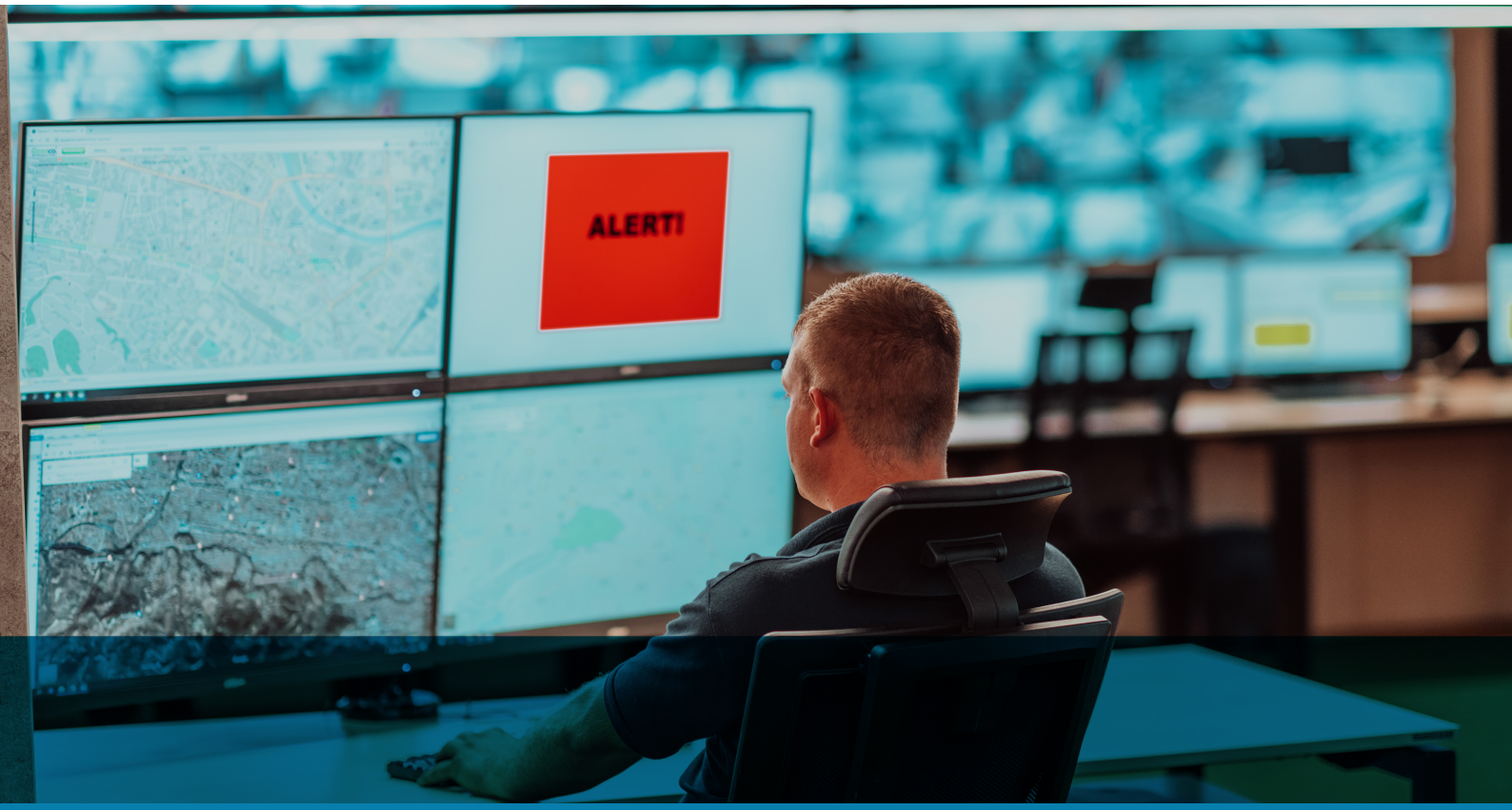


Cybersecurity Guidelines

for the Security and Fire Safety Industry

CoESS

euralarm

for a safer and more secure Europe

Introduction

Cybersecurity is no longer a "nice-to-have" in the security and fire safety industry. It is a quality requirement, an essential part of ensuring the resilience of your company and your clients – and for many businesses already a legal obligation. With new EU rules resulting from the NIS2 Directive and the Cyber Resilience Act (CRA), most organisations involved in product development, installation, monitoring and alarm services must integrate cyber-resilience into their everyday operations.

