Support and Maintenance for the Monokee Identity and Access Management On-Premises Platform

Software Defect Correction and Security Vulnerability (CVE) Management

1. Introduction and Purpose

This document describes the support and maintenance service that Monokee S.r.l. ("Monokee") provides for the Monokee Identity and Access Management (IAM) platform installed in the Customer's on-premises environment.

The service is limited to the **correction of defects in the Monokee software code** and to the **management of security vulnerabilities (CVE)** affecting the Monokee software and the third-party components distributed with it. Monokee does not operate, administer or monitor the Customer's environment: installation, configuration, operation and updating of the platform remain the responsibility of the Customer.

The following sections describe the scope of the service, the support channels and service levels, the defect management process, the vulnerability management process and the respective responsibilities of Monokee and the Customer.

2. Scope of the Service

2.1 Included in the service

- Diagnosis of reported malfunctions in order to determine whether they are caused by a Defect in the Monokee software.
- Correction of confirmed Defects in the Monokee software code.
- Provision of Workarounds, where available, pending the definitive correction.
- Identification, assessment and remediation of security vulnerabilities (CVE) affecting the Monokee software and the third-party components distributed with it, as described in Section 8.
- Delivery of corrections in the form of Hotfixes, Patches or Maintenance Releases, together with the related release notes and installation instructions.
- Making available new versions of the software to which the Customer is entitled under the purchased subscription (Section 9).

2.2 Excluded from the service

- Installation, deployment and configuration of Hotfixes, Patches, Maintenance Releases and new versions in the Customer's environments.

- Management, monitoring, backup and upgrade of the Customer's infrastructure, including hardware, virtualization, operating systems, databases, application servers not distributed by Monokee, networks, load balancers and certificates.
- Malfunctions caused by infrastructure, by configuration errors, by improper use of the platform or by third-party products not distributed by Monokee.
- Customizations, integrations, scripts or code developed or modified by the Customer or by third parties.
- Versions of the software that are no longer supported (Section 4).
- Development of new or custom features, training and consulting activities.

Excluded activities may be requested as separate services and will be quoted separately.

3. Definitions

Term	Definition
Defect	A reproducible error in the Monokee software code that causes the product to behave differently from its official documentation, when used in a supported version and in a supported configuration.
Workaround	A temporary procedure or configuration indicated by Monokee that avoids or mitigates the effects of a Defect or vulnerability pending the definitive correction.
Hotfix	A targeted correction released to resolve a specific Defect or vulnerability outside the ordinary release cycle.
Patch	A software package containing one or more corrections for a supported version.
Maintenance Release	A release of a supported version that consolidates previously released corrections.
Vulnerability / CVE	A security weakness in the Monokee software or in a third-party component distributed with it. CVE (Common Vulnerabilities and Exposures) is the public identifier assigned to known vulnerabilities.
CVSS	Common Vulnerability Scoring System, the industry standard used to rate the severity of a vulnerability.
Response Time	The time between the opening of a request by the Customer and its acknowledgement by a Monokee technician.
Business Hours	Monday to Friday, 9:00 to 18:00 CET/CEST, excluding Italian public holidays.

4. Supported Versions

The service covers the current major version of the Monokee IAM on-premises platform (N) and the previous major version (N-2). Corrections are released on the most recent Maintenance Release of the supported version concerned; the Customer may therefore be required to update to that Maintenance Release in order to receive a correction.

For versions no longer supported, Monokee will provide only the information already available and will recommend an update to a supported version.

5. Support Channels and Request Management

Requests can be submitted through the following channels:

- **Support portal (self-service):** the Customer contact opens a ticket in the "Support and Assistance" section of the portal.
- **Email to the Service Desk:** the Service Desk registers the request on the ticketing system.
- **Dedicated telephone number:** reserved for Severity 1 requests, which must always be confirmed by opening a ticket.

Every request is registered on the Trouble Ticketing (TT) system with a unique ticket number. The Customer can follow the status of each ticket directly from the portal. Requests are managed through the following phases:

- **Registration:** the ticket is registered and its receipt is acknowledged.
- **Qualification:** Monokee assigns the severity level and checks that the request falls within the scope of the service.
- **Analysis and correction:** the request is assigned to the technical team according to the process described in Section 7.
- **Closure:** the ticket is closed once the correction or Workaround has been delivered or the request has been answered. Resolutions are recorded in the Monokee Knowledge Base.

