Credemia Security Policy

ISO 9001 | ISO/IEC 27001 | ISO/IEC 27017 | ISO/IEC 27018

Document code: M1PR08. Italian source edition: 1. Italian source revision: 0. Italian source date: 30 June 2026. English product-specific draft updated on 15 October 2026.

Classification: Public.

Distribution: controlled copies for employees; uncontrolled copies for stakeholders who are not employees.

Source document revision history

Ed.	Rev.	Date	Description	Written by	Quality review	Management approval
0	0	31 January 2024	First issue	--	RQ	DIR
0	1	25 February 2025	Added complaint form and downtime reporting	--	RQ	DIR
0	2	3 February 2026	Sections 2 and 16	CS	RQ	DIR
1	0	30 June 2026	Adapted following merger by incorporation	CS	RQ	DIR

Your privacy and security are important to us. Pomiager US is committed to managing your data and continuously improving the security of its platforms.

Product scope: Credemia, supplied by Pomiager US. Website: https://credemia.com. Platform: https://app.credemia.com.

1 Purpose

This document describes the security measures adopted by Pomiager US to protect the data and information processed through its platforms, within an integrated management system compliant with ISO 9001, ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018.

2 Scope

This document applies to the Credemia platform supplied by Pomiager US as Software as a Service (SaaS). It is intended for customers, users and other external stakeholders.

3 Backups and disaster recovery

We retain complete backups of every database created on our platforms, allowing restoration to a point up to 30 days earlier.

Backups are managed and stored through a cloud service. The data centres currently used for backup storage are located within the European Union, in Ireland, the Netherlands and Italy.

You can contact the Helpdesk to restore any backup of your active database.

Disaster recovery

RPO (Recovery Point Objective): 0 to 24 hours. This is the maximum amount of data that a company can afford to lose during recovery. It means that you may lose up to 24 hours of work if the data cannot be recovered and we need to restore your latest daily backup.

RTO (Recovery Time Objective): 0 to 24 hours. If a disaster makes a data centre completely inoperable, the service must be restored in another data centre to recover operations.

Our daily backups are replicated in several locations and countries within the European Union: Ireland, the Netherlands and Italy.

4 Database security

Customer data are stored in a specific database and are not shared between customers.

Data-access control rules ensure complete separation between the databases of customers using the same cluster. Access from one database to another is not possible.

5 Clock synchronisation

The clocks of information-processing systems relevant to Pomiager US or its security domain are synchronised with a single reference source. Systems running on Azure Cloud are generally synchronised with Azure's time service. Azure synchronises server clocks with Coordinated Universal Time (UTC) through reliable time sources such as atomic clocks and satellite time services. This keeps the time consistent across services and virtual machines throughout the cloud infrastructure.

Clock synchronisation is essential for functions including event logging, scheduling, transaction management and security. Azure customers do not need to set the time manually on their virtual machines or services because Azure manages synchronisation automatically.

- The NtpClient provider obtains time information from time.windows.com.
- The VMICTimeSync service communicates the host's time to virtual machines and makes corrections after a virtual machine has been paused for maintenance.
- Azure hosts use Microsoft-owned stratum 1 devices to maintain accurate time.

6 Password security

Customer passwords are protected using industry-standard PBKDF2+SHA512, with salt and multiple iterations that make attacks more computationally expensive.

Pomiager US staff do not have access to your password and cannot retrieve it for you. If you lose it, the only solution is to reset it.

Login credentials are always transmitted securely over HTTPS.

Password policies: database administrators have a built-in setting to enforce a minimum user password length. Other password policies, such as required character classes, are not supported by default because they are counterproductive. See, for example, Shay et al. 2016 and NIST SP 800-63b.

Our applications allow two-factor authentication (MFA) to be enabled to make account access more secure.

7 Staff access

Application Helpdesk staff may access your account to check settings relating to a problem you have reported. They use their own special credentials rather than your password, which they cannot know.

Special staff access improves efficiency and security: we can reproduce the reported problem immediately without requiring you to share your personal password, and staff operations can be checked and audited separately.

Our Helpdesk staff make every effort to respect your privacy and access only the files and settings needed to diagnose and resolve your problem.