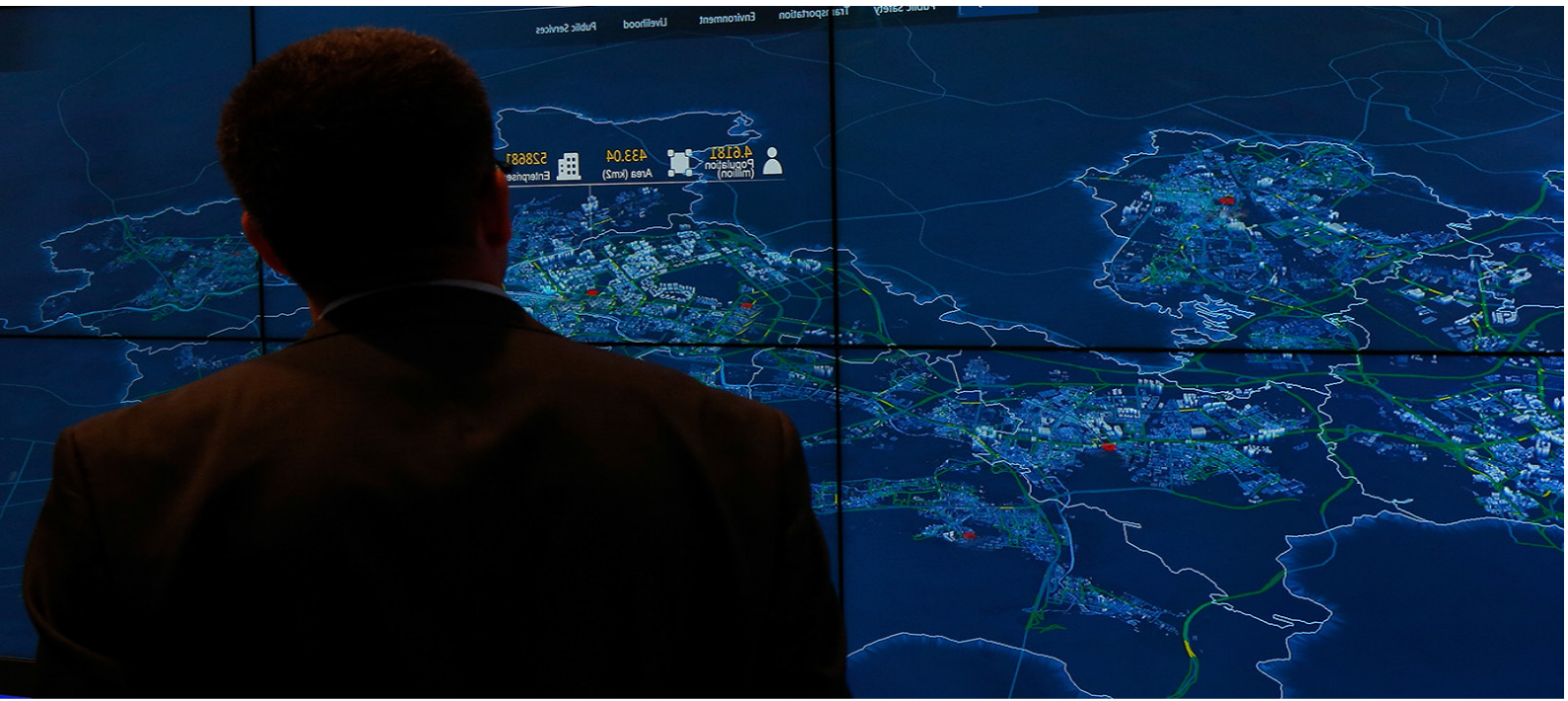
Because the reality is simple: anything connected can be attacked – whether it's a fire alarm, camera, or software platform. In today's interconnected systems, one weak link is enough to disrupt a protected site, your own and your clients' business.

For many, cybersecurity may still feel like a complex topic that is hard to navigate. But the essentials are simple: cybersecurity does not always require complex technology or large budgets. Many risks can be reduced with basic measures. And because most incidents start with human error, cybersecurity awareness and governance frameworks remain your strongest defence.

These updated CoESS-Euralarm Guidelines explain, in clear and practical terms, what every actor in the security and fire safety value chain must do to contribute to cybersecurity. They provide:

- A short overview of the key legal cybersecurity requirements relevant to the industry.
- Guidance on how to set up internal cybersecurity governance frameworks that ensure accountability and clear responsibilities.
- Concrete recommendations and technical measures following the established five-pillar approach also used by *CLC TC 79 WG 17 on Cyber Security for Connected Alarm Systems*. This covers the full lifecycle of security services: products, project design, installation and maintenance, monitoring services, and alarm response services.

By taking cybersecurity seriously, companies protect their operations, their customers, their brand, and the overall trust in the security and fire safety industry. These guidelines show that improving cyber-resilience is achievable for everyone, step by step. And the first is recognising that cybersecurity is now part of the job – for everybody.



THE HUMAN FACTOR: KEY FOR A RESILIENT CYBERSECURITY FRAMEWORK

FOR YOUR BUSINESS

- Set up an internal cybersecurity governance team and processes, and identify relevant cybersecurity roles, responsibilities and accountabilities among staff in your company. To reduce ambiguity and strengthen accountability, the European Union Agency for Cybersecurity, ENISA, has published a European Cybersecurity Skills Framework that defines 12 core cybersecurity role profiles within a company, each detailing their respective missions, tasks, required skills and competencies. A dedicated framework was developed for entities subject to the NIS2 Directive.
- Maintain an updated inventory of IT and OT components with documented cybersecurity features, vendor contact details, risks and IT/OT system interdependencies.
- Get an understanding of legal cybersecurity requirements applying to your business operations and security system / service chain, confirm compliance deadlines, and identify standards that can help fulfil conformity assessments and compliance.
- Conduct regular risk assessments and set in place / review regularly respective risk management, business continuity and incident handling processes.
  - Ensure all relevant cybersecurity roles are involved in the development, implementation and review of risk management, business continuity and incident handling processes.
  - Designate a dedicated Business Continuity Team, incl. responsibilities, rules and procedures for incident handling actions.
  - Prepare and test business continuity and incident handling processes to deal with different events, incl. through regular stress tests.
  - Ensure effective data and system back-up and recovery policy.

Certification under the ISO/IEC 27000 series is useful to establish, implement, maintain, and continually improve an information security management in your business.

FOR YOUR WORKFORCE

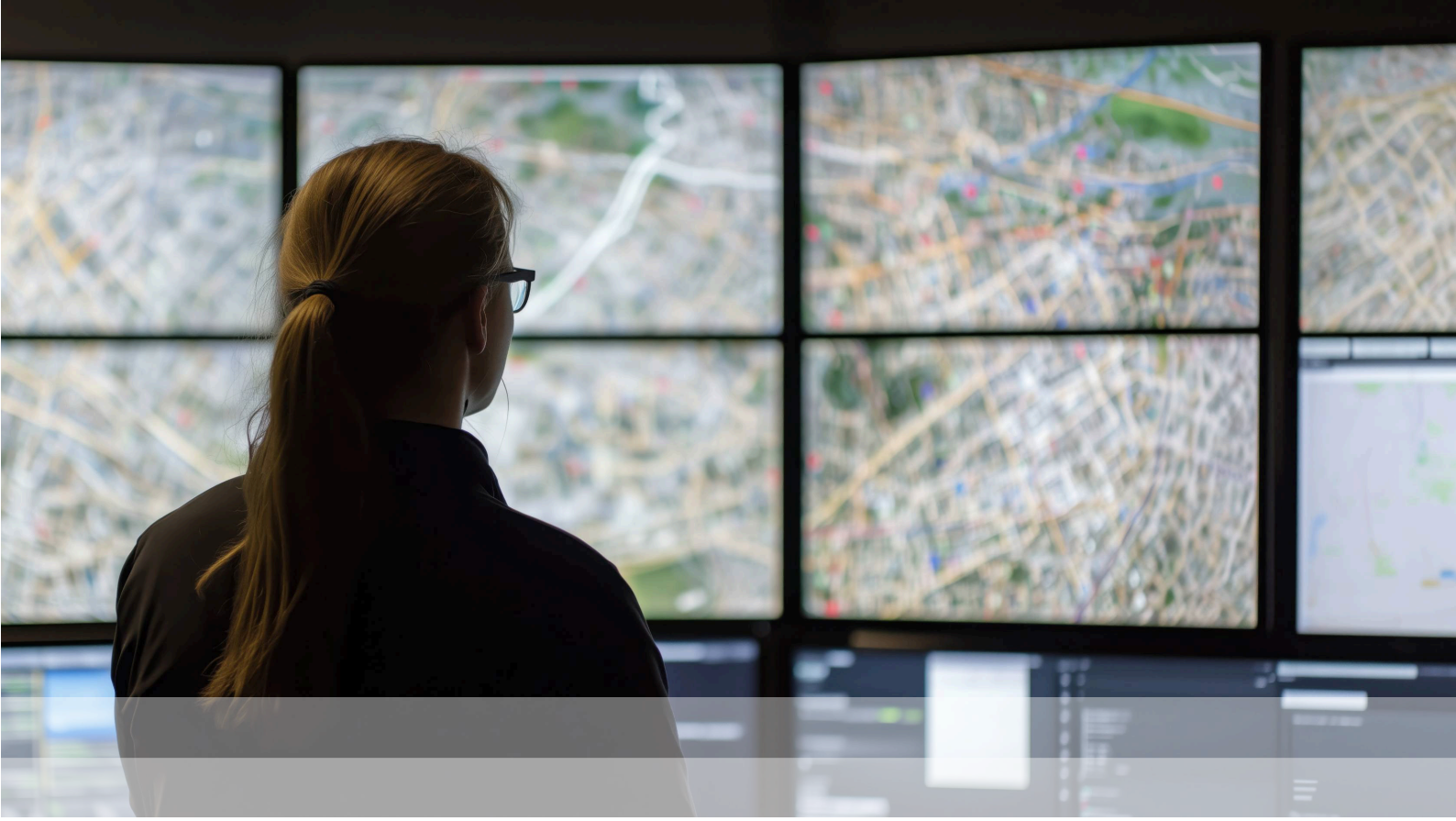
- Train management and supervisors to understand and champion cyber resilience.
- Train compliance teams to understand and monitor eventual legal cyber resilience obligations of your business.
- Train procurement and technical staff on how to assess vendors' compliance with relevant law and CE marking implications.
- Set in place dedicated re- and upskilling programmes, incl. refresher trainings, for all cybersecurity roles within your company. ENISA's European Cybersecurity Skills Framework can help defining curricula for different worker groups.
- Run tailored cybersecurity awareness programs specific to the different functions in your business.
- Create and maintain a cybersecurity culture of shared responsibility within the entire company:
  - Screen, monitor and audit all personnel in an appropriate way.
  - Provide regular mandatory cybersecurity hygiene training among all staff members including regular stress tests, product training (if necessary) and after-action reviews.
  - Set in place rules and procedures which, if implemented as instructed, will mitigate cybersecurity risks - for example for:
    - Accessing internet platform and public websites (e.g. white lists of platforms and websites).
    - Data privacy and permissions for accessing data.
    - Email, password, USB, general-purpose AI and cloud platform policies.
    - Software updates and anti malware measures.
    - Internal and external reporting lines and rules in case of a suspicion or incident.
- Build co-operative frameworks between stakeholders along the security chain, including joint coordination, preparedness plans and exercises for the case of a cyber incident.

FOR YOUR CUSTOMERS

- Get an understanding of legal cybersecurity requirements applying to your client's business operations.
- Conduct a cybersecurity risk assessment and make your customers aware of cybersecurity risks.
- Request an updated inventory of IT and OT components of the client that are connected to your infrastructure, with documented cybersecurity features, risks and vendor contact details.
- Agree on activities,controls, mutual responsibilities, joint stress tests and business continuity plans to manage the risks.
- Ensure that these responsibilities are sustained throughout the lifetime of the solution, e.g. by a service agreement.
- Assign information security tasks to one or more dedicated staff members.
- Update contact records on a frequent basis.
- Regularly review cybersecurity strategies and requirements.
- Train customer personnel.
- Set in place joint back-up procedure.

