OpenEMIS Data Security Policy

Purpose and commitment

OpenEMIS supports clients in operating education management information systems. All data hosted, stored, transmitted, processed or otherwise handled through an OpenEMIS engagement belongs exclusively to the client. OpenEMIS acts only as a service provider and custodian and may process client data solely to deliver authorised services or in accordance with the client's documented instructions.

This policy establishes mandatory controls for protecting client data. Access is highly restricted, developers are separated from identifiable client data and credentials, and all client data must be encrypted both in transit and at rest.

Objectives

- Protect the confidentiality, integrity and availability of client data.
- Comply with applicable data protection laws, contractual commitments and documented client instructions.
- Limit collection, access, use, disclosure, retention and copying to what is necessary for an approved purpose.
- Define accountability for access decisions, security controls and incident response.
- Support clients in meeting the rights of individuals whose personal data is held in OpenEMIS.

Scope and definitions

This policy applies to all OpenEMIS staff, contractors and other authorised personnel, and to every system, service, device, storage location, network and process used to handle client data.

Definitions

- **Client.** Client means the organisation that owns the data and has engaged OpenEMIS to provide services.
- **Client data.** Client data means all information supplied by or collected for the client, and all information generated, derived, logged, backed up or otherwise created through the engagement. It includes personal, operational, configuration and security data.
- **Personal data.** Personal data means information that identifies, relates to or can reasonably be linked with an individual, directly or indirectly.
- **Anonymised data.** Anonymised data means a copy from which direct and indirect identifiers have been removed or irreversibly transformed so that individuals and the client cannot reasonably be identified from the data available to the recipient.
- **Production environment.** Production environment means a live client system and its connected databases, storage, logs, backups and administrative interfaces.

Data protection principles

- **Client ownership and control.** Client data remains the client's property at all times. It must not be sold, licensed, reused, disclosed or used for product development, testing, analytics or any other secondary purpose without the client's documented authorisation.
- **Lawful and limited use.** Client data must be processed fairly, lawfully and only for specific, authorised purposes.
- **Data minimisation.** Only the minimum data required for an approved task may be accessed, copied or retained.
- **Accuracy.** Reasonable steps must be taken to keep client data accurate and to correct or remove inaccurate data in accordance with client instructions.
- **Retention limitation.** Client data must be retained only for the period required by the client agreement, documented client instructions or applicable law.
- **Security.** Client data must be protected against unauthorised access, disclosure, alteration, loss, destruction and unavailability.
- **Transparency and individual rights.** OpenEMIS must support the client in explaining how personal data is processed and in responding to valid requests concerning that data.
- **Controlled transfers.** Client data must not be transferred to another organisation or jurisdiction unless the transfer is authorised and subject to appropriate legal, contractual and technical safeguards.

Governance and responsibilities

Everyone who works for or with OpenEMIS is responsible for protecting client data and must follow this policy, the controls applicable to their role and the client's documented instructions.

- **OpenEMIS Data Security Officer.** Maintains this policy, advises on data protection risks, coordinates training and compliance reviews, supports incident response, and reviews arrangements involving third parties that may handle client data.
- **OpenEMIS Delivery Manager.** Oversees operational compliance for client engagements, confirms that access is necessary and approved, coordinates with the client, and ensures that incidents and access changes are escalated to the appropriate personnel.
- **OpenEMIS DevOps staff.** Implement and maintain technical security controls, including encryption, access management, monitoring, secure backups, restoration testing, vulnerability management and approved production administration.
- **Authorised Quality Assurance, Implementation and Support staff.** May access client data only when required for an assigned client task and must use approved systems and handling procedures.

Access to client data

Access to client data is highly restricted. It may be granted only to members of the following OpenEMIS role groups when access is necessary for their assigned duties:

- OpenEMIS Delivery Manager
- OpenEMIS Quality Assurance staff
- OpenEMIS Implementation staff
- OpenEMIS Support Analysts
- OpenEMIS DevOps staff

No other OpenEMIS staff role may be granted access to client data.

Access conditions

- Access must be approved through the designated access-management process and limited to the relevant client, system, data and time period.
- Access must follow least-privilege and need-to-know principles. Membership in an authorised role group does not provide automatic or unrestricted access.
- Each person must use an individual account. Shared accounts and the sharing of passwords, tokens or other credentials are prohibited.
- Multi-factor authentication must be used for privileged and remote access where the platform supports it.
- Access activity must be logged where technically feasible and reviewed in proportion to the sensitivity and risk of the data.
- Access must be removed promptly when the task ends, the person changes role, or the person no longer works on behalf of OpenEMIS.
- Direct access to a production database is restricted to authorised OpenEMIS DevOps staff when needed for approved administration or incident response. Other authorised personnel must use approved application interfaces and support tools.
- Third parties may access client data only with appropriate client authorisation, contractual safeguards and access controls equivalent to this policy.

Developer access and anonymised data

OpenEMIS Developers must not access raw or identifiable client data, client production environments containing that data, client passwords, or any other client credentials or secrets.

When development or defect investigation requires representative information, the following process is mandatory:

1. **Authorised copy.** A person in an authorised access role must create the smallest controlled copy needed for the task in an approved secure environment. A developer must not create or retrieve the copy from the client environment.
2. **Anonymisation.** Before the copy is provided to a developer, the authorised person must remove or irreversibly transform all client-identifiable information. This includes names, contact details, addresses, dates of birth, identification numbers, account numbers, location details, free-text identifiers and combinations of attributes that could identify an individual or the client. All passwords, tokens, keys and other secrets must be removed.
3. **Verification.** The authorised person must verify that the copy contains no client-identifiable data or credentials and record the purpose, recipient and approved retention period.
4. **Developer use.** The developer may receive and use only the verified anonymised copy, only for the approved task and only in an approved development environment. Re-identification or attempts to link the data back to the client or an individual are prohibited.
5. **Disposal.** The anonymised copy and all derived working files must be securely deleted when the approved task or retention period ends.