8 System security

All application cloud servers run hardened Windows distributions, with security patches updated directly by the cloud provider.

Installations are tailored and minimal to limit the number of services that could contain vulnerabilities.

Only Pomiager US system administrators are authorised to manage servers remotely.

9 Data encryption

Customer data are always transferred and stored in encrypted form, both in transit and at rest.

All data communications to customer instances are protected by advanced 2048-bit RSA encryption (SHA256withRSA).

All internal data communications between our servers are protected by current encryption technology.

Our servers are closely monitored for security. Patches are continuously updated to address the latest SSL vulnerabilities. Our applications receive an A grade in SSL assessments. You can consult the assessments through SSL Labs.

All our certificates use strong 2048-bit moduli with SHA-2 certificates.

All customer data, including database contents and stored files, are encrypted at rest in production and backups using AES-128 or AES-256.

10 Network protection

All data centre providers used by Pomiager US's cloud applications have substantial network capacity and infrastructure designed to withstand major OWASP-type attacks.

Server firewalls and intrusion prevention systems help detect and block threats such as brute-force password attacks.

11 Software security

Pomiager US applications are developed using secure coding best practices. Developers receive internal training to keep them informed about secure development practices. We encourage developers to investigate code and security issues. We are developing a page within the applications containing information about releases and known bugs.

Pomiager US's research and development processes include code review steps that address security, including security in new code.

12 Security by design

Our applications are designed to prevent the introduction of the most common security vulnerabilities:

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery

13 Allocation of responsibilities

Standard virtual machine configurations have been defined. Configurations are customised where necessary, with reference to guidelines from recognised national and international agencies such as AgID, NIST and CIS.

Pomiager US delivers its platforms as Software as a Service (SaaS). Security is therefore a shared responsibility between Pomiager US, as service provider, and the customer, as described below.

Provider responsibilities: Pomiager US is responsible for the security of the platform and its supporting infrastructure. This includes system configuration and hardening, installation of security patches and updates, monitoring, backups and restoration, separation of customer data, encryption in transit and at rest, and management of its staff's access. For physical and network infrastructure supplied by the cloud provider, Microsoft Azure's own measures apply.

Customer responsibilities: the customer is responsible for use of the platform and the data entered into it. This includes management of users and authorisation profiles assigned within its instance; keeping login credentials confidential; adopting strong passwords and enabling MFA; securing the devices and networks used to access the platform; and promptly reporting suspected account compromises as described in Section 15.

Division of responsibilities: the allocation of responsibilities between provider and customer must be clearly understood and documented to prevent security gaps and ensure that both parties understand their responsibilities. This allocation is detailed in service-level agreements (SLAs) and security policies.

14 Independent security checks

Pomiager US is audited by independent companies that inspect quality, data and information security, and secure application development. We have implemented an integrated management system for ISO 9001, ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018.

We conduct vulnerability and penetration tests at least every three months. Pomiager US's security team receives the results and implements appropriate corrective measures where necessary.

15 Compromised accounts

If you suspect an account has been compromised, for example through stolen credentials or unauthorised third-party access, report the event without undue delay to international@pomiager.com.

We will check the system, restore normal operations and inform you of the outcome.

16 Reporting security vulnerabilities and data breaches

To report a security vulnerability or data breach, email international@pomiager.com. Reports are treated with the highest priority. Pomiager US's security team examines and resolves the problem in collaboration with the person who reported it, after which appropriate communication is provided to the users and customers of the relevant platform.

If Pomiager US detects a data breach or data leak, it is handled under internal procedure PR01MOP_Procedura data breach.

Where the crisis team considers that a personal data breach is likely to create a high risk to individuals' rights and freedoms, the privacy contact must inform the affected data subjects without undue delay.

17 Downtime notifications

We undertake to give at least 72 hours' advance notice of planned application downtime for updates lasting more than one hour.

18 Complaints

If you need to submit a complaint, you may:

- Email international@pomiager.com.
- Use the tool available on our websites and platforms.

For every complaint, Pomiager US will:

- Respond promptly, keep the complaint under control and address its consequences.
- Take follow-up action to ensure the same problem does not recur elsewhere.
- Keep you informed about how the complaint is being handled.

We will respond to your complaint and seek to resolve it within five working days.