	PRODUCT	PROJECT DESIGN	INSTALLATION & MAINTENANCE
DESCRIPTION	The product is the combination of hardware and software elements that build an electronic device and constitutes a building block of the system. The product is subject to the European rules for placing on the EU market.	The project design is the selection and location of components such that the resulting system meets the protection objectives and scope of the system (s based on identified risks and known boundary conditions.	Installation refers to both the project installation and commissioning phases. They encompass the implementation of the design, specifically the assembling, mounting and connecting of the relevant system components and the activation and testing of the system according to the design. Maintenance is the combination of preventive and corrective activities during the life of the system, which are intended to retain it in, or restore it to, a state in which it can perform the required function.
RISKS	The cybersecurity risks for a product are usually based on the following cybersecurity threats. An attacker: • gains unauthorized access to a product and this cannot be reported by the product. • discloses confidential data stored or processed in a product or transferred to or from a product. • tampers data stored or processed in a product or transferred to or from a product and his action remains undetected. • gains access to data or exploits vulnerabilities in a functionality of the product that is not required for the intended purpose of a product. • impacts the availability of basic or essential functions of the product during or after an incident, e.g. a denial-of-service attack. • uses the product to negatively impact the availability of services provided by other devices or networks. • exploits known, not fixed vulnerabilities in a product. The inability to update the product, an uninstalled update or the unavailability of a manufacturer patch, combined with known vulnerability/ exploitability, makes this an important attack path in terms of the affected base and ease of vulnerability detection. • exploits a weakness in a product's default configuration, introduced by an individual weak configuration or introduced after it is made available on the market by installing malware. A missing reset functionality prevents restoring to a secure default configuration. • extracts remaining data from a product due to missing possibility to reset the product to its original state (e.g., after disposal of a product). The threats and risks are continuously evolving in time.	Cybersecurity in a safety and/or security project design is to be considered in the context of overall risk management, including information security and operation continuity, and IT strategy. The activities expected to happen and the values expected to be stored in the supervised premises define the most likely cyber-attacks to be protected against and their impact: malicious unsetting of the I&HAS, disclosure of personal, confidential or critical data or denial of service (OT security). Where the project involves connection of the system to a remote server on the cloud (for remote access, remote servicing or alarm transmission), the threats and risks to the IT infrastructure in the cloud and at the service company should be considered (IT security): malicious remote access to the system, disclosure of personal, confidential or critical data stored or transmitted in the IT infrastructure or denial of service of the IT infrastructure.	No new external threats and risks are related to the installation, commissioning and maintenance phases. However, the internal risks of misconfiguration of the products, systems and IT infrastructure and of misapplication of the recommendation for use of the system should be considered.
SOLUTIONS	A majority of the product and software manufacturers have taken a holistic approach to cybersecurity. Starting from a risk-based approach they make their products secure by design and by default and ensure transparency by communicating and making accessible necessary cybersecurity information and by disclosing identified vulnerabilities and delivering updates to their customers. This holistic approach is now considered as state-of-art and will be made legally mandatory by the Cyber Resilience Act as from December 2027. Technical protection mechanisms that allow products to be cyber protected are, for example: • logical access control • authentication • secure update • secure storage • secure communication • logging • deletion • user notification • recovery from incident • network monitoring • traffic control • input validation • attack surface reduction.	Structured project and system design processes begin with a security risk assessment to find and assess the impact of security related threats and vulnerabilities. The project design should then include a cybersecurity framework addressing the identified risks (both at OT and IT levels) and this should be adapted and fit for purpose. It is therefore essential to understand the customer's security objectives and requirements. The system design should also include the optimal and coherent application and setting of the technical protection mechanisms provided by the products and described in the manufacturer's documentation. This should include the expected cybersecurity policy and competence of the occupants of the supervised premises. The IT infrastructure (cloud and service company) should apply the best practices for IT security.	During the installation phase, all cybersecurity hardening guidelines defined in the Project Design including the ones provided by the product manufacturers are to be implemented. This includes changing default passwords, system access credentials and user accounts to fit to the customer's operations, both on the system itself and on the IT infrastructure. Furthermore, all devices connected to the security network need to be configured to reduce potential vulnerabilities. Configuration options include defining applications to install, activating or deactivating settings, and setting up user and system accounts as well as setting access rights, and the use of encryption. The recommendations for a cyber secure operation of the system should be clearly communicated to the users of the system and the occupants of the supervised premises. The cybersecurity updates should be installed as soon as they are available, should it be done by the product manufacturer, the service company or the remote access infrastructure service provider. Periodical maintenance of the system should verify that the products, the system and the IT infrastructure are up to date.

