24 March 2025
Executive Director
EMA/553746/2024

Policy on Identity and Access Management to EMA IT Systems

POLICY/0085
Status: Public
Effective date: 24 March 2025
Review date: 24 March 2028

Supersedes: N/A

1. Introduction and purpose

The purpose of this policy is to establish the rules and framework for managing user access to the Agency's IT systems and data (including records). This policy aims to ensure that access is granted appropriately, monitored continuously and reviewed regularly to protect the Agency's assets and comply with security and regulatory requirements.

2. Scope

This policy applies to all EMA staff members, Seconded National Experts (SNE), trainees, contractor personnel, interims, visiting and collaborating experts, users from the EU regulatory network, users from international organisations and external users who have access to Agency's IT systems and data. This policy outlines the key principles for the provision and de-provisioning of access, user profiling, access review and monitoring, and access request management within EMA.

3. Definitions

EMA staff members	Temporary *a*gents (TA), contract agents (CA)
Internal users	EMA *s*taff members, Seconded National Experts (SNE) and trainees
Interims	Temporary agency workers
Contractor personnel (including consultant)	Contractor means a natural or legal person, including a public entity, or a group of such person with whom the Agency has signed a contract (either directly or indirectly via an employing entity) for the

Official address Domenico Scarlattilaan 6 ● 1083 HS Amsterdam ● The Netherlands
Address for visits and deliveries Refer to www.ema.europa.eu/how-to-find-us
Send us a question Go to www.ema.europa.eu/contact **Telephone** +31 (0)88 781 6000 An agency of the European Union

	supply of products, execution of works, provision of services or supply of immovable property
Visiting experts	An individual who is assigned temporarily by the employing organisation for training (for the person or their organisation), information gathering or exchange of knowledge/best practices with EMA or other purposes within the mandate or remit of the Agency, and is an employee of an EU or non-EU public or academic organisation (e.g. national competent authority, international regulator3, research institutions or international organisations) or a student within such organisations. (see Policy 0083)
Collaborating experts	An individual, who on the basis of acquired expertise/knowledge, has been invited by EMA to perform a specific task within a pre-defined project within EMA's mandate and remit, and is a paid employee from an EU or non-EU, public or academic organisation (e.g. national competent authority, international regulator, research institutions or international organisations), or a post graduate student within such organisations. In exceptional cases, an individual can be invited from outside these organisations. (see Policy 0083)
EU regulatory network users	Members and alternates from EMA's Management Board, scientific committees, working parties and other groups/bodies, users from National Competent Authorities (NCA), users from the European Commission
International organisations' users	Users from third country authorities with whom the EMA has signed a confidentiality arrangement or mutual recognition agreement
External users	Users from industry (applicants, marketing authorisation holders), sponsors of clinical trials, members of the public
Generic account	A generic account is a type of user account that is not assigned to a specific individual but is instead used by multiple users or for a specific purpose
Least privileged	Minimum level of access necessary to perform required functions
Separation of duties	Process of distributing tasks and responsibilities among different individuals to reduce the likelihood of errors and fraud
Privileged accounts	Accounts with higher access levels. They grant elevated access to networks, computer systems or applications, allowing for actions that regular accounts cannot. These accounts can be used not only by individuals but also by applications, services, or software
Role-based access	Access permissions assigned based on the user's role within the organisation's IT systems
Need-to-know	Access to information granted only if it is necessary for the user to perform their job
Unique identifier	Unique sequence of letters and/or numbers assigned to each user by a machine or person, by which it is identified in a single and separate manner from any other user

Reporting officer	Reporting officer of EMA staff members, superiors in the Agency to whom an SNE is assigned, line manager of trainee's mentor or recruiting manager for interims
Operational Initiating Agents	EMA staff members in the divisions/task forces responsible for the respective contracts, given that they closely monitor the implementation of contracts and thus oversee the contractors' work

4. Policy statement

The policy ensures that access to Agency's IT systems and data is granted based on the minimum level of access necessary to perform the required functions based on the user's role, reviewed and monitored on a regular basis and promptly de-provisioned when no longer required. Identities and access shall be managed through a standardised process for access requests, approval and documentation to ensure compliance with security policy and procedures.

4.1. Security Principles

User authentication and validation must be performed before granting users access to Agency's IT systems and data.

Users' identities and accounts cannot be shared among users. Access to the Agency's IT systems and data must not be granted to generic accounts. Any exceptions must be formally justified, appropriately approved and documented.

Processes to identify and manage privileged accounts must be defined and documented.

Processes must be implemented to regularly review user accounts that have been inactive.

Authentication controls for all IT systems and data must be implemented via an automated and centralised system.

