RAMPEDUP

Data Security Policy

Governance and control requirements for protecting RampedUp systems, services, and data

POLICY OBJECTIVE
Protect the confidentiality, integrity, and availability of information entrusted to RampedUp through proportionate administrative, technical, and physical safeguards.

Document owner	Security & Compliance function
Approved by	Senior Management
Version	1.0
Effective date	Upon approval
Review cycle	At least annually and after material change
Classification	Internal Policy; customer-shareable on approval

Source baseline: RampedUp Data Security webpage, accessed September 1, 2026

1. Purpose

This policy establishes the minimum security requirements RampedUp applies to its information systems, cloud infrastructure, workforce practices, vendors, and handling of customer, company, and personal data. Its purpose is to reduce the likelihood and impact of unauthorized access, loss, alteration, disclosure, or disruption.

2. Scope

This policy applies to all RampedUp employees, contractors, temporary personnel, systems, applications, devices, networks, data repositories, and third parties that access, process, store, transmit, or support RampedUp information or services. It applies throughout the information lifecycle, from collection and creation through use, sharing, retention, return, and deletion.

3. Policy Governance

RampedUp shall maintain a documented information security program that is approved by senior management, communicated to relevant personnel, assigned to accountable owners, and reviewed periodically for continued relevance.

- Senior management approves this policy and provides reasonable resources for implementation.
- The Security & Compliance function coordinates the information security program, monitors compliance, and maintains supporting standards and procedures.
- System and data owners implement controls appropriate to the systems and information for which they are responsible.
- Workforce members acknowledge applicable Code of Conduct and confidentiality obligations and complete required security and privacy training.
- Failure to comply may result in removal of access, disciplinary action, contractual remedies, or legal action, as appropriate.

Supporting documents include the Information Security Policy, Privacy Policy, Code of Conduct, Incident Response Plan, retention requirements, Acceptable Use Policy, BYOD Policy, Business Continuity Plan, and relevant technical documentation.

4. Risk Management and Control Review

RampedUp shall identify and address information security risks using proportionate safeguards and periodic review. Material changes to systems, data use, vendors, threats, or applicable law shall be evaluated for security impact.

- Security controls shall be reviewed periodically and after significant incidents or material changes.
- Known weaknesses shall be documented, prioritized, assigned, and remediated within a timeframe proportionate to risk.
- Security exceptions must be documented, justified, approved by the responsible owner, time-limited where practical, and reviewed before renewal.

5. Infrastructure and Cloud Security

RampedUp hosts its platform and data on Amazon Web Services (AWS). Cloud services shall be configured, monitored, and maintained to support the confidentiality, integrity, and availability of RampedUp information.

- AWS Key Management Service (KMS) shall be used for key management and cryptographic controls where applicable.
- System backups shall use strong encryption, including AES-256 where stated for AWS KMS-protected backups.
- AWS Backup and redundant storage capabilities shall be used to support restoration from disk failure and other recoverable events.
- Cloud security, cost, and operational effectiveness shall be reviewed regularly.
- Physical and environmental security for AWS hosting facilities is managed through AWS controls; access to those facilities is restricted, logged, and monitored by AWS.

6. Data Protection and Encryption

RampedUp shall use layered safeguards to protect information in transit, at rest, and in backup repositories.

6.1 Encryption in transit

Data transmitted over external or untrusted networks shall be protected using TLS 1.2 or a stronger approved protocol where supported. Insecure protocols shall not be used to transmit credentials or sensitive information unless an approved compensating control is in place.

6.2 Encryption at rest and key management

Data at rest and backups shall be encrypted using industry-standard strong encryption appropriate to the service, including AES-256 through AWS KMS where applicable. Cryptographic keys shall be access-controlled and managed separately from protected data to the extent supported by the platform.

6.3 Sensitive information

Credentials, authentication data, and other sensitive information shall be protected through appropriate access controls, encryption, and segregation of duties. RampedUp employees shall not have access to customer passwords by design.

7. Identity and Access Management

Access to non-public RampedUp systems and information shall be limited to formally authorized users and granted according to business need and least privilege.

- Each authorized user shall have a unique user identity; shared accounts are prohibited unless technically necessary, documented, and controlled.
- Access shall be assigned using role-based controls. Relevant roles include System Administration, Instance Administration, and User, with access scoped to customer, partner, or user data.
- Access rights shall be reviewed periodically and adjusted or removed when responsibilities change or access is no longer required.
- Privileged access shall be limited to authorized personnel and used only for approved administrative purposes.
- Directors responsible for information systems shall ensure that systems are protected from unauthorized access, theft, damage, and unintended use.

