Rheonics Cybersecurity Policy

Version: 2.0
Effective Date: April 8, 2025
Last Reviewed: April 8, 2025
Policy Owner: Head of IT
Approved By: CEO

Contents

1. Introduction and Purpose

1.1. Rheonics is committed to protecting its information assets, including proprietary data, customer information, intellectual property, and IT infrastructure, from unauthorized access, use, disclosure, alteration, disruption, or destruction.

1.2. This policy establishes the framework for maintaining a secure environment for Rheonics' digital operations, aligned with:

- Regulations: Swiss FADP, GDPR (where applicable), U.S. state/federal laws, and other applicable national laws where Rheonics operates.
- Standards: Zero Trust principles, CIS Benchmarks, NIST guidelines (e.g., SP 800-88, SP 800-171 where applicable), and OWASP guidelines.

1.3. Objectives:

- Safeguard confidentiality, integrity, and availability (CIA) of data and systems.
- Minimize risks of cybersecurity incidents and ensure business continuity.
- Foster a security-aware culture among all personnel.
- Ensure compliance with legal, regulatory, and contractual obligations.

2. Scope

Applies to all Rheonics employees, contractors, consultants, interns, volunteers, and third parties ("Users") accessing Rheonics systems, data, or facilities. Covers:

2.1. Assets

- Hardware
- Software (including SaaS/IaaS/PaaS)
- Data (electronic and physical)
- Networks
- Physical facilities

2.2. Activities

- On-site work
- Remote work
- Use of company-owned devices
- Use of personal devices (BYOD)
- Development activities
- Third-party vendor interactions

3. Roles and Responsibilities

Role	Key Duties
Management	Champion policy; allocate resources; ensure overall compliance & risk management.
IT/Security Team	Implement/manage controls; lead incident response; conduct audits & assessments.
All Users	Comply with policy; use strong passwords + MFA; report incidents promptly; complete training.

4. Policy Statements

4.1. Data Security

- **Classification & Handling:** Data must be classified and handled according to sensitivity (See Appendix A). Requirements increase with sensitivity.
- **Encryption:** Restricted and Confidential data must be encrypted at rest and in transit using strong, industry-standard algorithms.
- **Disposal:** Secure methods must be used: NIST SP 800-88 compliant wiping for electronic media; cross-cut shredding (P-4 or higher) for physical documents containing Confidential or Restricted data. Data retention schedules must be followed.

4.2. Access Control

- **Least Privilege & RBAC:** Access is granted based on job function necessity (least privilege) using Role-Based Access Control (RBAC).
- **Authentication:** Unique User IDs required. Strong Passwords (See Appendix B) and MFA are mandatory for cloud services, remote access, administrative accounts, and systems handling Confidential/Restricted data.
- **Reviews:** Access rights reviewed quarterly by managers/system owners; revoked immediately upon termination or role change. Formal approval process required for access grants/changes.

4.3. Acceptable Use Policy (AUP)

- **Business Purpose:** Rheonics resources are primarily for business use. Limited incidental personal use is permitted if it does not interfere with duties, consume excessive resources, incur costs, or violate policies/laws.

- **Prohibited Activities:** Including, but not limited to: illegal activities, harassment, accessing/distributing offensive material, copyright infringement, unauthorized system modification, circumventing security controls, installing unauthorized software, introducing malware, unauthorized data sharing/exfiltration, excessive personal use.

- **User Vigilance:** Users must exercise caution with email (phishing), web Browse (malicious sites), and handling attachments/links.

4.4. Network Security

- **Perimeter & Segmentation:** Firewalls, IDS/IPS maintained. Network segmentation isolates critical systems (e.g., R&D, production) and data stores.

- **Wi-Fi:** Secure WPA3-Enterprise (or WPA2-Enterprise minimum) for internal networks. Guest Wi-Fi must be logically separated and provide no access to internal resources.

- **Remote Access:** Only via company-approved VPN with MFA. Split-tunneling may be restricted.

- **Zero Trust:** Implementation of Zero Trust architecture principles (e.g., micro-segmentation, continuous verification, device health checks) is ongoing, targeting completion by Q1 2026 for critical networks.

