

## **Orientation**

This standard specifies basic IT security requirements.

The organizations of today face a number of security-related challenges when it comes to collecting, processing, storing and transferring information. This standard is aimed primarily to small and medium-sized organizations that are in need of practical action in order to effectively protect important information as part of their business.

This document constitutes Basic level – basic IT security and should act as a first step in organizations' efforts to enhance the ability to deal with risks linked with information management. This standard aims to specify requirements for certification in accordance with the basic level.

## **What is information security?**

Information security involves preservation of confidentiality, integrity and availability of information. Information is an asset which, like other important business assets, is of value to businesses and therefore needs appropriate protection. Information security measures aim to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, review, playback or destruction.

## **1 Scope**

This guideline includes basic and specific requirements for small and medium-sized organizations.

National organisations may offer certifications for SME in accordance with this guideline. The scope of certification can be restricted to a specific organizational element and/or a technical function (one or more systems or processes).

## **2 References**

This guideline contains dated or undated references to regulations in other publications. These normative references can be found in the body copy. The publications are listed below. With regard to dated references to publications that have subsequently been amended or supplemented, such amendments and supplements are only valid if they have been inserted into these regulations. For undated references, the latest edition of the publication applies.

EN ISO/IEC 17021 Conformity assessment – Requirements for bodies providing audit and certification of management systems

EN ISO/IEC 17024 Conformity assessment – General requirements for bodies operating certification of persons

DISA Computer-aided information security training for users. (2017). Swedish Civil Contingencies Agency (MSB).  
<https://www.msb.se/sv/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/DISA---Datorstodd-informations sakerhetsutbildning-for-anvandare/>

## **3 Definitions**

The definitions, terms and abbreviations specified below are applicable when using this document.

### **3.1 user account (user)**

An account with the minimum access rights possible, this allows the user to do their work and is used for working on tasks that do not relate to system administration.

### **3.2 application**

This refers to a software program with the aim of constituting a link between the computer's operating system and the user. Examples of applications are Microsoft Excel, Google Chrome, Adobe Photoshop, Spotify and McAfee Antivirus, etc.

### **3.3 authorization**

Assigned rights to use an information asset in a specified manner. Rights that can be assigned may allow you to read, write, edit or delete information.

### **3.4 computer**

This includes laptop computers, desktop computers, servers or similar.

### **3.5 mobile devices**

This includes mobile phones, tablets and wearables (e.g. smartwatches) or similar.

### **3.6 network devices**

This includes routers, firewalls, manageable switches and suchlike. It also includes all devices – with the exception of guest devices on the guest network – that are connected to the organization's network and that are not specified under 3.4 computer or 3.5 mobile devices.

Networked VSS cameras, printers and smart devices are examples of this.

### **3.7 organization's resources**

These are resources that are owned or managed by the organization within the organization's infrastructure/environment.

### **3.8 operating system**

This refers to one or more programs with the aim of constituting a link between the computer's hardware and the user's software. Windows , Linux and Mac OS are examples of this.

### **3.9 portable storage media**

This refers to USB sticks, external hard disks, CDs and DVDs or similar.

### **3.10 software**

This refers to software in the sense of an organized collection of data and machine instructions which execute tasks in a computer system. This includes both operating systems and applications, but also programming tools under the programs that come within the definitions above.

### **3.11 service accounts**

Service accounts are accounts that are not used by administrators or users, but by services that need an account for access purposes, for example. An account belonging to a database service that needs rights to be able to write to a server or an account belonging to an antivirus program that needs to be able to read users' files are examples of this.

### **3.12 strong passwords**

A strong password must not appear in known password dumps/password lists and contain at least 10 characters. Passwords must be made up of upper and lower case letters and special characters and not include a word that appears in a dictionary or similar where substitution has occurred (e.g. replacing a letter in a word with a digit).

## **4 Requirements**

### **4.1 Computers and mobile devices**

#### **4.1.1 General:**

- Default passwords for user accounts for computers and mobile devices must be changed to strong passwords that are not reused.  
Note: No passwords are to be reused (this includes both passwords used previously and using the same password on different devices) by either employees or groups of employees.  
Passwords that have been used within the organization must not be used privately, or vice versa .
- Strong passwords must be defined in a decision by the organization. As a minimum, passwords must comply with the security level as specified in the standard.
- Encryption of storage space on computers and mobile devices must be enabled wherever possible.

