EDQM applications security notice

1. General aspects

1.1 Information security: organisational structure and governance

The EDQM has put in place an organisational and governance structure for information security in collaboration with the Information Security Officer and the technical experts responsible for day-to-day operations. It is based on the ISO 27001 standard.

An information systems security policy (ISSP), supported by operational procedures, describing all security controls in place. The security of our solutions is governed as part of a formal information security management system (ISMS).

1.2 Risk management

A risk management methodology formalising the risk evaluations performed (identification of assets, critical business processes, threats and vulnerabilities) is in place. A strategic risk analysis is performed at least once per year and with each major information system change, and also covers personal and sensitive (e.g. health and financial) data.

The methodology followed by the EDQM is based on ISO 27005. A treatment plan for identified risks is drawn up at the end of each risk analysis and implemented in the form of projects or planned activities. The risk treatment plan documents the analysis in detail and outlines a hierarchy of actions to be taken. Each corrective action is added to the action plan and is formally tracked, traced and its effectiveness regularly reviewed.

1.3 Systems and applications development policy

Since security is of primordial importance to the EDQM, we apply the best security practices to our development activities in line with our “Security by Design” approach and “Defence in depth” principle.

Processes for EDQM developers are established and documented. They contain the principles for secure development and a policy for reviewing code (vulnerability detection, treating errors, managing access and entry and securing storage and communications).

Special attention is paid to the most critical security risks identified by, for example, the OWASP Top 10 or alerts from the French Computer Emergency Response Team (CERT-FR). Security tests and security review milestones are integrated into the systems development and implementation processes and these are performed by our operational teams.

1.4 Incident management

An incident management process is in place, which enables the prevention, detection and resolution of these events within the information system. It comprises:

- a guide for assessing and classifying security events;
- the treatment of security events;
- simulation exercises for the crisis management team;
- tests for the incident response plan;
- customer communication if the crisis management team is activated.

These procedures are subject to a continuous improvement process for the monitoring, evaluation and overall management of incidents and the corrective actions taken.

All security incidents enter at the first level of technical support, regardless of whether they are detected by the customer, internally or by an external source such as our security operations centre (SOC). The incident is traced using an internal incident management tool and confirmed by our operational teams. A dedicated e-mail address is used to report a security incident.

The second and third levels are activated according to the severity level assigned to the incident. At each level, the EDQM ISSM oversees the correction operations and communication with the customer and/or the relevant authorities.

1.5 Security audits

Security audits are regularly carried out to ensure continued compliance with the information security policy and to evaluate the performance of our systems. There are two types of security audit:

- organisational (governance, ISMS, etc.) performed by internal or external auditors;
- technical (intrusion tests, vulnerability scans, configuration audits, etc.) performed by internal or external auditors.

We ensure that auditors apply the latest methodologies. The nature and frequency of audits depend on the solutions audited and the scope of the audit. If a non-compliance is identified, a corrective action is implemented and added to the action plans. All of these measures are formally tracked, traced and their effectiveness regularly reviewed.

1.6 Human resources security

New staff members agree to keep all information to which they have access as part of their duties confidential and sign a confidentiality agreement upon taking up their duties.

All EDQM employees are required to abide by a dedicated work instruction on the use of the information system that defines their data protection obligations.

All internal and external IT administrators are required to abide by a charter that covers their privileged access.

A data security and confidentiality awareness campaign for EDQM employees is in place. New employees undergo an information-system security awareness session. Security-related communications are regularly sent to the entire EDQM staff. Test campaigns are organised and run to ensure that staff members react appropriately when they encounter a threat.

1.7 Personal data compliance

Personal data are processed in accordance with applicable data protection laws, such as the convention 108+.

For more information on how we process personal data, please read our personal data protection policy document (work in progress).

2. Data protection

2.1 User access and password policy

Users access EDQM applications via HTTPS authentication. Users activate their account via an activation link sent to their e-mail address. They then protect access to their account by creating a password when they first log in.

Passwords are chosen by the user and must comply with the level of complexity set by the platform. Users are advised to create a complex and unique password and to protect it (e.g. by storing it in a password safe such as KeePass). Users are reminded that they must never share their passwords. Passwords are only stored in hashed form on our servers and EDQM staff have no access to any plaintext passwords.

