RampedUp, LLC Information Security Policy

Document Owner: Information Security Officer (ISO) / Security Lead
Approved By: Senior Management
Effective Date: March 5, 2026
Review Cycle: At least annually and upon material changes to systems, services, threat landscape, or regulatory requirements
Applies To: All RampedUp employees, contractors, temporary staff, vendors/sub-processors, visitors, and any other individuals granted access to RampedUp systems and/or data

---

1. Purpose

RampedUp manages large-scale contact and company data, and data security is a core priority. This Information Security Policy ("Policy") defines the governance framework, responsibilities, and minimum control requirements to protect the **confidentiality, integrity, and availability** of RampedUp information assets and Customer Data, while promoting responsible and ethical behavior among all users.

RampedUp maintains a formal security program and supporting policies (Information Security, Privacy, Code of Conduct, Incident Response Plan, Data Retention, Acceptable Use) and expects equivalent protections from sub-processors disclosed publicly at https://rampedup.io/sub-processors.

---

2. Scope

This Policy applies to:

- RampedUp's cloud infrastructure, applications, networks, endpoints, logs, and supporting services ("Information Resources")
- All environments (production, development, test)
- All data processed, stored, or transmitted by RampedUp, including Customer Data and personal data where applicable
- All access paths (corporate network, remote access, administrative consoles, APIs, CI/CD, and vendor integrations)

---

3. Security Program Governance

RampedUp maintains formal, documented information security policies and procedures that are:

- **Approved by senior management**
- **Communicated to staff and available for reference**
- **Assigned clear ownership and responsibilities**
- **Enforced with disciplinary provisions for non-compliance**
- **Reviewed periodically for continued relevance**

RampedUp's IT Security Policy undergoes regular reviews to remain aligned with evolving technologies and emerging threats. The Policy requires regular security awareness training, ongoing compliance monitoring by IT/security, and establishes that non-compliance can lead to loss of access, disciplinary action, and/or legal consequences.

---

4. Social Measures (Ethics, Governance, Sustainability)

4.1 Positive Impact and Governance

We view our positive impact on the world as a core principle of RampedUp. We embed dedicated governance and sustainability resources into our platforms governed by policy.

4.2 Anti-Corruption Policy

RampedUp has **zero tolerance** for any corruption in business activities. Bribes or other improper or unauthorized payments—directly or indirectly—including kickbacks, benefits, or advantages to any person or entity are prohibited and may result in termination and/or legal action.

4.3 ESG Policy

As a cloud-based company with a relatively small physical footprint, RampedUp minimizes environmental impact through digital workflows, efficient resource usage, and responsible business travel. We provide equal employment opportunities, prohibit discrimination and harassment, support flexible work where feasible, prohibit bribery and corruption, maintain documented data privacy and security controls, and consider ESG-related risks as part of broader risk management.

4.4 AI Policy

RampedUp is committed to the ethical and responsible use of Artificial Intelligence (AI). Our primary focus is leveraging AI to extract business insights from **publicly available data** for customers. We use AI responsibly and with limited scope, respecting legal and ethical boundaries at all times.

---

5. Employee Management, Training, and Security Awareness

5.1 Screening and Hiring Controls

- RampedUp checks references and performs background checks appropriate to role and jurisdiction **before** granting access to production systems and/or Customer Data.
- Background screening scope is risk-based and may include identity verification, employment verification, and criminal background screening where permitted by law.

5.2 Agreements, Code of Conduct, and Confidentiality

- Employees and contractors must acknowledge RampedUp's Code of Conduct and confidentiality obligations as a condition of access.
- Every employee/contractor must sign an agreement to follow RampedUp confidentiality and security standards for handling Customer Data.

5.3 Security Awareness Program (Minimum Annual)

RampedUp implements and maintains an Information Security Awareness Program geared towards employees, contractors, and relevant third parties to ensure understanding of:

- RampedUp's Information Security Program and responsibilities
- Common threats and risks to information resources
- Acceptable use, information classification and privacy
- Social engineering and phishing (including assessments and reinforcement education)
- Secure code training for engineering and role-based security training for specific teams/departments
- Annual crisis management and emergency response exercises
- Annual IT disaster recovery and continuity plan testing, training, and exercises
- Applicable security and privacy laws and regulations (including GDPR and U.S. state privacy laws such as CCPA/CPRA where applicable)

5.4 Security Handling Practices (Operational Expectations)

Personnel are trained and required to take basic steps to maintain security, confidentiality, and integrity of Customer Data, including:

- Locking rooms and file cabinets where records are kept
- Not sharing or openly posting passwords in work areas
- Following clean desk and clear screen expectations
- Encrypting sensitive information when transmitted electronically over public/untrusted networks
- Reporting suspicious attempts to obtain Customer Data to designated personnel immediately

5.5 Attestations

Upon reasonable request and subject to confidentiality constraints, RampedUp can provide attestations confirming completion of employee screening and required training.

