maintenance policy

Signox LogX Team

2025-07-09

Table of Contents

# 1 Smart Roster System - Maintenance Policy (Signox)

## 1.1 Purpose

This document outlines the maintenance responsibilities of Signox for the Smart Roster system, clarifying what is covered under our support and what is outside our scope. It also provides best practices and guidance for clients to ensure system reliability and compliance.

## 1.2 Scope of Maintenance

### 1.2.1 Covered by Signox

* **Core Application Code:** All backend and frontend modules as delivered, including APIs and integrations within the original project scope.
* **Database Schema & Migrations:** Structure, migrations, and integrity of the delivered database. Includes schema updates required for new features or bug fixes.
* **Bug Fixes:** Resolution of bugs in delivered modules within the agreed support period. Includes critical, high, and normal priority issues as defined in the service agreement.
* **Security Patches:** Updates to address vulnerabilities in the delivered codebase, including urgent patches for newly discovered threats.
* **Documentation:** Updates to technical and user manuals for delivered features, including release notes and change logs.
* **Deployment Scripts:** Docker, compose files, and CI/CD scripts as provided. Includes updates for supported environments.
* **Monitoring Integrations:** Provided monitoring scripts and dashboards (e.g., Prometheus, Grafana). Includes configuration support for delivered monitoring tools.
* **Initial Training & Onboarding:** Training sessions and materials for system administrators and key users at the time of delivery.
* **Release Management:** Delivery of new versions, patches, and hotfixes as per the support agreement.

### 1.2.2 Not Covered by Signox

* **Custom Code Changes:** Any modifications made by the client or third parties after delivery, including unsupported plugins or scripts.
* **External Integrations:** Third-party services or APIs not included in the original scope, or changes to those services after delivery.
* **Client Infrastructure:** Hardware, network, or cloud resources not provisioned or managed by Signox, including firewalls, load balancers, and backup systems.
* **User Data Management:** Data entry, migration, or manual corrections performed by client staff. Signox does not manage or validate client-entered data.
* **Unsupported Plugins/Extensions:** Any add-ons not delivered or approved by Signox, including browser extensions or mobile apps.
* **Ongoing Training:** Training beyond the initial onboarding and documentation, unless specified in a separate agreement.
* **End-User Devices:** Maintenance of client/user hardware, browsers, or mobile devices.
* **Compliance with Local Policies:** Ensuring compliance with local data protection, privacy, or educational regulations is the client’s responsibility.

## 1.3 Maintenance Best Practices (For Clients)

* **Backups:** Regularly back up the database and configuration files. Test restore procedures periodically to ensure data integrity.
* **Monitoring:** Use provided dashboards to monitor system health and performance. Set up alerting for critical issues and review logs regularly.
* **Updates:** Apply security and bug fix updates as released by Signox. Review release notes for impact and schedule updates during maintenance windows.
* **User Management:** Periodically review user roles and access rights to prevent privilege creep and unauthorized access.
* **Incident Reporting:** Report issues via the agreed support channel for timely resolution. Provide logs, screenshots, and error details for faster troubleshooting.
* **Change Management:** Document and review any client-side changes to ensure maintainability and support eligibility. Notify Signox before making significant changes.
* **Compliance:** Ensure your use of the system complies with local laws and institutional policies, especially regarding data privacy and user consent.

## 1.4 Support Process

* **Issue Reporting:** Contact Signox support via the agreed channel (email, ticketing system, etc.). Include a detailed description, steps to reproduce, and relevant logs/screenshots.
* **Response Times:** As per your service agreement. Issues are prioritized based on severity and business impact.
* **Escalation:** Critical issues (e.g., system outage, data loss, security breach) are prioritized for rapid resolution. Escalate unresolved issues through the designated escalation path in your agreement.
* **Status Updates:** Signox will provide regular status updates for ongoing incidents and maintenance activities.
* **Resolution & Verification:** Once resolved, issues are verified with the client before closure. Documentation is updated as needed.

## 1.5 Examples of Maintenance Scenarios

* **Covered:**
  + A bug in the attendance module prevents session validation—Signox investigates, patches, and updates documentation.
  + A security vulnerability is discovered in the backend API—Signox issues a patch and notifies all clients.
  + A new version of the Docker deployment script is released to support a new OS version.
* **Not Covered:**
  + The client modifies the timetable module code, causing errors—Signox support is not responsible for custom code issues.
  + A third-party SMS gateway changes its API—Signox is not responsible unless it was part of the original scope.
  + A trainee’s device cannot access the system due to outdated browser—client IT support is responsible.

## 1.6 Compliance & Security Notes

* **Data Privacy:** Signox ensures secure handling of user data within the delivered system. Clients are responsible for ongoing compliance with data protection laws (e.g., GDPR, FERPA).
* **Access Control:** Only authorized users should be granted admin or sensitive roles. Regularly audit user permissions.
* **Incident Response:** In case of a security incident, follow the incident reporting process and cooperate with Signox for investigation and remediation.

**Last updated:** July 2025