Security Overview

Security Overview — BasicAS Group

Last Updated: 2026-02-10 **Security Lead:** John (AI Director) **Approval Authority:** Alem (CEO)

Executive Summary

This document provides a high-level overview of security practices, policies, and systems for BasicAS Group. It consolidates information from multiple security workstreams and serves as a navigation hub for detailed security documentation.

Security Posture

Current State (2026-02-10)

- ✅ **System Integrity Protection (SIP):** Enabled
- ✅ **Credential Rotation Infrastructure:** Complete (awaiting execution)
- ✅ **Network Hardening Configuration:** Complete (awaiting deployment)
- ✅ **Docker Security:** Containers run with least privilege
- ✅ **API Security:** Token-based authentication for all services
- ⚠ **Firewall:** Not yet enabled (deployment blocked, sudo required)
- ⚠ **SSH:** May be enabled (needs verification)
- ⚠ **Secrets Management:** Some plaintext passwords in docker-compose.yml (task #310)
- ⚠ **MFA:** Not yet enabled for Mattermost external access (task #309)

Risk Level: **MEDIUM**

- **High-risk items:** Plaintext secrets, no firewall, SSH possibly enabled
- **Mitigation:** LAN-only access + Cloudflare Tunnel for external services

- **Timeline:** Deploy hardening + secrets management within 30 days

---

Security Domains

1. Network Security

Status: Configuration ready, deployment blocked

Key Controls:

- macOS Application Layer Firewall (ALF) - configured, not yet enabled
- Cloudflare Tunnel for external access (Mattermost, Planka, Documenso)
- Service port binding (localhost vs. 0.0.0.0)
- SSH remote access disablement
- Bluetooth disablement

See: network-hardening.md

---

2. Credential Management

Status: Infrastructure complete, awaiting execution

Key Controls:

- API key rotation (90-day cycle)
- macOS Keychain storage (encrypted at rest)
- Automated import tool (credential-import.js)
- Secure deletion of temp files (7-pass shred)

Services Covered:

- Anthropic, ElevenLabs, Telegram, Discord, Z.ai
- one.com SMTP, Cloudflare API

See: credential-rotation.md

---

3. Application Security

Docker Services

Service	Port	External Access	Auth Method
Mattermost	8065	Cloudflare Tunnel	Password + optional MFA
Planka	3100	Cloudflare Tunnel	Password
Documenso	3003	Cloudflare Tunnel	Password
BookStack	6875	LAN only	Password + API token
MC Dashboard	3030	LAN only	No auth (trusted network)

Security Gaps:

- MC Dashboard has no authentication (LAN-only, consider adding auth)
- BookStack admin password is default (`password`) - MUST change
- Planka token expiry is 365 days (too long, consider 30-90 days)
- Documenso public signup enabled (consider invite-only)

Recommendations:

1. Change all default passwords
2. Enable MFA for external-facing services
3. Add authentication to MC Dashboard
4. Shorten token expiry periods
5. Disable public signup where not needed

---

4. Data Security

Databases

All databases are:

- □ Internal-only (not exposed to internet)
- □ Password-protected
- □ Backed up regularly
- ⚠ Passwords in plaintext in docker-compose.yml (task #310)

Backups

- **Location:** ~/backups/ + external disk (when Full Disk Access fixed)
- **Frequency:** Manual (needs automation - task #262)
- **Encryption:** Not yet implemented (consider encrypting backups)

Sensitive Data Storage

- **API Keys:** macOS Keychain (encrypted)
- **Passwords:** docker-compose.yml (plaintext) ← FIX THIS

- **User Data:** PostgreSQL/MariaDB (internal)
- **Documents:** MinIO (Documenso), file system (BookStack)

---

5. Access Control

User Management

User	Role	Services
Alem	Admin	All services (full access)
John (AI)	System Admin	CLI tools, read-only on critical files
Edita (AI)	Assistant	Limited access via John delegation
External users	Team members	Mattermost, Planka (invite-only)

API Access

- **BookStack:** Token-based (read/write API)
- **Mattermost:** OAuth + personal access tokens
- **Planka:** JWT tokens (365-day expiry)
- **Documenso:** Session-based

---

6. Monitoring & Logging

Current Logging

- **Docker logs:** All containers (30-day retention)
- **Mission Control:** Task audit trail (SQLite)
- **LaunchAgent logs:** mc-dashboard, mc-session-worker
- **Firewall logs:** Not yet enabled (awaiting deployment)
- **Intrusion detection:** Not implemented

Log Locations

- Docker: `docker logs <container>`
- Mission Control: ~/system/databases/mission-control.db (history table)
- LaunchAgents: ~/system/logs/
- System: `/var/log/` (requires sudo)

Monitoring Gaps

- No real-time alerting (task #259 - health check daemon)
- No centralized log aggregation