5.6 Access Restriction by Business Need

Access to Customer Data is limited to employees/contractors with a documented business need, using least-privilege and role-based controls (see Sections 9–10).

5.7 Disciplinary Measures and Offboarding

- Security policy violations may result in loss of access, disciplinary action, termination, and/or legal action.
- Terminated personnel are prevented from accessing systems by immediate account deactivation, revocation of credentials/tokens, and retrieval of company assets.

---

6. Infrastructure and Third-Party Hosting

6.1 AWS Hosting and Core Controls

RampedUp is hosted on **Amazon Web Services (AWS)** and uses:

- **AWS Key Management Service (KMS)** and **AES-256 encryption** for system backups and key management
- **AWS Backup** with automatic redundancy restoration to protect against disk failures and maintain data integrity
- Regular monitoring of programs (including cost, security, and effectiveness)

6.2 Third-Party / Sub-Processor Management

RampedUp maintains a structured third-party/sub-processor review process and demands equivalent security from its sub-processors listed publicly:

- https://rampedup.io/sub-processors

RampedUp maintains a vendor risk assessment program, including a **23-point vendor risk assessment** for key suppliers and sub-processors. Where appropriate, onboarding and periodic reassessments validate security posture and contractual obligations.

6.3 Assurance and Certifications

RampedUp leverages AWS assurance documentation, including AWS SOC reporting. AWS provides third-party System and Organization Controls (SOC) reports; the **AWS SOC 3 Security, Availability, Confidentiality, & Privacy report** is publicly available from AWS.

The AWS SOC 3 Security, Availability, Confidentiality, & Privacy Report is publicly available as a whitepaper.

---

7. Data Protection (Encryption, Minimization, Retention, Deletion)

7.1 Encryption in Transit

- Data in transit is protected using **TLS 1.2** (or stronger where supported).
- Transmission of sensitive information over untrusted networks must use strong encryption.

7.2 Encryption at Rest and Backups

- Data at rest and backups are encrypted using strong encryption, including **AES-256 via AWS KMS** for backups and key management where applicable.
- Storage media containing sensitive information must be encrypted.

7.3 Cryptographic Erasure and Secure Deletion

- When an account expires or is closed, associated data is deleted using **cryptographic erasure** to ensure it is no longer recoverable.
- Admin users may have permission to delete data from the service, subject to role-based controls and auditability.
- Data provided for specific client relationships is securely deleted or returned at the end of the term using cryptographic erasure.

7.4 Data Retention and Minimization

- RampedUp practices **data minimization**: collect/process/store only the minimum personal data necessary for a specific, defined purpose.
- Certain datasets are not republished if they have not been refreshed within a defined period (e.g., **15 months**).

7.5 Secure Disposal Standard

Where applicable, RampedUp disposes/destroys data using techniques consistent with industry standards for secure sanitization (e.g., cryptographic erasure and secure wipe procedures). Storage media must be securely overwritten/sanitized prior to disposal or reuse.

7.6 Removable Media Restriction

Customer Data must not be stored on removable media (USB flash drives, external drives, tapes, CDs, etc.) except for explicitly approved backup or data interchange purposes, and only with strong encryption and documented controls.

---

8. Acceptable Use, Workstation Security, and Remote Work

8.1 Screen Lock and Inactivity Controls

- Password-activated screen locking must engage after inactivity (maximum **15 minutes**).
- Users must lock screens when leaving devices unattended.

8.2 Password Hygiene and Credential Protection

- Passwords must never be stored in plain text, emailed, shared, or written down.
- Credentials must be kept confidential and conveyed only using secure methods.
- Suspected credential compromise must be reported immediately.

8.3 Mobile Devices (Laptops/Phones/Tablets)

RampedUp maintains policies for appropriate use and protection of laptops, phones, and other mobile devices, including:

- Encryption where supported
- Automatic locking
- Timely updates/patching
- Endpoint protection against malware/spyware where applicable
- Reasonable physical safeguards against loss/theft

8.4 Telecommuting Controls

Remote personnel must maintain protections against viruses, spyware, and unauthorized intrusions, including:

- Updated OS and application patching
- Company-approved endpoint protection and/or malware controls
- Secure network usage practices (avoid insecure public Wi-Fi without approved protections)

---

9. Identification, Authentication, and Password Policy

9.1 Unique User Identity and Lifecycle Management

- Only formally authorized users may access RampedUp systems.
- Each user has a **unique user identity**.
- RampedUp maintains documented procedures for approved account creation, timely removal, and modification (privilege changes) across environments.

9.2 Least Privilege

RampedUp enforces least privilege by limiting access to commands, data, and Information Resources necessary for authorized functions.

9.3 Password Policy (RampedUp Standard)

RampedUp's Password Policy applies to anyone with access to company systems and data:

- Minimum **12 characters**
- Mix of **upper/lowercase, numbers, special characters**
- Password expiration at intervals not exceeding **90 days**
- Prohibits reuse of last **5** passwords
- Password resets/account recovery require secure, verified procedures
- Account lockout after **10** failed login attempts (to defend against brute-force attacks)

Where system enforcement is not technically available, users and administrators must comply with the requirements when selecting passwords.

9.4 Session Controls

- Interactive sessions are terminated/locked after inactivity not exceeding **15 minutes**.

9.5 MFA and Secure Administrative Access

- Multi-factor authentication (MFA) is required for privileged access and administrative consoles, and for remote access pathways into sensitive environments where applicable.

---

10. Access Control (RBAC, Privileged Access, Reviews)

10.1 Role-Based Access Control (RBAC)

RampedUp uses RBAC to ensure only authorized users can access systems that could store or transmit Customer Data. Role categories include:

- **System Administration**

- **Instance Administration**
- **User**

Access is scoped to customer/partner/user data to support least-privilege operations.

10.2 Privileged Access Restrictions

- System administrator/root/privileged access is limited to individuals requiring such access to perform job responsibilities.
- System administrators restrict user access to only the commands, data, and resources necessary for authorized functions.

10.3 Access Reviews

- Privileged access rights are reviewed at least **quarterly**.
- A full access review is performed at minimum **annually**.

10.4 Immediate Deprovisioning

User access is promptly removed upon termination or when access is no longer required.

---

11. System Security (Scanning, Hardening, IDS, Patch/Vuln Remediation)

11.1 Security Alert Monitoring

RampedUp monitors relevant industry and vendor advisories for security alerts pertaining to its networks and information resources to enable timely mitigation.

11.2 Vulnerability Scanning

RampedUp uses industry-standard vulnerability scanning tools and performs scanning at least **monthly**:

- External (internet-facing) Information Resources: **monthly minimum**
- Internal Information Resources: **monthly minimum**

11.3 Vulnerability Remediation and Patch Management

RampedUp maintains a documented remediation process for vulnerabilities discovered through:

- Industry publications/advisories

- Vulnerability scanning
- Malware scanning
- Security log review

Patching and remediation are prioritized based on risk and exploitability, with prompt application of security patches appropriate to severity.

11.4 Intrusion Detection

RampedUp deploys intrusion detection and/or prevention capabilities (IDS/IPS and/or cloud-native detections) in active mode to detect suspicious activity.

11.5 System Hardening

RampedUp hardens Information Resources, including:

- Removing/disabling unused services
- Installing and maintaining appropriate firewall/security group protections
- Closing unused ports
- Changing default account names and/or default passwords
- Restricting administrative access to only those needing it
- Assigning security administration responsibilities for host configuration to designated individuals

---

12. Network Security

12.1 Segmentation and Secure Architecture

RampedUp implements network segmentation patterns appropriate to cloud architecture to isolate internet-facing services from trusted internal services and data stores.

12.2 Protective Controls

RampedUp uses layered controls such as:

- Network filtering devices and firewalling (e.g., security groups)
- IDS/IPS and/or cloud-native threat detection
- Anti-virus & anti-malware solutions where applicable
- Logging/monitoring to detect and respond to unauthorized/suspicious activity

12.3 Encryption Requirements

- Strong encryption is required for transfer of sensitive information outside controlled facilities or over untrusted networks.
- Sensitive information is protected in transit and at rest using strong cryptography (TLS 1.2+ for transit; AES-256 for encrypted backups/at-rest controls where applicable).

12.4 Data Storage Limitations

RampedUp does not store, download, copy, or duplicate Customer Data unless required for delivery of the Services. Where storage is required, Customer Data is protected with strong encryption and logical access controls.

---

13. Monitoring, Logging, and Auditability

13.1 Logging and Monitoring Approach (AWS-Native)

RampedUp uses AWS services (e.g., **CloudTrail**, **VPC Flow Logs**) for logging and monitoring key systems.

13.2 Log Retention and Review

- Monitoring logs are retained for approximately **30–90 days** with periodic review.
- Security-relevant logs (authentication events, administrative actions, access logs, and key security control logs) are retained consistent with business needs and risk; where required for assurance and investigation, RampedUp retains logs for **at least 6 months** to support auditability and incident response.
- Security logs are restricted to authorized individuals.

13.3 Anomaly Detection

RampedUp monitors for indicators of compromise including suspicious inbound/outbound transfers, anomalous access patterns, and unusual administrative activity.

---

14. Incident Response and Notification

14.1 Incident Response Plan

RampedUp maintains a formal Incident Response Plan covering: preparation, identification, containment, investigation, eradication, recovery, follow-up, and monitoring.

Key practices include:

- Centralized logging and monitoring with AWS services (CloudTrail, VPC Flow Logs)
- Ability to quickly isolate affected systems (e.g., security group changes)
- Secure wiping and KMS-based cryptographic controls where applicable
- Engagement with AWS Support for cross-validation where needed

14.2 The 7 Steps of RampedUp Incident Response

1. **Preparation:** Ensure logging is enabled using Amazon EC2, AWS CloudTrail, and VPC Flow Logs; collect and aggregate logs centrally; encrypt sensitive data at rest using AWS KMS.
2. **Identification:** Use behavioral-based rules to identify and detect suspected breaches; determine impacted accounts/systems; open a case with AWS Support for cross-validation.
3. **Containment:** Use AWS CLI/SDK and predefined restrictive security groups; save current security group state; isolate the host with restrictive ingress/egress rules.
4. **Notification:** Notify affected parties via email within **72 hours** of becoming aware, consistent with GDPR expectations. Impacted persons will be notified within **14 business days** if not sooner.
5. **Eradication:** Secure wipe files; response times may be faster with automation; delete any KMS data keys if used.
6. **Recovery:** Restore network access to original state; validate service integrity.
7. **Follow-up:** Verify deletion of data keys (if KMS used), cross-validate with AWS Support, and document findings and response actions; impacted persons notified via email.

14.3 Incident History

RampedUp reports **no personal data breaches in the prior three years**.

---

15. Business Continuity and Disaster Recovery

15.1 BCMS Alignment

RampedUp maintains a Business Continuity Management System (BCMS) aligned with **ISO 22301** (aligned but not formally certified).

15.2 BCP/DR Procedures and Testing

- Documented Business Continuity Plans (BCP) and Disaster Recovery (DR) procedures are maintained and tested periodically.
- Critical data is backed up and available offsite via AWS Backup with encrypted and redundant storage.

16. Physical Security

As a cloud-based provider with a relatively small physical footprint, RampedUp relies primarily on AWS physical security controls for hosting infrastructure. AWS documents a series of controls for their hosting infrastructure. Critical data is backed up and available offsite via AWS Backup, with encrypted and redundant storage. Access to hosting facilities is limited, logged, and monitored

RampedUp also safeguards corporate devices and any physical media in its control:

- Devices and equipment are reasonably safeguarded against unauthorized physical access, damage, loss, theft, and environmental threats.
- Storage media containing sensitive information must be encrypted and sanitized before disposal or reuse.

---

17. Privacy, Compliance, and DPO Function

17.1 Privacy Program

RampedUp maintains documented privacy and security controls to comply with applicable privacy laws inside and outside the United States, including EU/UK data protection laws and U.S. state privacy laws such as **CCPA/CPRA** where applicable.

- Privacy Policy: https://rampedup.io/privacy-policy-1

17.2 DPO Function

RampedUp maintains a **Data Protection Officer (DPO) function** to support privacy governance and regulatory alignment where required.

---

18. Data Broker Registrations (U.S.)

RampedUp maintains active data broker registrations in U.S. states where registration is currently required, including:

- **California Data Broker Registration Number: 538248**
  CPPA manages California's Data Broker Registry.

- **Oregon Data Broker Registration Number: 00344**
  Oregon registry is managed by the Department of Consumer and Business Services.
- **Texas Data Broker Registration Number: 20250186**
  Registry info: https://www.sos.state.tx.us/statdoc/data-brokers.shtml
- **Vermont Data Broker Registration Number: 0409326**
  Registry search: https://bizfilings.vermont.gov/homepage

---

19. Vendor Risk Management and Sub-Processors

RampedUp maintains a vendor risk assessment program and structured third-party/sub-processor review process. Sub-processors are disclosed publicly and subject to ongoing review expectations:

- https://rampedup.io/sub-processors

---

20. Enforcement, Exceptions, and Continuous Improvement

20.1 Enforcement

This Policy is enforceable for all covered personnel and third parties. Violations may result in loss of access, disciplinary action, termination, contract termination, and/or legal consequences.

20.2 Exceptions

Exceptions require:

- Documented justification and risk assessment
- Approval by the Security Lead/ISO
- Compensating controls
- Time-bounded review and renewal/closure

20.3 Continuous Improvement

RampedUp reviews this Policy regularly to stay aligned with evolving technologies, threats, business changes, and applicable legal/regulatory requirements.