All records of user logins (e-mail address, date and time) are logged and stored for one year.

A logical separation is in place to prevent users from one organisation from accessing data from another organisation.

2.2 Logical access control for the EDQM's information system

A strict logical access control policy for EDQM employees is in place:

- rights are attributed based on the principles of least privilege and "need to know" and are monitored by business entities;
- access rights and permissions attributed to a user or system are based on a registration, modification and deactivation procedure that involves managers, IT administrators and HR;
- all employees use named user accounts for their everyday connections;
- all login sessions expire after a defined period, the length of which depends on the sensitivity of the application used;
- if a user forgets their password, their identity is verified before the password can be reset;
- passwords are complex and expire after a defined period, after which they must be changed;
- storing passwords in unencrypted files or on paper is prohibited;
- all users are provided with a secure password manager that has been validated by the security teams.

All remote access to the information system (IS) is via a VPN connection. It is only possible to connect to the VPN using a previously identified and authorised device and a password known only by the user.

2.3 Managing administrator access to production platforms

A strict policy for administrator access to platforms is in place:

- it is prohibited to use default passwords (provided by the manufacturer) on systems and equipment;
- two-factor authentication with full traceability is mandatory for remote system administrator access as well as for employee access to sensitive areas;
- system administrators have a named account dedicated exclusively to administrator tasks that is separate from their user account;
- rights are attributed and monitored based on the principles of least privilege and "need to know", and only if this need is justified;
- rights and access for system administrator accounts are reviewed regularly in collaboration with the departments affected;
- if an administrator leaves the organisation, their system administrator account is deactivated immediately.

2.4 Data encryption

Your data are encrypted in transit using the most robust and reliable encryption techniques and algorithms.

Server certificates are countersigned by a renowned certification authority.

User passwords are hashed.

2.5 Data retention

Application files are deleted automatically after 3 years following the creation date. Templates (files that have a given layout but without any data/results) are not deleted automatically; the user may decide to delete them whenever appropriate.

2.6 Payment protection

All payments made on-site are processed by our certified partner PCI-DSS. The EDQM never stores any payment details.

3. Infrastructure security

3.1 Secured IT infrastructure

Administration of the EDQM's infrastructure is handled by a dedicated team that implements security controls in accordance with ISO 27001, under the supervision of the ISSM.

The following measures are taken to secure all pieces of equipment:

- an inventory is stored in an asset management database;
- setting up a hardening process with accompanying guides describing the parameters that need to be modified to ensure a secured configuration;
- control lists restrict access to admin functions;
- all infrastructure equipment are administered through a bastion host, applying the principle of least privilege;
- all infrastructure equipment configurations are backed up;
- logs are collected, centralised and constantly monitored by the administrator team and the external SOC in order to detect production and security incidents;
- automated vulnerability analyses are performed on the infrastructure. The ISSM and operational teams ensure technology monitoring for new vulnerabilities;
- protection against malicious activity and software is installed on our servers.

3.2 Availability & resilience

EDQM applications are permanently available and maintenance is performed when the EDQM office is closed. The service availability is measured on a monthly basis with the objective to be greater than 99.9%.

The critical components of the infrastructure are mirrored on different servers.

Full backups are performed at least once per day and are stored on a remote server. Backup restoration tests are regularly performed. Backups are saved for one year.

3.3 Recovery

In the event of damage to the infrastructure that hosts critical EDQM applications, the disaster recovery plan would allow for activities to restart at a second site.

The level of service commitment following an incident for critical applications is as follows:

- Recovery time objective: 24 h (not including weekends);
- Recovery point objective: 12 h (not including weekends).

3.4 Physical security

Security measures are in place to control physical access to the EDQM sites:

- a right of access policy;
- cameras located at the entrances and exits of installations and sever rooms;
- badge-controlled secured access areas;
- anti-intrusion systems;
- intrusion detection processes (24 h security guarding and video surveillance);
- a round-the-clock surveillance centre that controls the opening of the entrance and exit doors.