6. Support Levels and Service Levels

6.1 Severity levels

Requests are classified according to the following severity levels, which apply only to malfunctions attributable to a Defect in the Monokee software:

Severity	Definition	Channels
Severity 1 – High	A Defect that prevents the use of a primary function of the platform (for example, authentication or provisioning) and causes the total blocking of the service, with no Workaround available.	Dedicated telephone number, followed by a ticket
Severity 2 – Low	A Defect that causes the unavailability of a secondary function or a limited, non-permanent disruption that does not significantly affect the service, or a Defect for which a Workaround is available.	Portal, email or telephone

Security vulnerabilities are classified separately, according to the criteria in Section 8.

6.2 Basic Support

Included in the subscription fee. Coverage during Business Hours, with the following Response Times:

Severity	Response Time (Business Hours)
Severity 1 – High	Within 2 business hours
Severity 2 – Low	Within 4 business hours

6.3 Premium Support

Quoted separately. In addition to Basic Support, Premium Support extends coverage outside Business Hours (24/7, including weekends and public holidays) with the following Response Times:

Severity	Response Time (24/7)
Severity 1 – High	Within 1 hour in 95% of cases; the remaining 5% within 2 hours
Severity 2 – Low	Within 4 hours in 95% of cases; the remaining 5% within 8 hours

Service levels refer to Response Times. Since the correction of a Defect depends on its complexity, Monokee does not guarantee a resolution time but will provide a Workaround or correction with priority proportional to the severity.

7. Corrective Maintenance – Defect Management

Corrective maintenance aims to diagnose and remove the causes of Defects in the Monokee software code. The process includes the following steps:

- **Qualification:** the Service Desk checks that the request is complete and assigns the severity level.
- **Analysis (Second Level):** the technical team analyzes the information provided by the Customer, reproduces the malfunction where possible and determines whether it is caused by a Defect in the Monokee software or by factors outside the scope of the service. In the latter case the ticket is closed with an explanation.
- **Workaround:** where available, Monokee indicates a Workaround to the Customer, who is responsible for applying it.
- **Escalation:** Defects that require changes to the code are escalated to the Monokee development team (Problem Management).
- **Correction and release:** the correction is developed, tested and delivered as a Hotfix, Patch or as part of the next Maintenance Release, at Monokee's discretion based on severity, together with release notes and installation instructions.
- **Closure:** the ticket is closed once the correction has been delivered. Installation in the Customer's environments is the responsibility of the Customer.

Monokee manages corrections through its own internal release and configuration management processes, which ensure that each correction is traceable to the ticket and to the version in which it is released.

8. Security Vulnerability (CVE) Management

8.1 Scope

The vulnerability management service covers:

- the source code of the Monokee IAM platform;
- the third-party libraries, frameworks and runtimes included in the installation packages distributed by Monokee;
- container images, where the platform is distributed by Monokee as containers.

Vulnerabilities in operating systems, databases, application servers, network devices and any other components provided or managed by the Customer are excluded. These remain the Customer's responsibility. On request, Monokee will indicate the compatibility of the platform with the updates of these components.

8.2 Identification

Monokee identifies vulnerabilities through:

- continuous monitoring of public sources, including the NVD (National Vulnerability Database), vendor security advisories and the CISA Known Exploited Vulnerabilities (KEV) catalog;
- Software Composition Analysis (SCA) of third-party dependencies, based on the Software Bill of Materials (SBOM) of each release;
- static analysis of the code and security testing performed during the development cycle;
- reports from Customers, partners and independent researchers, received through the coordinated vulnerability disclosure process (Section 8.6).

8.3 Assessment and classification

Each identified vulnerability is analyzed to determine whether it actually affects the Monokee platform, taking into account whether the vulnerable component or function is used, how it is exposed and whether it can be exploited. Applicable vulnerabilities are classified according to the CVSS base score, adjusted where appropriate to the context of the platform. Vulnerabilities that are being actively exploited (for example, those listed in the CISA KEV catalog) are treated with the highest priority, regardless of their score.

