EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

FRA Security Strategy

Physical and IT Security

12 December 2024

Table of content

Introduction

In light of the rapidly evolving environment and emerging security threats, the Agency should implement a security strategy that addresses both physical and IT security areas, including measures to safeguard cybersecurity.

This holistic approach ensures that security is integrated in everyday operations, allowing the Agency to mitigate risks and respond effectively to potential threats.

This strategy aims to safeguard the integrity and functionality of the Agency's operations by protecting its people and assets within the Agency premises, and by securing the digital infrastructure against cyber threats, unauthorised access, and data breaches.

This strategy outlines the objectives, roles, and responsibilities for implementing and maintaining security.

1 Physical Security

Physical security involves measures and controls to protect an organisation's personnel, facilities, and assets from physical threats. This includes activities and tools aimed at preventing unauthorised access, security threats and natural disasters, and ensuring the safety and security of the premises and people.

The next sections describe the objectives, roles and responsibilities of the involved actors, actions, and communication aspects as well the underlying organisational processes and policies.

1.1 Objectives

The main objectives of the Security Strategy are:

Ensure the safety of all personnel, visitors, and assets within the Agency premises: This involves employing trained security staff to conduct checks on staff and visitors, installing surveillance systems to monitor activity outside the perimeter of the premises, and establishing controlled access points to limit entry to authorised staff only.

Prevent unauthorised access to sensitive areas: Implement multi-layered security controls such as scanners and keycard access to restrict entry in areas within the premises. Access control reviews ensure that only those with appropriate clearance can enter secure zones like the office spaces where employees are located, IT datacentre, etc.

Mitigate risks of physical threats and natural disasters: This includes the installation of locking mechanisms, alarm systems, outside lighting to deter criminal activity, and motion detectors. Additionally, having emergency response plans and conducting regular drills to help minimise the impact of emergency evacuations due to fire and other unforeseen events.

1.2 Key Principles

The key principles guiding the overall physical security are around prevention, detection, responding to incidents and remedy actions:

- Prevention: Implement proactive measures such as visible security presence, assessments of security controls, staff awareness information sessions and evacuation exercises.
- Detection: Use of surveillance and monitoring technologies such as motion sensors, real-time CCTV, and intrusion detection systems to quickly identify breaches while ensuring compliance with data protection requirements.
- Response: Establish action plans with clear roles, communication strategies, and predefined responses for various security and data breaches. Organise training to ensure that all involved actors and staff maintain adequate readiness levels.
- Remedy: Plan to restore normal operations swiftly using backup systems, incident analysis, and support affected operations.

1.3 Roles and Responsibilities

The following roles and responsibilities are required:

- Facilities Officer: Ensures that security measures, processes, and policies are integrated into building maintenance and operations.
- Security Manager: Oversees the implementation and management of physical security protocols and informs management on security-related matters.
- Security Guards: Conduct security checks when individuals enter the premises, conduct regular patrols, monitor surveillance systems, and respond to security incidents.
- All staff: Adhere to security policies and report any suspicious activity.
- Director: Responsible for the governance of physical security systems within the Agency. The Director is supported by the Head of Administration and other relevant staff, as required.

1.4 Actions linked to objectives

The following list presents an overview of the foreseen actions to address the defined objectives in terms of physical security.

- Install a surveillance system for peripheral protection and motion detectors in the building while adhering to the applicable regulations. Ensure coverage of entry/exit points and restricted locations. Regularly maintain equipment for optimal performance.
- Implement access control systems by utilising ID badges to ensure secure access to authorised staff. It is essential that access logs are checked and reviewed when required and that are not used longer than required.
- Strengthen physical security with appropriate security doors and locks. Ensure that these physical barriers are regularly checked for proper operation which is to prevent unauthorised access in the premises.
- Regularly audit security risks to identify and fix vulnerabilities. Scheduled maintenance of equipment and of the employed control mechanisms to ensure their effectiveness. Identifying weaknesses and taking corrective actions are crucial. External consultants may provide unbiased evaluations.
- Develop emergency response plans and conduct regular drills. Create emergency response plans that describe procedures for various situations, such as fire, natural disasters, and security breaches. Clearly specify the roles and responsibilities of all staff members during such emergencies. Conduct regular drills and training sessions to ensure employees are familiar with the processes and can respond effectively in actual situations.

1.5 Related organisational policies and processes

To meet the requirements of the physical security objectives and actions, the following organisational policies and processes are in place.

- Building security policy
- Video Surveillance policy
- Crisis management policy

- Facilities management process

2 IT security

The protection of the Agency's digital assets is of critical importance. The IT Security section of the present security strategy lays out the approach to safeguarding the Agency's information systems and data.

By implementing IT and network security measures, ensuring the confidentiality, integrity, and availability of information, and complying with relevant data protection, information security and cybersecurity regulations, the Agency endeavours to establish a robust defence against cyber threats.

This section outlines the objectives, roles, responsibilities, and key principles of the Agency's IT security strategy, highlighting the actions needed, and the underlying organisational policies and processes to secure the digital assets of the Agency.

2.1 Objectives

Apply security controls in an efficient and proportional manner, and guarantee adequate protection of personal data in accordance with the data protection regulation as well the rules on the exchange of EU classified information:

- All Agency data and systems must have security controls to protect confidentiality, integrity, and availability.
- Internet-facing systems need stringent controls due to their exposure to threats and the potential damage from compromises.
- Sensitive non-classified data and their systems require strict protection, with additional controls for personal data as needed.

Identify assets, and assess and manage risks and opportunities:

- The threat landscape is constantly evolving, with new threats potentially emerging due to various actions or events. Actions such as adopting new technology or developing new systems may introduce previously non-existent threats. Similarly, external events can create situations where new threats or threat actors arise.
  The adoption of new technology should always be preceded by a security assessment and data protection impact assessment.
- Maintaining an up-to-date inventory of resources, documentation, hardware and software assets, along with a security risk management process, is essential. This ensures that assets are accounted for, risks are assessed, responses to risks are identified and approved, and actions are monitored and implemented according to plans.
- Monitor and take appropriate actions: The Agency shall proactively monitor indicators of compromise (e.g. network logs indicating a potential issue), and notifications received from CERT-EU and other trusted third parties. The Agency shall take proactive and reactive actions that it considers necessary to mitigate or avoid security risks.

Raise awareness:

- All users with access to Agency data or systems shall receive information and relevant updates on security including calls for action, cybersecurity awareness, and relevant policies and procedures.

2.2 Key Principles

The key principles guiding the overall IT security are:

- Layer security approach: Implement multiple security layers to protect digital assets. If one layer is breached, others remain intact. Layers include physical security, network controls, application practices, and data protocols, reducing the risk of a successful IT security attack.
- Continuous Monitoring: Use automated tools for ongoing surveillance of networks and systems. This approach detects potential incidents early, allowing swift responses. Monitoring includes analysing network traffic, system logs, user activities, and other data to identify threats in real-time.
- Engage in active collaboration with the Cybersecurity Emergency Response Team (CERT-EU) and related Commission services, closely following and implementing their recommendations.
- Risk Management involves identifying, assessing, and prioritising risks to mitigate their impact. This includes analysing potential threats, evaluating their impact and likelihood, and then prioritising and addressing the most critical vulnerabilities.

2.3 Roles and Responsibilities

- Local Cybersecurity Officer: Oversees the IT security provisions and their execution.
- IT Security Team: Implements and manages security technologies and processes.
- All staff: Adhere to security policies and report any suspicious activity.
- Director: She/he has the overall responsible for the governance of information systems security within the Agency. The Director is supported by the Head of Administration and other relevant staff, as required.

2.4 Actions linked to objectives

The following list presents an overview of the foreseen actions to address the defined objectives in terms of IT security.

- Set up firewalls, intrusion detection and prevention systems, and antivirus software. Ensure that these security measures are properly configured to protect against a wide range of cyber threats.
- Regularly update and patch software to protect against vulnerabilities. Promptly apply updates to operating systems, applications, and firmware. Keeping software up to date is critical in protecting against known exploits and reducing the attack surface.
- Utilise the CERT-EU as well as external services and conduct security assessments and penetration testing. Perform scheduled internal and external security assessments to identify weaknesses in the IT infrastructure. Use the findings to remediate vulnerabilities and strengthen cyber defence controls.
- Use strong authentication methods, like multi-factor authentication, to reduce the risk of unauthorised access even if passwords are compromised.
- Use strong encryption protocols for encrypting sensitive data both during transmission across networks and when storing it on devices or servers. Comply with the rules for handling EU classified information when dealing with EU restricted data.

- Raise awareness amongst end users through information sessions and keep them informed of any ongoing cyber threats.

2.5 Related organisational policies and processes

To meet the requirements of the IT strategy's objectives and actions, the following organisational policies and processes are in place.

- ICT policy
- Digital Services steering committee policy
- ICT Security and data management policy
- Crisis management policy
- Data breach policy
- Business Continuity Policy
- Rules on the exchange of EU classified information

3 Communication with stakeholders

Keep staff informed about physical and IT security policies and updates through intranet, newsletters, emails, and briefings. Ensure that these updates are clear and understandable, emphasising adherence to security protocols and the role each employee has in protecting Agency's assets. Providing current information ensures awareness and compliance.

Establishing and maintaining communication channels with local law enforcement services (fire brigade, police, etc.) and Commission services is crucial. Meetings and collaborative exercises (drills, assessments, etc.) are essential for enhancing understanding and preparedness for various security threats. Such communication ensures a swift and effective response to any incidents that may arise.

Regularly participate in meetings, conferences, and forums to share knowledge, discuss best practices, and stay informed about the latest updates especially from CERT-EU and Commission services.

Conclusions

The Agency implements physical and IT security measures as described in its policies and processes, which are periodically updated and audited by Commission services.

By raising staff awareness, maintaining systems, staying updated on IT advancements, and applying recommended cybersecurity controls, the Agency aims to uphold high security standards and to comply with data protection, cybersecurity and other regulatory requirements.

The overall goal is to ensure a secure environment that supports the Agency's business and protects its assets.

END OF DOCUMENT