501CISO

501C CYBERSECURITY LEADERSHIP

Powered by ClearTone Consulting, LLC

SaaS System Ownership Best Practices

Prepared by
Brian Scott

501CISO
501C CYBERSECURITY LEADERSHIP
Powered by ClearTone Consulting, LLC

SAAS SYSTEM OWNERSHIP

Best Practices and Standard Operating Procedures (SOP)

Purpose

To ensure consistent, secure, and compliant use of all SaaS systems through defined responsibilities and best practices for internal system owners.

---

1. **System Ownership & Accountability**
    - Each SaaS platform must have a named **Internal Owner**.
    - Owners are responsible for:
        - Vendor communication
        - License/user management
        - Configuration management
        - Access control oversight
        - Compliance and audit support
    - Document ownership in a **SaaS Inventory Register** (owner, department, purpose, criticality).

---

2. **Access Management**
    - Use **least privilege** access model.
    - Ensure **SSO** or **MFA** is enabled (MFA is mandatory).
    - Conduct **quarterly access reviews** (internal users, partners, API/service accounts).
    - Remove stale/inactive accounts within 5 business days.
    - Document **admin accounts**, their purpose, and business justification.

3. **Data Protection and Privacy**
    - Classify data (Public, Internal, Confidential, Regulated) handled by the SaaS tool.
    - Ensure data is encrypted **in transit** and **at rest**.
    - Avoid storing regulated data (e.g., ePHI, PII, PCI) unless specifically approved.
    - Understand vendor's **data retention** and **deletion policies**.
    - Configure automated **backups** where available, and test restoration at least annually.

4. **Configuration & Change Management**
    - Maintain a **system configuration baseline**.
    - Any changes to configuration (e.g., security settings, API integrations) must:
        - Be approved by the internal owner.
        - Be documented with the reason and date.
        - Be tested in a sandbox/test environment when feasible.
    - Notify IT or security team of major changes (e.g., integrations, data exposure risks).

5. **Third-party Integrations**
    - All integrations must be approved by Security/IT prior to implementation.
    - Maintain a **list of active integrations**, their purpose, and access level.
    - Use **API keys or OAuth tokens** securely; rotate them annually or when an integration is removed.

6. **Monitoring and Incident Response**
    - Subscribe to and monitor **vendor security alerts or status pages**.
    - Enable **audit logs** or **admin activity logs**, if supported.
    - Retain logs for at least 90 days (preferably 180+).

- Report suspected compromise or data exposure **immediately** to IT/Security.
- Maintain **contact info for vendor support and escalation**.

---

7. Training & Awareness

- System owners should complete annual **security awareness training**.
- Ensure system users are also trained on platform-specific secure use guidelines.
- Provide **onboarding guidance** to new users that includes:
    - Appropriate use policies
    - Data sensitivity awareness
    - Support/escalation process

---

8. Vendor Management

- Keep contracts and **Security/Data Processing Agreements** on file.
- Ensure vendors provide:
    - SOC 2 Type II or equivalent
    - Data breach notification clauses
    - Geographic location of data storage
- Perform **annual security risk review** for critical SaaS vendors.

---

9. Decommissioning or Offboarding

- Follow defined **offboarding SOP** when the SaaS tool is no longer in use:
    - Export/archive important data
    - Remove user access
    - Revoke API tokens and integrations
    - Terminate license and billing
    - Document process in a system retirement checklist