Access to the Agency's IT systems and data is restricted and must be granted on the principle of least privilege, based on role, following approval by relevant function or entity. Exceptions can be made on a need-to-know basis and must be recorded.

Access to critical systems and sensitive information must be implemented following the principle of separation of duties. Roles and responsibilities should be segregated to prevent conflicts of interest and minimise the risk of unauthorised or fraudulent activity.

Access management processes must be documented and approved with regards to the creation, modification, monitoring and revocation of access privileges to Agency's IT systems and data.

4.2. Roles and Responsibilities

Reporting Officers[1]

Responsible for assigning the correct role to internal users and interims in accordance with designated job role profile. This process triggers the creation, modification or deletion of accounts as well as requests to access systems and data required to perform their duties.

[1] Reporting officer of EMA staff members, superiors in the Agency to whom an SNE is assigned, line manager of trainee's mentor or recruiting manager for interims.

Operational Initiating Agents

Responsible for assigning the correct roles for contractor personnel and approve requests to access systems and data required to perform their duties in accordance with designated role profile (e.g. as described in contracts).

EMA entity and mentor receiving visiting and collaborating experts

Responsible to define the to be access granted to EMA IT systems to visiting and collaborating experts, in accordance with their assignment.

HR

Responsible for developing and maintaining job role profiles to be adopted across the Agency. HR personnel also collaborate with Reporting Officers to ensure staff members are assigned the appropriate job role profile during the onboarding process.

Information Security Steering Committee (ISSC)

Responsible for overseeing the implementation of the Agency's information security strategy, which aims to protect its information assets. The ISSC ensures that the information security strategy is aligned with the business objectives.

Information Management Division

Responsible for implementing and maintaining access controls and for system monitoring access activities. This includes setting up appropriate tools for user authentication methods, access controls and identity verification processes.

Information Security Advisory Function

Responsible for conducting compliance checks at least annually to ensure full adherence with this policy, related guidelines and processes. The Information Security team must provide ISSC with the results of the validation and compliance checks. The Information Security Advisory Function is also responsible for developing and conducting regular awareness and training sessions to help users stay updated on the latest security threats and best practices for protecting sensitive information, with a view to reduce the risk of data breaches and cyber-attacks.

IT Service Desk

Responsible for creating, modifying and deleting accounts, as well as granting and revocating access. All processes must be thoroughly documented including detailed audit trails, records of access requests, and approval logs to ensure accountability.

Security Operation Centre

Responsible for the continuous monitoring, detection and response to cybersecurity incidents to protect the Agency’s IT systems and data. The SOC must collaborate with the Information Security Advisory Function and Information Management Division during incident investigations.

Users

Responsible for using IT systems appropriately. Users must keep their account details confidential and report any suspicious activities related to their credentials.

4.3. Identity Management

4.3.1. Unique Identifier

Users are assigned a unique username or identifier on the principle of one user/one ID to ensure individual accountability. These cannot be shared between users.

4.3.2. Email Suffixes

Different suffixes in email addresses (e.g., @ext.ema.europa.eu, @ema.europa.eu) are used to distinguish between EMA staff members, SNE, interims, contractor personnel, trainees, visiting experts, collaborating experts, EU regulatory network users, highlighting the differences in their user profiles.

4.3.3. Access Authentication

Users must be positively identified and authenticated before gaining access to IT systems and data. Multifactor authentication is mandatory. All users requesting password resets or changes to authentication credentials must have their identity verified beforehand. Access to IT systems must be blocked if risks are detected on an account.

4.4. Access Management

The IT Service Desk will manage access based on the user's role following approval by relevant functions as described hereafter and summarised in the Annex. Records of access requests, their approval, provisioning and de-provisioning must be maintained for tracking/investigatory purposes.

4.4.1. Access request

Users must submit access requests through the designated identity and access management system. A process for user account provisioning (onboarding) must be defined to clearly indicate the required access and assigned role.

4.4.2. Access approval

While users may access some EMA IT systems without prior authorisation based on legal or business requirements (e.g. EMA's ticketing systems), other systems require approval before being granted access by the IT service desk.

For internal users and interims, role-based access to IT systems and data is granted automatically based on the job role profile designated by their Reporting Officer. Additional permissions require approval from the Reporting Officer. After access has been granted, the Reporting Officer must be informed.

Visiting experts and collaborating experts have reduced access to EMA IT systems based on a need-to-know basis. If required, the receiving EMA entity will decide on the access granted to EMA systems and the access request is handled by the mentor. Access to IT systems and data for contractor personnel is granted after approval from the relevant Operational Initiating Agent, subject to provision of a confidentiality undertaking and declaration of absence of interest.