Any copied, anonymised or derived dataset remains the property of the client and remains subject to this policy.

Encryption and credential protection

All client data must be encrypted in transit and at rest using approved encryption methods and key-management controls. This requirement applies regardless of the data's format, sensitivity or location.

- Encryption at rest applies to databases, file systems, object storage, logs containing client data, backups, exports, temporary files, removable media and working copies used for anonymisation.

- Encryption in transit applies to communications between users, systems, services, application programming interfaces, storage locations and external recipients. Only approved secure protocols and transfer mechanisms may be used.
- Client data must not be sent through unencrypted email, consumer file-sharing services or other unapproved channels.
- Encryption keys must be stored separately from encrypted data, restricted to authorised personnel and services, rotated as required by the approved key-management process, and protected against unauthorised disclosure.
- Where OpenEMIS manages passwords, passwords must be protected using an approved one-way salted password-hashing method. System credentials, tokens and keys must be held in an approved secrets-management service and must not be embedded in source code or shared informally.
- Client passwords and credentials must never be disclosed to OpenEMIS Developers.

Storage, backup, retention and disposal

Electronic data

- Client data may be stored only in approved environments, drives, servers and cloud services that meet OpenEMIS and client security requirements.
- Client data must not be stored on personal devices or unmanaged local drives. Temporary local storage on an approved managed device is permitted only when technically necessary, authorised, encrypted and deleted immediately after the task.
- Removable media may be used only when specifically authorised. It must be encrypted, inventoried, physically secured and securely erased after use.
- Systems that store or process client data must use supported security controls, including access restrictions, security updates, malware protection and network protections appropriate to the environment.
- Backups must be encrypted, access-controlled and stored securely. Restoration procedures must be tested regularly in accordance with approved backup procedures.

Paper records

Printing client data should be avoided. When a legitimate task requires paper records, they must be kept out of public view, stored in a locked location when unattended and destroyed using an approved secure-disposal method when no longer required.

Retention and deletion

Client data must be retained and deleted in accordance with the client agreement, the client's documented instructions, approved retention schedules and applicable law. Deletion must cover active data, exports, temporary copies and working files. Backup copies must expire through the approved backup-retention process and remain protected until deletion.

Secure handling and use

- Authorised users must access only the client data needed for the approved task and must not create unnecessary copies or datasets.
- Workstations and sessions must be locked when unattended, and client data must not be displayed where unauthorised people can view it.
- Client data must not be discussed, displayed or shared informally, including through personal messaging, personal email or public collaboration channels.

- Transfers and disclosures must use approved secure channels, be limited to authorised recipients and include only the minimum necessary data.
- Client data must not be used in demonstrations, training, testing, screenshots or documentation unless the client has authorised the use and all identifiable information has been removed.
- Suspected access errors, accidental disclosures, loss, corruption or insecure storage must be reported immediately through the designated security incident process.

Data accuracy and availability

- OpenEMIS must apply reasonable controls to prevent unauthorised or accidental alteration of client data.
- Authorised personnel must follow approved change, validation and reconciliation procedures when updating client data.
- Known inaccuracies must be corrected or referred to the client in accordance with the client's instructions and the responsibilities assigned to the relevant role.
- Backups, restoration procedures and continuity controls must support the availability requirements agreed with the client.

Security incidents

A suspected or confirmed loss, unauthorised access, disclosure, alteration, destruction or unavailability of client data is a security incident. Anyone who becomes aware of an incident must report it immediately through the designated incident process and must preserve relevant evidence.

- OpenEMIS will assess, contain, investigate and remediate the incident using the approved incident-response process.
- The OpenEMIS Delivery Manager and Data Security Officer will coordinate communication with the client and other responsible personnel.
- The client will be notified in accordance with the client agreement and applicable law. OpenEMIS will provide the information reasonably required for the client to assess impact and meet its obligations.
- Lessons learned and corrective actions must be documented and tracked to completion.

Client requests and lawful disclosure

Client data requests

The client controls decisions concerning access to, correction of, export of and deletion of client data. Requests received directly from an individual must be referred promptly to the client unless applicable law requires another response. OpenEMIS will assist the client with verified requests in accordance with the client agreement, documented client instructions and applicable law.

Lawful disclosure

A request from a court, regulator, law-enforcement agency or other authority must be referred to the client and appropriate legal or security personnel unless OpenEMIS is legally prohibited from doing so. Before disclosure, OpenEMIS must verify the request's authority and scope, disclose only the minimum legally required data, use a secure transfer method and document the disclosure.

Training, compliance and review

- Personnel must complete data security and privacy training appropriate to their role before receiving access and at intervals required by the approved training programme.
- Compliance with this policy may be verified through access reviews, logging, security testing, internal review and client or contractual assurance activities.
- Suspected non-compliance must be reported and addressed promptly. Access may be suspended while a concern is investigated.
- Exceptions must be documented, risk-assessed, time-limited and approved by the appropriate security and client authorities. No exception may authorize OpenEMIS Developers to access identifiable client data or client credentials, or permit client data to remain unencrypted in transit or at rest.
- This policy must be reviewed periodically and whenever there is a material change to legal obligations, client commitments, OpenEMIS roles, systems or security risks.