Annex XII (EMA/2019/12/DED)

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

21 September 2015
EMA/530488/2014

Executive Director

Security Policy

POLICY/0076

Status: Public
Effective date:
Review date:
Supersedes: Several ISERV and IT policy039

Table of contents

30 Churchill Place ● Canary Wharf ● London E14 5EU ● United Kingdom
Telephone +44 (0)20 3660 6000 **Facsimile** +44 (0)20 3660 5555
Send a question via our website www.ema.europa.eu/contact

1. Introduction and purpose

The European Medicines Agency has a responsibility for the effective management of security in relation to: people working at its premises, stakeholders, information held, and property. The Agency takes a layered approach to security management, with physical and procedural measures complementing each other to mitigate security risks.

Security is everyone's responsibility, and a prime responsibility of all levels of management, and it is expected everyone to contribute towards achieving the Agency's overall security objectives. This policy describes the European Medicines Agency's strategic approach and commitment to the management of security risks. The Agency will encourage initiative and adopt best practice in a culture where employees and managers are aware of their individual security responsibilities and are actively engaged and committed to improving standards of security.

2. Scope

This policy applies to all staff members, delegates, contractors, visitors and other authorised persons working within the premises of the Agency without exception.

3. Policy Statement

The Agency's security objective is to ensure the confidentiality, integrity and availability of its information systems and the safety of its staff and assets. It's also to ensure the continuity of its core tasks and minimise business damage by reducing the likelihood and minimising the impact of security incidents.

The Agency will achieve this by:

- continual and effective improvement of security performance;
- compliance with all applicable legislation, Agency's requirements and any other adopted requirements, in particular all security systems should not be excessive and the should not violate the rights of individuals to data protection and privacy;
- the setting and review of security objectives and targets to reduce risks to acceptable levels. determining criteria for accepting risks and identify the acceptable levels of risk;
- review of the security policy and procedures to ensure their suitability, adequacy and effectiveness;
- provision of suitable and sufficient security information, instruction and training to enable all staff to carry out their jobs competently and comply with requirements of the security policy;

- selection and monitoring of competent third parties to ensure appropriate standards of security are achieved;
- effective communication and cooperation with stakeholders so they are aware of our security expectations;
- provision of adequate and appropriate resources to implement this policy and to ensure it is properly communicated and understood.
- review of the security policy and procedures to ensure their suitability, adequacy and effectiveness;

4. Roles and Responsibilities

Executive Director and/or Deputy Executive Director

Security at the Agency comes within the task of the Executive Director and/or Deputy Executive Director as part of the day to day activities (Regulation (EC) No 726/2004, article 64.2(a)).

Data Protection Officer

- Ensures in an independent manner the internal application of the provisions of data protection legislation
- Advises the controllers on matters concerning the application of data protection provisions.
- Keeps a register of all personal data processing operations and responds to requests from the EDPS

Chief Policy Adviser

- Preparation for, implementation and monitoring of new legislation and revision of existing legislation;
- Preparation, implementation and monitoring of new policies and revision of existing policies;
- Management of emerging events with policy, political, reputational consequences for the EMA, or important public health impact (crisis management);
- Liaising with and coordination of EMA interactions with the EU Institutions.

Heads of Division, Heads of Department and Heads of Service

- Are responsible and will be consulted on all matters relating to policies and procedures and are responsible for promoting adoption within their respective areas of operation.
- Ensuring that all staff are aware of their security responsibilities and receive appropriate security guidance and training relevant to their job role.

Data Controllers

- Must understand the value of the data and are therefore responsible for specifying, implementing and monitoring safeguards to protect the confidentiality, integrity and availability of the information throughout its lifecycle. This includes establishing controls which manage the creation, storage, access, distribution, amendment, copying, archiving and disposal of information.

Security Officers

- Advise Agency users and others working with the Agency on matters of information and physical security.
- Shall monitor the implementation of the Agency Security Policy, approved by the Executive Director.
- Shall advice and report to his/her Line managers, the system and data owners, IT Program and project leaders on information systems security matters
- Shall collaborate with the Agency's Data Protection Officer

Users

- Must ensure compliance with this policy and be responsible for his/her activities.
- Must report any violations of this policy to the security teams – Security office and IT service desk.
- All authorised Users who have access to information are required to keep the information secure to the level required by the Data Controller

5. Security Systems

The section below lists the Agency security systems. These are described in a succinct way for the purposes of this document however further details with specific controls and procedures are described in relevant annexes.

In exceptional circumstances and for investigation purposes only and to substantiate allegations of criminal activity, gross misconduct or failure to comply with legal duties, a request can be made for the transfer of personal data, the request must be clear, defined and should be carried out in compliance with the principles and limits of Regulation (EC) 45/2001 and the rules established for the conduct of administrative enquires.

5.1. Man guarding

The Agency employs the services of an external man-guarding company to ensure a twenty four hour supervision of staff and visitors, and to patrol its premises.

5.2. Access control

The Agency uses an automated access control system (AACS) to ensure that EMA occupied areas, sensitive areas and assets are only accessibly to those with a legitimate business need. Specific sub-policies have been written defining the access privileges to be granted to specific user groups including Agency staff, delegates and contractors.