8.4 Remediation timelines

Starting from the confirmation that a vulnerability affects a supported version, Monokee commits to the following target timelines for providing a correction or, where a correction is not yet available, a mitigation:

Severity	CVSS score	Target timeline
Zero-Day	Any (actively exploited or publicly disclosed, no fix available)	Mitigation instructions within 24 hours; Hotfix made available within 2 calendar days of the availability of a fix
Critical	9.0 – 10.0	Mitigation as soon as possible; Hotfix within 30 calendar days
High	7.0 – 8.9	Hotfix or Patch within 30 calendar days
Medium	4.0 – 6.9	Within 90 calendar days or in the next Maintenance Release
Low	0.1 – 3.9	In the next scheduled Maintenance Release

If a correction depends on a fix released by the supplier of a third-party component, the timelines start from the availability of that fix. In the meantime Monokee will provide, where possible, a mitigation or Workaround.

8.5 Zero-day and actively exploited vulnerabilities

A Zero-Day is a vulnerability affecting the platform that is publicly disclosed or actively exploited and for which no correction is yet available from Monokee or from the supplier of the affected component. Zero-Day vulnerabilities are handled through an emergency process, regardless of their CVSS score, and the timelines run from the moment Monokee becomes aware of them. Where the correction depends on a third-party supplier, the two-day timeline runs from the availability of that supplier's fix; in the meantime Monokee provides instructions for a mitigation. Where there is evidence that the vulnerability has been exploited against the platform, Monokee also activates its security incident management process and, where Personal Data are affected, notifies the Customer in accordance with Section 7 of Part A of the DPA.

8.6 Communication to the Customer

For vulnerabilities rated Critical or High, Monokee will send a security advisory to the Customer's designated security contacts. For vulnerabilities rated Medium or Low, the information will be included in the release notes. Security advisories contain, where applicable:

- the CVE identifier and a description of the vulnerability;
- the affected versions and components;
- the severity and the CVSS score;
- available mitigations or Workarounds;
- the version that contains the correction and the installation instructions.

On request, Monokee will also confirm whether a specific public CVE affects the platform, including when the vulnerable component is present but cannot be exploited ("not affected" statement). It will also provide the SBOM of the supported versions.

8.7 Coordinated vulnerability disclosure

Suspected vulnerabilities must be reported through the Monokee security contact channel and not through public channels. Monokee will acknowledge receipt of the report, keep the reporter informed of progress and agree with them on the timing of any public disclosure. Details that could facilitate exploitation will not be disclosed until a correction or mitigation is available to Customers.

8.8 Customer responsibilities for vulnerabilities

- Designate and keep up to date at least one security contact to receive advisories.
- Apply corrections and mitigations promptly, according to their severity.
- Manage vulnerabilities in the infrastructure and in the components under its responsibility.
- Report suspected vulnerabilities to Monokee confidentially.

This process supports the Customer in meeting supply chain security requirements, including those set out in the NIS2 Directive.

9. Software Updates and New Versions

Under the purchased subscription, Monokee makes available to the Customer:

- Maintenance Releases, which consolidate corrections and security fixes;
- new versions of the platform, including the new features covered by the subscription.

Each package is distributed with release notes and installation instructions. Planning and installation of updates in the Customer's environments are the responsibility of the Customer. Assistance with installation and upgrades can be requested as a separate service.

10. Customer Responsibilities

In order to receive the service, the Customer agrees to:

- use a supported version of the platform in a configuration that complies with the official documentation;
- designate qualified contact persons authorized to open requests;
- provide a description of the malfunction and the information needed for the analysis, such as logs, screenshots, the steps needed to reproduce the issue and the version in use;
- collaborate in the reproduction and verification of the malfunction and, where agreed, provide remote access for diagnostic purposes, under the Customer's supervision;
- maintain a test environment in which corrections can be verified before they are installed in production;

- install corrections, Maintenance Releases and security fixes in its environments within a reasonable time.

Monokee is not responsible for any delays caused by the Customer not fulfilling the above obligations.