	MONITORING	ALARM RESPONSE
DESCRIPTION	Monitoring services are guaranteed by technical and/or alarm response support services in an Alarm Receiving Centre (ARC). The former handles system deficiencies and determines a technical response and maintenance, while the latter receives, identifies and handles an incoming alarm.	Alarm response follows up on a positive remote alarm/incident evaluation. In this case, an ARC may notify the customer, a mobile patrol and/or law enforcement for alarm response, potentially with on-site support.
RISKS	Hackers can get access to connected IT and OT. In lateral movements, they don't stop with one attack but move from one initial access point through other systems, infiltrating and staying in the entire IT and OT infrastructure, often remaining undetected. This can compromise data privacy, technical and alarm response, endangering assets, information, personnel, and the entire business continuity of the ARC.	Risks depend on the nature of the alarm response. In principle, all alarm data and verification, communication, CCTV and access control can get hacked, manipulated, leaked and disabled. This can compromise data privacy and the integrity of alarm response. Through lateral movements from one initial access point through other systems, hackers can infiltrate and stay in the entire IT and OT infrastructure, often remaining undetected. Such attacks endanger assets, information, personnel, and the entire business continuity of the ARC.
SOLUTIONS	Restrict physical access to all connected devices and applications, log and monitor activities to detect unusual behavior. Business continuity plans, incl. breach detection and containment, backup management, recovery and crisis management. Check regularly current threat landscape and adequacy of cybersecurity status. OT / HARDWARE (incl. operating, communication, CCTV, alarm and access control systems) • Certified and compliant with the latest standards and legislation. • Monitor that all (own & client's) connected applications and hardware are maintained and up-to-date with the manufacturer's security and anti-virus updates, applicable product updates, end-of-life notices and vulnerability notifications. • Place internet-facing devices in an isolated network, not the main company network, and let them only communicate with "white-listed" systems. • Disable USB ports on all devices where possible • Decommissioning of technical obsolescence IT / SOFTWARE • IT infrastructure certified and compliant with the latest standards and legislation. • Regular inventory of authorised software applications running on network connected security devices. • Monitor that all (own & client's) connected applications and hardware are maintained and up-to-date with the developer's security and anti-virus updates, applicable product updates, end-of-life notices and vulnerability notifications. • Password protected, based on password policy • Configure specific firewall rules, and deny all unauthorized traffic • Security and alarm transmission system event logs • Cybersecurity checks before and after updates, assess applicability & impact of changes with respect to system design objectives	Restrict physical access to all connected devices and applications, log and monitor activities to detect unusual behavior. Business continuity plans, incl. breach detection and containment, backup management, recovery and crisis management. OT / HARDWARE (incl. operating, communication, CCTV, alarm and access control systems) • Certified and compliant with the latest standards and legislation. • Regular checks that all (own & client's) connected applications and hardware are maintained and up-to-date with the manufacturer's security and anti-virus updates. • Place internet-facing devices in an isolated network, not the main company network, and let them only communicate with "white-listed" systems. • Disable USB ports on all devices where possible • Decommissioning of technical obsolescence IT / SOFTWARE • IT infrastructure certified and compliant with the latest standards and legislation. • Regular checks that all (own & client's) connected applications and software are up-to-date with the developer's security and anti-virus updates. • Password protected, based on password policy • Configure specific firewall rules, and deny all unauthorized traffic • Resilient and secure operating, communication and access control systems (GPS-steered, time-limited codes) across the entire security chain • Decommissioning of technical obsolescence • Cybersecurity checks before and after updates, assess applicability & impact of changes with respect to system design objectives



REGULATORY OVERVIEW

NIS2 Directive (EU) 2022/2555

The NIS2 Directive sets cybersecurity requirements for operators of Critical Infrastructure that are identified as essential and important entities. It imposes mandatory risk management, incident reporting, and governance obligations, requiring companies to implement technical, operational, and organizational cybersecurity measures, including supply chain risk management. The Directive takes a supply chain security approach and is therefore also important for security system and service providers to essential and important entities. EU Member States had to transpose NIS2 into national law by 17 October 2024.