5.3. CCTV

For the safety and security of its building, assets, staff and visitors, the European Medicines Agency operates a video-surveillance system to protect the personal data, privacy and other fundamental rights and legitimate interests of those caught on camera.

5.4. Mail

All mail addressed to the EMA is delivered and security scanned. These items are then collected and brought to the Mailroom. Physical courier mail received by the Agency is registered centrally by its mail services. All mail is then registered on a decentralised basis by one of its Divisions/Departments/Services or Offices if it contains information which may involve action, follow-up or commitment by the Agency. Outgoing mail drawn up within the Agency is registered on a decentralised basis by the originating Division/Department/Service or Office.

5.5. Secure Print

Users send prints to multi-functional devices (MFDs) using the secure print 'Follow Me' driver and can only be accessed by the person printing the document using their personal access control card.

5.6. Confidential waste

Confidential waste disposal of paper and electronic records such as CDs, and disposed of by the confidential waste contractor and the Agency receives certificates of confidential destruction after collection.

5.7. Archives

Paper and electronic records (portable data storage devices) are stored at a secure off-site storage facility. The movements of archived documents and content description are tracked and recorded in the Agency's archives systems. Only named staff can retrieve and manage archived documents from the offsite storage.

5.8. Computer Accounts

The access to the Agency's IT systems is provided through personal accounts, which are non-transferable and unique. Shared accounts should be avoided due to their lower security and lack of accountability.

5.9. Authentication

Protecting access to IT resources is vital to ensure that systems remain secure. The Agency may offer different options to access IT resources such as password, tokens, smart cards or combination of two (two-factor authentication). All users must remain vigilant in guarding access to the Agency's resources and protecting them from threats inside and outside the Agency.

5.10. Databases and Applications control

Access to a data in e.g. Databases, folders, Exchange Public folders, and any type of electronic data can be requested by submitting a request to the IT Service Desk (there are however exceptional cases where access can be requested directly to the Data owner/Business Administrator, e.g. SIAMED). Access will automatically be removed as well immediately when an EMA user has left the Agency.

5.11. Email and Internet Services

The use of the IT equipment of EMA, in particular the e-mail services and Internet access, is in principle restricted to official use. However, a limited use of the e-mail and Internet services of EMA for

personal use is permitted as long as such utilisation is not contrary to the interests of EMA and the European Union and remains within reasonable limits.

5.11.1. Monitoring internet activities

Monitoring is used to protect the security of the IT Infrastructure against network-oriented internal and external threats (viruses, malicious software, etc.). Internet activities is collected and generally used only for security and capacity management purposes.

The internet must not be used for purposes which are illegal, unethical or harmful to the Agency.

5.12. Information Classification and Handling

This policy is consistent with the notion that information must be protected according to its sensitivity, criticality, and value. The Agency data classification scheme must be followed and enforced for every new Data or document created. All restricted or confidential data or information held on an external storage device or portable device must be encrypted using an Agency approved method.

5.13. Incident Response and Handling

It is critically important to respond quickly and efficiently when security breaches occur. The Agency primary focus is to ensure that all security incidents are handled in a structured and consistent manner.

5.14. Bring your own Device (BYOD)

Although employees may, at their own expense, be using personal devices to carry out their duties, to process organisational information and to access the Agency network. BYOD rules must be defined for the proper use of BYOD devices at the Agency in order to protect the confidentiality, integrity and the availability of services and the Agency's sensitive data.

5.15. Use of Cloud Services

Cloud computing is an alternative way of delivering computing resources and services. As such, this policy would apply to the use of these services (e.g. Dropbox, google drive, skydrive, icloud, amazon cloud services). Only Services that have been assessed and approved by IT can be used for EMA data. If there is a new business requirement that requires the use of cloud services, it should be treated as any other IT project at the Agency.

6. Systems Testing

The Agency must perform regular systems testing (Penetration testing, vulnerability testing, risk assessments and "sweeps" – technical surveillance counter measures (TSCM)) to evaluate the effectiveness of the security control and to identify any vulnerability, weakness or system misconfiguration.

7. Compliance

Failure to comply with this policy and its annexes may result in a security breach which in turn may lead to disciplinary or legal action by the Agency in line with the provisions of the Staff Regulation.

8. Awareness and Communication

Security awareness improves security and user behaviour. An awareness program should be created to inform and educate users on the security policy of the Agency.

9. Reporting

If sensitive information is lost, disclosed to unauthorised parties, or suspected of either, or any unauthorised use of the Agency's information systems has taken place or suspected of taking place notify the security teams – Security office or IT service desk.

10. Related documents

This Security Policy is supported by appropriate procedures/standards/rules/manuals that are documented under:

ISERV Security annexes folder: https://docs.eudra.org/webtop/drl/objectId/0b0142b2830ee793

IT Security annexes folder: https://docs.eudra.org/webtop/drl/objectId/0b0142b2830ee794

11. Changes since last revision

n/a

London,

Andreas Pott

Deputy Executive Director