4.5. Company-Owned Endpoint Security

- **Protection:** All company-owned endpoints (desktops, laptops, mobiles) must have company-managed Endpoint Detection & Response (EDR) or approved Antivirus software, running and updated.

- **Patching:** Operating Systems and applications must be kept updated via the company's patch management process. Critical patches applied within defined timelines [Rheonics to define timelines, e.g., 72 hours for critical OS].

- **Encryption:** Full-disk encryption (e.g., BitLocker, FileVault) is mandatory on laptops and portable devices.

4.6. Bring Your Own Device (BYOD)

- **Approval & Standards:** Use of personal devices (BYOD) to access non-public Rheonics data requires explicit approval and adherence to minimum standards (See Appendix D).

- **Security Requirements:** Includes MDM enrollment, supported OS versions, security software, encryption, passcodes, remote wipe capability, and data segregation/containerization.

- **Disclaimer:** Rheonics reserves the right to manage/wipe company data from BYOD devices; Rheonics is not responsible for personal data loss during security actions.

4.7. Software Security & Management

- **Authorized Software:** Only licensed software approved by IT may be installed. Users are prohibited from installing unauthorized applications.
- **Patch Management:** Applies to all software (OS, applications, firmware) on all systems (servers, endpoints, network devices).
- **Vulnerability Management:** Regular vulnerability scanning conducted. Critical vulnerabilities must be remediated within defined timelines [Rheonics to define]. Penetration testing performed periodically on critical systems.
- **Secure Development:** (If applicable) Development teams must follow secure coding practices (e.g., OWASP Top 10), conduct code reviews, and use security testing tools (SAST/DAST).
- **Software Composition Analysis (SCA):** Open-source components must be inventoried and scanned for vulnerabilities. Use of End-of-Life (EOL) software/components is prohibited unless explicitly risk-accepted by Management/IT Security.

4.8. Physical Security

- **Access Control:** Access to Rheonics facilities, server rooms, and R&D labs restricted via physical controls (badges, keys, biometrics). Access logs maintained for sensitive areas.
- **Visitor Management:** Visitors must sign in, be issued temporary identification, and be escorted in non-public areas.
- **Workstation Security:** Users must lock workstations when unattended (Windows+L / Ctrl+Cmd+Q).
- **Clear Desk/Screen:** Sensitive information (physical documents, screens) should be protected from unauthorized viewing, especially in open areas or when leaving desks unattended. Secure disposal bins used.

4.9. Cloud Security

- **Approved Services:** Use of cloud services (SaaS, IaaS, PaaS) for Rheonics data must be approved by IT/Security.
- **Configuration & Monitoring:** Services must be configured securely, aligning with CIS Benchmarks where applicable (AWS/GCP/Azure). Conditional Access

policies (e.g., geo-location, device compliance) must be enforced. API and user activity logging enabled and monitored.

- **Data Protection:** Ensure cloud providers meet Rheonics' data security, encryption, backup, and residency requirements via contracts and assessments.

4.10. Third-Party / Vendor Management

- **Risk Assessment:** Security assessments conducted before engaging vendors who access, process, store Rheonics data or connect to networks. Risk level determines assessment depth.
- **Contractual Requirements:** Contracts must include clauses covering confidentiality, data protection (including DPAs if processing personal data under GDPR/FADP), security controls, incident notification, and audit rights.
- **Ongoing Monitoring:** Periodic review of critical vendor security posture.

4.11. Incident Response

- **Reporting:** Suspected incidents must be reported **immediately** (target within 1 hour of discovery) via [it@rheonics.com] or [24/7 Internal Company Teams channel].
- **Response Plan:** Rheonics maintains an Incident Response Plan (IRP). See Appendix C for basic flow.
- **Critical Incidents:** (e.g., ransomware, confirmed data breach) Trigger escalation and containment actions (target within 4 hours). Legal/Executive notification follows timelines dictated by regulations (e.g., GDPR/FADP 72-hour breach notification where applicable).
- **Cooperation:** All Users must fully cooperate with incident response investigations.