#### **4.1.2 Creating backups**

- Information must be backed up to the extent decided upon by the company regularly.
- At least one backup must be available only to individuals with administrative system access rights.  
Note: Information backed up may be checked by carrying out regular random inspections.

#### **4.1.3 Protection against malicious code**

Software for protection against malicious code:

- must be installed on all computers and mobile devices that are or may be connected to external networks such as the Internet.
- must be updated automatically or by means of a special procedure.
- must be configured to automatically search files and emails on arrival (including when downloading and opening files on network devices and portable storage media)
- must scan websites on computers and alert the user if the website contains malicious code Note: The software must use warnings or blocking to ensure that the user is aware of websites that contain malicious code and prevent the code being executed initially.
- must be configured to execute regular scans for malicious code.
- may be protected from user actions like removing the software or changing its configuration.

#### **4.1.4 Use of the organization's resources for private use**

- Decisions must be made on whether the organization's resources may be used for private use, and if so to what extent.

#### **4.1.5 Use of private equipment**

- Decisions must be made on whether private equipment may be used within the organization, and if so to what extent.

8 | **GUIDELINE No 13:2024**

- Private equipment used within the organization must be subject to the at least same security requirements as the rest of the organization's equipment.



- Specific work rules and procedures must be documented and followed for private equipment used within the organization.

## **4.2 Software and applications**

### **4.2.1 General**

- All software that is subject to copyright must be licensed for use within the organization.
- Software must always be downloaded from the official distributor's website or similar verifiable sources.
- Applications for mobile devices must only be downloaded from trusted sources.
- Only software and applications that are necessary for the business are to be installed .  
Note: See section 4.1.4
- Software and applications that are not used must be uninstalled as soon as possible.  
Note: Downloading applications to mobile phones and tablets from trusted sources involves the organization's own internal site for approved programs and applications, for example.

### **4.2.2 Security updates**

- Security updates must be installed automatically for operating systems, software and applications that run on computers, network devices and mobile devices, where technically possible.
- Operating systems, software, applications and network devices for which security updates are no longer installed must be removed or moved to logically or physically separated segments where they can be managed on the basis of special rules.  
Note: If this requirement is not met, the organization must justify why it accepts the risk of deviating from the above requirement.

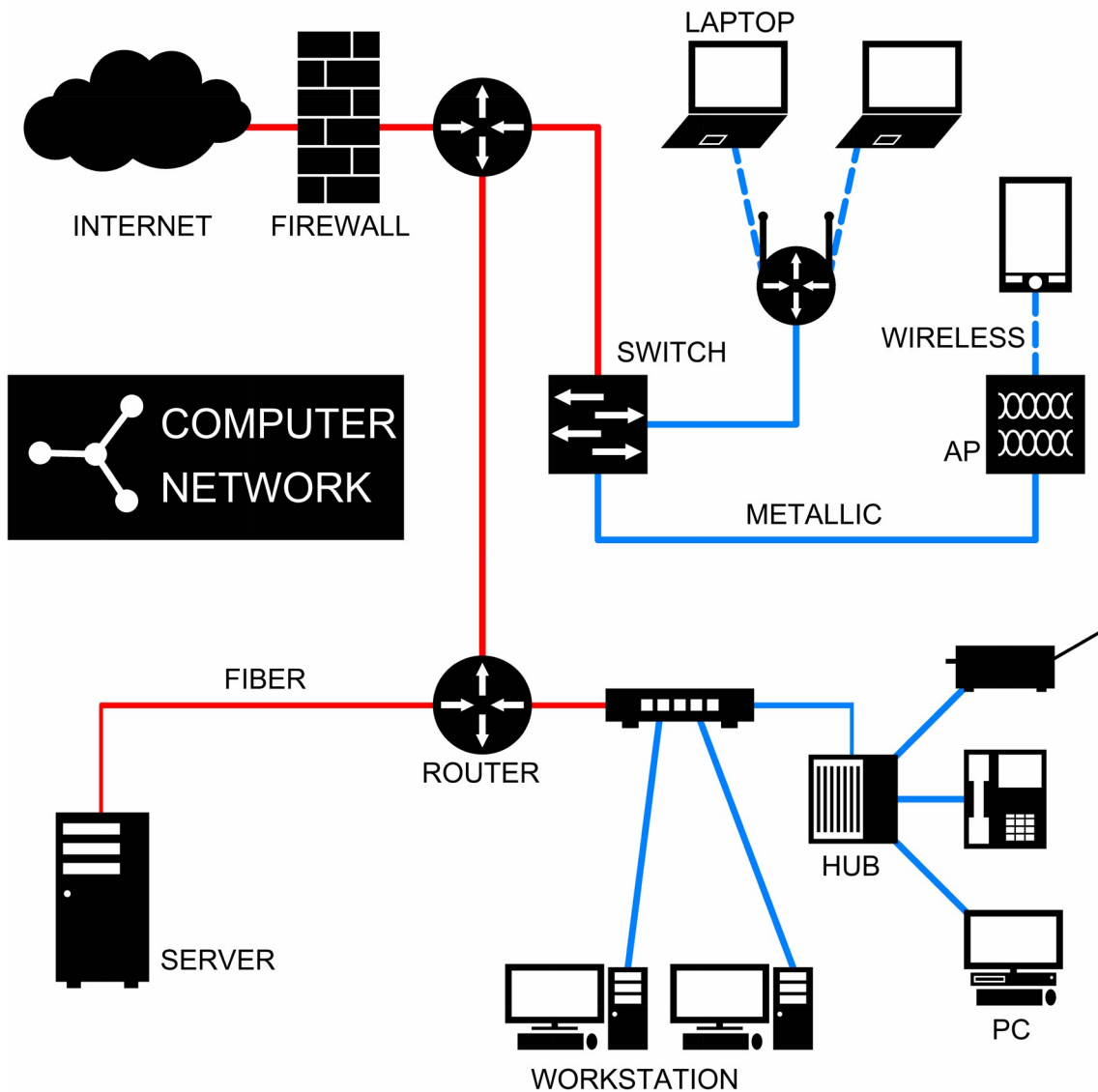
### **4.2.3 Automatic program launch and automatic playback**

- Automatic program launch must be limited to applications that are identified by the organization as being necessary to launch automatically.  
Note: Decisions on the applications identified must be made by the organization.
- Automatic playback must be disabled for all files from portable storage media.

## **4.3 Networks**

### **4.3.1 General**

- One or more network devices with firewall functionality must be installed between the company's internal network and external networks such as the Internet.  
Note: If there is no internal network, computers must be provided with firewall functionality between computers and external networks such as the Internet.
- The network must be broken down into components, each with a specific mission according to the needs of the organization. Each component must be in a separate local network partitioned from the rest of the network. The connectivity needs between the different networks must be studied and limited to a strict necessity. See drawing.



- Before a network device is installed, the default password must be changed to a strong password that is not reused, where technically possible.  
Note: No passwords are to be reused (this includes both passwords used previously and using the same password on different devices) by either employees or groups of employees.
- Passwords that have been used within the organization must not be used privately, or vice versa.
- Passwords for administrative accounts (including service accounts) on network devices must be changed at intervals decided upon by the organization.
- All open connections (i.e. permitted ports and services) in the firewall must be decided upon by the organization.  
Note: This decision should be documented (including an explanation of the needs of business)
- Firewall rules that are no longer needed must be deleted or disabled.

## 11 GUIDELINE No 13:2024

- Computers that do not need to connect to the Internet must be prevented from initiating connections to the Internet
- The administrative interface used to configure the organization's firewall or firewalls should not be accessible from external networks such as the Internet. If it is accessible from external networks it must be protected by MFA.
- All wireless networks must be encrypted and protected by a secure protocol, and with a strong password or certificate.  
Note: A secure protocol is a protocol in line with prevailing good practice. WPA2-PSK(AES) or equivalent is recommended at present.
- Configurations of all internal network devices (e.g. switches and servers) must be backed up. This must be repeated when configuration is changed.