Access to IT systems and data for members of EMA's Management Board, scientific committees, working parties and other groups/bodies is approved by the relevant secretariat.

Access to IT systems and data for other EU regulatory network users or external users is managed by the appointed representative of each organisation.

Access to IT systems and data for users from international organisations must be approved by the Head of International Affairs in accordance with set agreements and nominations.

4.4.3. Access rights review

Access to IT systems and data is reviewed at least annually, involving relevant functions that grant approval to users.

Processes must be defined and documented so that inactive and dormant accounts are investigated, and appropriate automated or manual action is taken to deactivate these accounts.

4.4.4. Access revocation

Processes for user account de-provisioning (off-boarding) must be defined and implemented so that user's accounts and access are revoked no later than the day after the last day of the user's employment or contract validity with EMA, national competent authority or other organisations, as relevant.

Access to relevant IT systems for members of EMA's Management Board, scientific committees, working parties, and other groups/bodies is revoked no later than the day after the end of the member's mandate from the relevant body.

Usernames or identifiers and authentication credentials of former users must not be reused to prevent unauthorised access and maintain unique identifiers for audit trails.

Exceptions must be formally documented and approved.

4.5. Monitoring and Reporting

Access to IT systems and data is monitored and reported and actions that directly or indirectly affect or could affect the confidentiality, integrity or availability of data are managed via the incident management process, personal data breach notification process[2] and SOP/EMA/0168 for handling unintended disclosure of confidential information to external recipients by EMA staff, as applicable.

4.6. Compliance

Access management practices will comply with the Agency's security policy, regulations, and standards, such as Regulation (EU) No 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions and bodies and offices and agencies and on the free movement of such data and Regulation (EU, Euratom) 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union.

Regular audits (external and/or internal agreed with the Head of Audit) and ex-post controls are required to assess compliance and identify areas for improvement.

Any exceptions to the policy must receive prior approval and documentation from the Information Security Officer and be reported to the ISSC. Any policy violations must be reported to the Information Security Service and subsequently to the ISSC.

[2] Annex I of IGPDP - Personal Data Breach Management [EMA/124596/2020]

4.7. Incident response

Incident management processes are established, requiring each incident to be reported immediately to ensure prompt investigation, mitigation, analysis, and documentation.

Any suspected or confirmed access control breaches must be reported immediately to the IT Service Desk.

If the suspected or confirmed breach includes personal data, the Data Protection Officer and the relevant Data Protection Coordinator must be informed, and the data breach management procedure must be initiated[3].

If the incident has led to the unintended disclosure of confidential information to external recipient(s), SOP/EMA/0168 must be followed.

4.8. Training and awareness

All EMA staff members, Seconded National Experts (SNE), trainees, interims and contractor personnel must receive training on security best practices, including identity and access management, during onboarding and periodically thereafter. Annual information security awareness and training activities will be organised by the Information Security Advisory Function to emphasise the significance of identity and access management and best practices.

5. Related documents

Security Policy (Policy 0076)

Security Incident Management Process - EMA/601652/2020

Internal Guidance on Privileged Access Management - EMA/113063/2023

SOP/EMA/0168 - Handling incidents of unintended disclosure of confidential information to external recipients by EMA staff

Personal Data Breach Notification Form TEMPLATE - EMA/894897/2018

Records Management and Archives policy (Policy 0026)

Policy on visiting and collaborating experts involved in the activities of the European Medicines Agency (Policy 0083)

Regulation - EU - 2023/2841 - EN - EUR-Lex

6. Changes since last revision

New policy

Amsterdam,

[Signature on file]

Emer Cooke

Executive Director

[3] Annex I of IGPDP - Personal Data Breach Management EMA/124596/2020

Annex: Overview of functions involved in the account management approval and reviews

The following table provides an overview of the functions or entities responsible for the approval and review of users' access before these are granted by the IT service desk, whether directly or by defining the user's role.

User type	**Responsible functions or entities**
EMA staff members (TA/CA)	Reporting officer
Seconded National Experts (SNE)	Superiors in the Agency to whom an SNE is assigned
Trainees	Line manager of trainee's mentor
Interims	Recruiting manager
Visiting and Collaborating experts	EMA receiving entity and mentor
Contractor personnel	Operational Initiating Agents
Members from EMA's Management Board, *s*cientific *c*ommittees, working parties and other groups/bodies	Secretariat of Management Board, scientific committees, working parties and other groups/bodies concerned
Other users from NCAs	Appointed representative of the NCA
Users from the European Commission	Appointed representative of the European Commissions
International organisations' users	Head of International Affairs
External users	Appointed representative of the organisation concerned, if defined