EU Cyber Resilience Act (CRA) 2024/2847

The Cyber Resilience Act (CRA) imposes mandatory cybersecurity requirements for the providers of products with data connection to a device or network, including alarm systems, IoT sensors, and remote monitoring software. Providers must implement security-by-design principles, conduct risk assessments, and provide for free security updates and vulnerability disclosures for the product's lifecycle. Multiple security products (such as access control, cameras and alarm systems for residential settings) are classified as "Important Products" for which manufacturers must comply with stricter conformity assessment procedures. The CRA will apply as of December 2027. Requirements for the reporting of actively exploited vulnerabilities apply however already as of September 2026.

The EU is considering further changes and simplification to its cybersecurity framework, notably regarding cybersecurity incident reporting; the proposal is currently under negotiation and has not been adopted by August 2026.

EU Cybersecurity Act 2019/881

The Cybersecurity Act establishes a voluntary EU cybersecurity certification framework for ICT products, services, and processes, managed by ENISA. Though not mandatory, the act encourages adoption of EU-wide certification schemes to demonstrate compliance with security standards. The scheme for ICT products (so-called Common Criteria, EUCC) is available.
By opting for certified products, users and integrators strengthen their supply chain assurance and may more easily demonstrate due diligence under NIS2 or CRA audits. As of 2025, a scheme for cloud services is under development. Other schemes are planned for 5G communications and managed security services. A revision of the CSA was proposed in 2026 to adapt it to new regulatory environments and business needs in times of increased cybersecurity threats, incl. transparency and simplification of product certification processes and maintenance of European individual cybersecurity skills attestation schemes developed by ENISA. It also addresses the possibility of a third country posing cybersecurity concerns to ICT supply chains, e.g. through future lists of high-risk suppliers and other risk management measures.

Other relevant EU legislation

The GDPR requires data controllers and processors to implement appropriate technical and organizational measures to protect personal data, including against cyber threats (Art. 32), with potential fines for breaches.

The Radio Equipment Directive (RED) mandates that connected radio devices - like alarms systems and sensors - must include safeguards to protect networks, personal data, and user privacy (applies as of August 2025 and is expected to be repealed when CRA starts applying).

The EU AI Act requires providers and users of high-risk AI systems (e.g. biometric identification, critical infrastructure management) to implement cyberresilience measures and prevent manipulation or exploitation of vulnerabilities (applies as of December 2027 or August 2028, depending on the system or use case).

WHERE TO FIND MORE INFORMATION IN YOUR COUNTRY

Austria	A-SIT Center for Information Technology Security www.onlinesicherheit.gv.at
Belgium	Centre for Cybersecurity Belgium www.ccb.belgium.be
Bulgaria	National Center for Incident Response in Information Security www.govcert.bg
Croatia	Information Systems Security Bureau www.zsis.hr
Cyprus	Digital Security Authority www.dsa.cy
Czech Republic	National Cybersecurity Center www.govcert.cz
Denmark	Danish Resilience Agency www.samsik.dk
Estonia	Information System Authority www.ria.ee
Finland	National Cybersecurity Centre www.kyberturvallisuuskeskus.fi
France	National Agency for the Security of IT Systems www.ssi.gouv.fr
Germany	Federal Agency for IT Security www.bsi.bund.de
Hungary	National Cyber Defence Institute www.nki.gov.hu
Ireland	National Cybersecurity Centre www.ncsc.gov.ie
Italy	National Cybersecurity Agency www.acn.gov.it
Latvia	National Cybersecurity Centre www.mod.gov.lv/lv/kiberdrosiba
Lithuania	National Cybersecurity Centre www.nksc.lt
Luxembourg	House of Cybersecurity www.lhc.lu
Malta	Digital Innovation Authority www.mdia.gov.mt
Norway	National Security Authority www.nsm.no
Poland	CERT Polska www.cert.pl
Portugal	National Cybersecurity Centre www.cncs.gov.pt
Romania	National Cybersecurity Directorate www.dnsc.ro
Slovakia	National Cybersecurity Centre www.nbu.gov.sk
Slovenia	Agency for Communication Networks and Service www.akos-rs.si
Spain	National Cybersecurity Institute www.incibe.es
Sweden	National Cybersecurity Centre www.ncsc.se
Switzerland	National Cybersecurity Centre www.ncsc.admin.ch
The Netherlands	National Cybersecurity Centre www.ncsc.nl
United Kingdom	National Cybersecurity Centre www.ncsc.gov.uk