### 4.3.2 Guest network

- The guest network must be separated from the organization's internal network  
Note 1: The password for the guest network will only be disclosed to authorized persons. Note 2: Regular work must not take place via the guest network.
- Administrative and technical control measures must be implemented for visitor access to network and internet.

### 4.3.3 Traffic protection

- When using public networks (such as public Wi-Fi and wired public networks), traffic must be protected from unauthorized access by means of a VPN or similar.
- Communication between client and server for email must be protected with encryption.  
Note: Encryption may take place with the help of TLS (Transport Layer Security).
- The organization's domain name for DNS must be protected with DNSSEC.

## 4.4 External IT services, including cloud storage

### 4.4.1 Agreement

- There must be a legally binding agreement between the organization and the supplier when using external IT services and cloud services.

### 4.4.2 Scope of the agreement

The agreement should normally include the following terms:

- Who owns the information.
- Who has access to the information.
- Where the information is stored (geographically).
- Which service level (accessibility, support, troubleshooting, etc.) the organization can expect from the supplier and agreed deliveries (availability on the Internet, for example)
- The fact that the supplier has a security level through accreditations, certificates or other independent evidence that corresponds to or surpasses the requirements in accordance with this standard.
- How security incidents are handled by the supplier and reported to the client.
- The fact that information is backed up and how data recovery takes place and what time scale is acceptable.
- If information is encrypted, and if so how.
- Responsibilities after agreement ended or terminated.

#### **4.4.3 GDPR**

- If the service includes processing or storage of personal data, the supplier must certify that it is compliance with requirements in accordance with the European General Data Protection Regulation (GDPR) and other EU-regulations regarding cyber security.
- A personal data assistant agreement must exist between the supplier and the organization if so required.

### **4.5 Access rights**

#### **4.5.1 User accounts**

- User accounts must be created following decisions by the organization. Note: These decisions should be documented.
- System administrator access rights may only be assigned and used by individuals performing system administration tasks.
- Administrative accounts must only be used to implement permitted administrative activities such as system maintenance.
- User accounts must be assigned to individual employees.
- User accounts must be deleted or disabled when they are no longer needed (e.g. when an employee leaves the organization).

#### **4.5.2 Service accounts**

- Service accounts must be created by authorized person from IT.
- Their usage purpose must be documented and protected from unauthorized access. (It may affect the critical software and applications)

#### **4.5.3 Access Rights**

- Individual employees must only have access to the systems required by their work
- Shared storage areas must be configured so that individual employees can only access the information required by their work
- Access rights must be assigned by authorized custodian person with specified procedure.
- Access rights must be reviewed when employee's role is changed.
- Access rights must be removed when employee leaves organization.

#### **4.5.4 Passwords**

- As a minimum, users must be authenticated using strong passwords that are not reused before access to programs and computers will be permitted. If technically possible, user accounts should be protected with MFA.
- Passwords for system administrator accounts and service accounts must be changed at intervals decided upon by the organization
- If it is suspected or can be demonstrated that a password has been disclosed to anyone other than the user themselves, it must be changed immediately.
- Passwords must be changed to the extent and at the intervals required by the business

### **4.6 Information security training**

13 **GUIDELINE No 13:2024**

All employees must complete basic training on information security at least once a year or as recommended in the company's data protection policy.

## 5 **Bibliography**

The following standards and documents have been used as a basis for the standard:

EN-ISO/IEC 27001:2017 Information technology – Security techniques – Information security management systems – Requirements.

EN-ISO/IEC 27002:2017 Information technology – Security techniques – Code of practice for information security controls.

SIS – TR 50:2015 Terminologi för Informationssäkerhet

MSB1138 Informationssäkerhet för småföretag. Praktiska råd och rekommendationer. Swedish Civil Contingencies Agency

NIST Digital Identity Guidelines (2017), NIST – National Institute of Standards and Technology.

National Cyber Security Centre NCSC, Cyber Essentials.

## **European guidelines**

### Fire

- Guideline No1 F - Internal fire protection control
- Guideline No 2 F - Panic & emergency exit devices
- Guideline No 3 F - Certification of thermographers
- Guideline No4 F - Introduction to qualitative fire risk assessment
- Guideline No5 F - Guidance signs, emergency lighting and general lighting
- Guideline No 6 F - Fire safety in care homes
- Guideline No7 F - Safety distance between waste containers and buildings
- Guideline No 8 F - Preventing arson – information to young people
- Guideline No 9 F - Fire safety in restaurants
- Guideline No 10 F - Smoke alarms in the home
- Guideline No 11 F - Recommended numbers of fire protection trained staff
- Guideline No 12 F - Fire safety basics for hot work operatives
- Guideline No 13 F - Fire protection documentation
- Guideline No 14 F - Fire protection in information technology facilities
- Guideline No 15 F - Fire safety in guest harbours and marinas
- Guideline No 16 F - Fire protection in offices
- Guideline No 17 F - Fire safety in farm buildings
- Guideline No 18 F - Fire protection on chemical manufacturing sites
- Guideline No 19 F - Fire safety engineering concerning evacuation from buildings
- Guideline No 20 F - Fire safety in camping sites
- Guideline No 21 F - Fire prevention on construction sites
- Guideline No 22 F - Wind turbines – Fire protection guideline
- Guideline No 23 F - Securing the operational readiness of fire control system
- Guideline No 24 F - Fire safe homes
- Guideline No 25 F - Emergency plan
- Guideline No 26 F - Fire protection of temporary buildings on construction sites
- Guideline No 27 F - Fire safety in apartment buildings
- Guideline No 28 F - Fire safety in laboratories
- Guideline No 29 F - Protection of paintings: transports, exhibition and storage
- Guideline No 30 F - Managing fire safety in historic buildings
- Guideline No 31 F - Protection against self-ignition and explosions in handling and storage of silage and fodder in farms
- Guideline No 32 F - Treatment and storage of waste and combustible secondary raw materials
- Guideline No 33 F - Evacuation of people with disabilities
- Guideline No 34 F - Fire safety measures with emergency power supply
- Guideline No 35 F - Fire safety in warehouses
- Guideline No 36 F - Fire prevention in large tents
- Guideline No 37 F - Photovoltaic systems: recommendations on loss prevention
- Guideline No 38 F - Fire safety recommendations for short-term rental accommodations
- Guideline No 39 F - Fire protection in schools
- Guideline No 40 F - Procedure to certify CFPA-E Fire Safety Specialists in Building Design
- Guideline No 41 F - Safety Instructions for the use and charging of small and medium size lithium ion powered devices
- Guideline No 42 F - Procedure to certify CFPA\_ Fire Safety Specialists in Building Design

Natural hazards

Guideline No1 N - Protection against flood

Guideline No2 N - Business resilience - An introduction to protecting your business  
Guideline No 3 N - Protection of buildings against wind damage

Guideline No4 N - Lighting protection

Guideline No5 N - Managing heavy snow loads on roofs  
Guideline No6 N - Forest fires

Guideline No7 N - Demountable / Mobile flood protection systems

Guideline No8 N - Ensuring supplies of firefighting water in extreme weather conditions  
Guideline No 9 N - Protection against hail damage

Guideline No 10 N - Heavy rain and flash flood prevention and protection

Security

Guideline No1 S - Arson document

Guideline No2 S - Protection of empty buildings

Guideline No3 S - Security systems for empty buildings

Guideline No4 S - Guidance on keyholder selections and duties  
Guideline No 5 S - Security guidelines for museums and showrooms

Guideline No6 S - Security guidelines emergency exit doors in non-residential premises  
Guideline No 7 S - Developing evacuation and salvage plans for works of art and

heritage

buildings  
Guideline No 8 S - Security in schools

Guideline No9 S - Recommendation for the control of metal theft  
Guideline No 10 S - Protection of business intelligence

Guideline No11 S - Cyber security for small and medium-sized enterprises

Guideline No 12 S - Security Guidelines for Businesses







[www.cfpa-e.eu](http://www.cfpa-e.eu)