5. Enforcement

Violations will be addressed based on severity and intent, subject to local employment law.

Violation	Example	Consequence (Examples)
Minor	Accidental policy deviation; missed non-critical training	Written warning; mandatory retraining
Major	Shared credentials; repeated minor violations; installing unauthorized P2P software	Suspension; formal disciplinary action
Critical / Intentional	Intentional data breach; malicious activity; sabotage	Termination; potential legal action

6. Policy Maintenance

- **Review Cadence:** Reviewed at least annually by the Policy Owner (Head of IT) and stakeholders.
- **Review Triggers:** Ad-hoc reviews triggered by: Major security incidents, significant regulatory changes (e.g., new data privacy laws), major technology/infrastructure changes (e.g., large cloud migration), audit findings.
- **Updates:** Approved changes communicated to all Users.

7. Appendices

7.1. Appendix A: Data Classification

Classification	Example	Handling Requirements
Restricted	Customer PII, R&D source code, crypto keys	• Encryption (at rest/transit) • Strict Access Logs • Need-to-know + explicit approval • Annual access review
Confidential	Employee records, financial data, internal strategies	• MFA recommended/required • Need-to-know basis • Limited sharing internally
Internal	Meeting notes, internal policies,	• No external sharing without approval

	general comms	• Use company systems
Public	Marketing materials, website public content	• No restrictions on handling/sharing

7.2. Appendix B: Password Requirements

- **Minimum Length:**
  - User accounts: 12 characters
  - Admin/Service accounts: 16 characters
- **Complexity:** At least 3 of 4: uppercase, lowercase, numbers, symbols (~!@#$%^&*()-_=+[]{}|;:'",.<>/?). Cannot contain username or common dictionary words.
- **Rotation:** 90 days maximum (unless using approved continuous authentication methods).
- **History:** Previous 5 passwords cannot be reused.
- **Storage:** Must not be written down unsecured. Use company-approved password manager (e.g., Bitwarden, 1Password) for storing complex unique passwords. Sharing passwords prohibited. MFA bypass prohibited.

7.3. Appendix C: Incident Response Flow

- **Detection & Analysis:** Identify potential incident.
- **Reporting:** Report IMMEDIATELY (within 1 hour target) to IT/Security via defined channels.
- **Triage & Assessment:** IT/Security assesses severity and impact.
- **Containment:** Isolate affected systems/accounts (within 4 hours target for critical incidents).
- **Eradication:** Remove threat/vulnerability.
- **Recovery:** Restore systems/data securely.
- **Post-Incident Review:** Lessons learned, process improvement.
  - **Notification**: Legal/Regulatory/Customer notifications performed as required based on assessment (e.g., within 72 hours for GDPR/FADP personal data breaches).

7.4. Appendix D: BYOD Minimum Standards

- **Approval:** Required before accessing non-public data.
- **Device Requirements:**
  - **OS Versions:** Must run currently vendor-supported versions (e.g., Windows 11+, macOS 14+, iOS 16+, Android 13+)
  - **Security:** Screen lock/biometrics enabled; device encryption enabled; approved security software (AV/anti-malware) may be required; device not jailbroken/rooted.
  - **MDM:** Enrollment in Rheonics' Mobile Device Management (MDM) solution is mandatory.
  - **Remote Wipe:** Capability must be enabled for company data/profile.
- **Data Segregation:** Company data accessed/stored via approved applications within a managed profile or container (e.g., Microsoft Intune MAM, Android Work Profile). No copying of company data to personal apps/storage.
- **Network:** Connect via secure Wi-Fi; avoid untrusted public Wi-Fi for work.

8. Contact and Acknowledgment

- **Security Questions/Concerns:** Contact [it@rheonics.com] or IT/Security Team via internal channels.
- **Report Incidents:** Use **urgent** methods: [it@rheonics.com] AND [24/7 Internal Company Teams channel - #security-incidents].
- **Acknowledgment:** All users are required to read, understand, and acknowledge receipt of this policy electronically via [HR Portal, Training System] upon onboarding and following significant updates. Failure to acknowledge does not negate the applicability of the policy.

Approved By:

CEO Signature: Date: