Audit Logging Policy

Audit Logging Policy

Adapted from GitLab's Audit Logging Policy.

Why

We can only investigate what we logged. In the 2026 mailbox incidents, the **login and source-IP evidence had already gone** from Nextcloud's activity stream (it kept about 6 months), and mail submission headers don't record the sender's IP. This policy closes that gap.

What must be logged

System	Events	Owner
LDAP / mail (Postfix, Dovecot)	Successful and failed logins with username, source IP and time; messages sent per authenticated user	Federated Computer
Roundcube	Logins (`userlogins` log) with IP	Federated Computer
Nextcloud	Logins, failed logins, app-password and 2FA changes, admin actions, sharing (the **admin_audit** app)	Security DRI
BookStack, ERPNext	Logins and admin changes (built-in audit logs)	System owners
Servers and field devices	SSH logins, sudo use, config changes	Tech lead

Retention

Keep security logs for **at least 12 months**, so an incident found months later can still be investigated. Logs must be protected from changes and readable only by admins.

Review and alerts

- Alert when one account sends unusually many messages per hour, or logs in from a new country.
- The Security DRI checks failed-login and sending-volume summaries monthly, and DMARC aggregate reports (sent to admin@) monthly.

Status

As of October 2026, retention and alerting are **not yet confirmed** with Federated Computer. That is an open action from the 2026 incident report.

Revision #1
Created 2026-10-20 23:51:32 UTC by MCP Server
Updated 2026-10-21 00:02:15 UTC by MCP Server