- No security event correlation
- No automated anomaly detection

Recommendation: Implement health check daemon + log aggregation (ELK stack or Loki)

---

7. Incident Response

Current Procedures

1. **Detection:** Manual monitoring, user reports
2. **Triage:** John investigates, escalates to Alem
3. **Containment:** Stop affected service, isolate system
4. **Recovery:** Restore from backup, rotate credentials
5. **Post-Mortem:** Document in ~/system/reports/security/

Gaps

- No formal incident response plan (IRP)
- No on-call rotation (single point of failure: Alem)
- No security incident tracking system
- No runbook for common incidents

Recommendation: Create formal IRP + incident runbooks (task #323-326)

---

8. Compliance & Governance

Policies (In Development)

- ☐ Information Security Policy (ISO 27001 aligned) - task #323
- ☐ Business Continuity Plan (BCP) - task #325
- ☐ Disaster Recovery Plan (DRP) - task #326
- ☐ Data Processing Agreements (DPA) - task #278
- ☐ Privacy Policy (GDPR) - not yet started

Compliance Frameworks

- **ISO 27001:** Targeted (not yet certified)
- **GDPR:** Applicable (EU clients, data processing)
- **SOC 2:** Not yet pursued
- **PCI-DSS:** Not applicable (no payment card processing)

Security Roadmap

Immediate (Next 30 Days)

1. **Deploy network hardening** - Alem to execute firewall + SSH disablement (15 min)
2. **Rotate all credentials** - Follow credential-rotation.md process (30 min)
3. **Change default passwords** - BookStack, Planka, Documenso (10 min)
4. **Enable Mattermost MFA** - task #309 (30 min)
5. **Move Docker secrets** - Extract from docker-compose.yml - task #310 (2 hours)

Short-Term (Next 90 Days)

1. **Automated backups** - task #262 (cron + rsync to external disk)
2. **Health check daemon** - task #259 (monitor all services)
3. **Security policies** - tasks #323-326 (ISO 27001 alignment)
4. **Incident response plan** - Formal IRP + runbooks
5. **MC Dashboard auth** - Add password or token-based access

Long-Term (Next 180 Days)

1. **Central secrets vault** - Migrate to HashiCorp Vault or 1Password
2. **Log aggregation** - ELK stack or Loki + Grafana
3. **Intrusion detection** - Deploy Snort or Suricata
4. **Zero-trust architecture** - mTLS for service-to-service comms
5. **ISO 27001 certification** - External audit + certification

---

Security Contacts

Internal

- **Security Lead:** John (AI Director) - via Mission Control or Mattermost
- **Executive Approval:** Alem (CEO) - direct escalation
- **Emergency Contact:** Alem mobile (for after-hours incidents)

External

- **Cloud Provider:** Cloudflare (DDoS protection, tunnel)
- **Domain Registrar:** one.com (DNS, email)

- **Infrastructure:** Self-hosted (Mac Studio)

Security Tools & Resources

Tools In Use

- **macOS Keychain:** Credential storage
- **Docker:** Service isolation
- **Cloudflare Tunnel:** Secure external access
- **BookStack API:** Documentation access control
- **Mission Control:** Task audit trail

Tools Planned

- **HashiCorp Vault:** Centralized secrets management
- **ELK/Loki:** Log aggregation
- **Snort/Suricata:** Intrusion detection
- **WireGuard/Tailscale:** VPN for remote access

Related Documents

Security Documentation

- **Credential Rotation:** credential-rotation.md
- **Network Hardening:** network-hardening.md
- **Security Standards:** ~/system/rules/security.md
- **Anti-Hallucination Rules:** ~/system/rules/agent-anti-hallucination.md

Operational Documentation

- **Infrastructure Runbook:** ~/system/context/docs/runbooks/infrastructure.md
- **Service Runbooks:** ~/system/context/docs/runbooks/
- **Ops Agent:** ~/system/context/docs/runbooks/ops-agent.md

Governance

- **GOVERNANCE.md:** ~/system/context/org/GOVERNANCE.md
- **Task Management:** ~/system/rules/task-management.md
- **Mission Control:** ~/system/databases/mission-control.db

Audit Log

Date	Change	Author	Approval
2026-01-31	Credential rotation infrastructure built	John	Alem
2026-01-31	Network hardening config prepared	John	Alem
2026-02-10	Security docs consolidated	John	Pending
TBD	Network hardening deployed	Alem	-
TBD	Credentials rotated	Alem	-

Maintained by: John (AI Director) **Reviewed by:** Alem (CEO) **Next Review:** 2026-03-10 (monthly)

Revision #6
Created 2026-02-17 22:14:37 UTC by John
Updated 2026-07-26 20:00:17 UTC by John