LIST OF CYBERSECURITY GUIDELINES AND STANDARDS

SECURITY OF IT SYSTEMS

ISO/IEC 27000 series: Information security, cybersecurity and privacy protection
This series of standards makes a set of 100 good practice guidelines for managing the risks affecting or involving business, commercial, national and personal information. It enhances the confidentiality, integrity and/or availability of the information content of IT systems, networks and services.
Information, FAQ and forum about this series can be found at the following address: https://www.iso27001security.com

SECURITY OF PRODUCTS AND OT SYSTEMS

IEC 62443 series: Industrial communication networks - Network and system security
This series of standards addresses security for operational technology (OT) in automation and control systems. The series is divided into different sections and describes both technical and process-related aspects of automation and control systems security. Its provisions are also suitable to protect electronic fire safety and electronic physical security systems.
Further description can be found at the following address: https://en.wikipedia.org/wiki/IEC_62443

ETSI EN 303 645: Cyber Security for Consumer Internet of Things: Baseline Requirements
This standard provides a set of baseline requirements for security in consumer Internet of Things (IoT) devices. It contains technical controls and organizational policies for developers and manufacturers of Internet-connected consumer devices. This standard can be downloaded for free here.

EN 18031 series: Common security requirements for radio equipment
This series of standards, published by the CEN and CENELEC, outlines essential information security requirements for radio-based devices and systems. By aligning with the Radio Equipment Directive (2014/53/EU) and its accompanying Delegated Act, these standards support manufacturers and stakeholders in maintaining compliance and consistency across European markets. They also establish common testing protocols, performance criteria, and security guidelines, thereby aiding cross-border interoperability and addressing evolving industry needs.

STANDARDS SUPPORTING THE CYBER RESILIENCE ACT (CRA, (EU) 2024-2847)

Many new standards are currently in preparation by CEN, CENELEC and ETSI to help manufacturers designing, manufacturing and maintaining digital products (hardware products and software products) that comply with the essential requirements of the CRA. The most relevant works in progress for fire safety and physical security systems are the following:

prEN 40000-1 series: horizontal standards and guidelines covering the threats and security objectives, the principles for cyber resilience, generic security requirements and vulnerability handling.

prEN 62443-4-x: vertical standard covering the essential requirements of the CRA for OT systems and based on the existing other parts of the IEC 62443 series.

prEN ETSI 304 632: Essential cybersecurity requirements for smart home products with security functionalities. This vertical standard is intended to cover the products that be long to the category of important products class I, Smart home products with security functionalities.

prEN 4000-10: Cybersecurity essential requirements for products with digital elements used in identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers. This vertical standard is intended to cover the products that belong to the category of important products class I , Identity management systems and privileged access management software and hardware.

ABOUT EURALARM

Euralarm represents the fire safety and security industry, providing leadership and expertise for industry, market, policy makers and standards bodies. Our members make society safer and secure through systems and services for fire detection and extinguishing, intrusion detection, access control, video monitoring, alarm transmission and alarm receiving centres.

Founded in 1970, Euralarm represents over 5 000 companies, employing 700 000 people, within the fire safety and security industry with an estimated revenue of € 67 billion. Euralarm members are national associations and individual companies from across Europe.

Euralarm
Gubelstrasse 11
CH 6300 Zug
Switzerland

E-mail: info@euralarm.org
Website: euralarm.org

ABOUT CoESS

CoESS acts as the voice of the Security Industry. The main objective of CoESS is to represent and support the growth of an industry that delivers solutions of high quality and professionalism, focused on the selection and development of qualified staff and technology. The core values of CoESS are Quality, Safety, Compliance and Trust. It is the umbrella organization for 23 national private security employers' associations, of which 17 in EU Member States. CoESS is recognised by the European Commission as a European sectoral social partner and is active in a constructive Social Dialogue with UNI Europa.

Confederation of European Security Services (CoESS)
avenue des Arts 56 | Kunstlaan 56
B-1000 Bruxelles-Brussel
Belgium

E-mail: info@coess.eu
Website: coess.eu