8. Password and Authentication Requirements

All persons with access to RampedUp systems and data shall follow these minimum password requirements:

- Passwords must contain at least 12 characters and include uppercase letters, lowercase letters, numbers, and special characters where the system supports those controls.
- Passwords must be changed at least every 90 days where password-based authentication is used and enforced by the system.
- The previous five passwords must not be reused.
- Passwords must not be stored in plain text, emailed, shared, or written down in an insecure manner.
- Accounts shall be locked or otherwise protected after 10 failed login attempts to reduce brute-force risk.
- Password resets and account recovery must use secure identity-verification procedures.

9. Logging, Monitoring, and Security Operations

RampedUp shall maintain logging and monitoring appropriate to the risk and criticality of its systems. AWS services such as CloudTrail and VPC Flow Logs may be used to record activity and network events for key systems.

- Monitoring logs shall generally be retained for approximately 30 to 90 days, subject to system capability, operational need, legal obligation, and incident preservation requirements.
- Logs and alerts shall be reviewed periodically to identify suspicious activity, operational issues, and control failures.
- Access to logs shall be restricted to authorized personnel, and relevant evidence shall be preserved when an investigation or legal obligation requires it.
- Affected systems may be isolated promptly, including through security-group or comparable configuration changes.

10. Incident Response and Breach Notification

RampedUp shall maintain and periodically test a formal Incident Response Plan covering preparation, identification, containment, investigation, eradication, recovery, follow-up, and monitoring.

- Suspected security events must be reported promptly through established internal channels.
- Incidents shall be triaged, documented, assigned, investigated, contained, and remediated according to severity.
- Secure wiping and KMS-based cryptographic controls shall be used where appropriate during containment or remediation.
- Where a personal data breach involves client data, affected customers shall be notified within 72 hours after RampedUp becomes aware of the breach, consistent with applicable contractual and legal requirements.
- Impacted persons shall be notified within 14 business days where notification is required, unless applicable law requires a shorter period or law enforcement directs a delay.
- Lessons learned shall be documented and used to improve controls.

Historical statements about the absence of prior breaches are point-in-time disclosures and are not ongoing policy requirements.

11. Data Retention, Minimization, and Secure Deletion

RampedUp shall collect, process, and retain only the information reasonably necessary for defined business, legal, contractual, or operational purposes and shall not retain information longer than necessary.

- Retention periods shall be defined by data category, purpose, contract, and applicable legal requirements.

- Certain datasets shall not be republished when they have not been refreshed within the defined period; the current published example is 15 months.
- Authorized administrators may delete data from RampedUp services in accordance with access controls and approved procedures.
- At the end of a contract or account lifecycle, client-related data shall be returned or securely deleted as required by contract and policy.
- Cryptographic erasure shall be used where applicable so that deleted data is no longer recoverable through access to the relevant encryption keys.
- Legal holds, dispute preservation, or other binding obligations may suspend ordinary deletion schedules.

RampedUp shall not intentionally source data from websites directed to minors or websites that are obviously soliciting information from minors.

12. Third-Party and Sub-Processor Security

Third parties that access, process, store, transmit, or materially support RampedUp information shall be evaluated and managed according to the risk they present.

- RampedUp shall maintain a structured vendor risk assessment process, including its 23-point assessment for key suppliers and sub-processors.
- Security, privacy, confidentiality, availability, and data-handling expectations shall be addressed through contracts or other appropriate controls.
- Responsible system owners shall ensure that third parties understand and uphold their security responsibilities.
- Material sub-processors shall be maintained on RampedUp's public sub-processor list at https://rampedup.io/sub-processors.
- Third-party performance and risk shall be reviewed periodically and when material changes occur.

13. Business Continuity and Disaster Recovery

RampedUp shall maintain business continuity and disaster recovery capabilities designed to sustain or restore critical services following disruption.

- The Business Continuity Management System is aligned with ISO 22301 but is not represented as formally certified.
- Business Continuity Plans and Disaster Recovery procedures shall be documented, assigned, maintained, and tested periodically.
- Critical data shall be backed up using encrypted and redundant storage, with offsite availability through AWS Backup.
- Recovery objectives shall be defined and monitored for critical services.
- Disaster recovery and communication exercises shall be performed periodically, and test reports and corrective actions shall be retained internally.

14. Security Awareness and Workforce Responsibilities

Personnel shall receive security and privacy awareness training appropriate to their responsibilities, including responsibilities under incident response and business continuity processes.

- Training shall be provided during onboarding and refreshed periodically for relevant personnel.
- Personnel shall protect authentication information, follow acceptable-use requirements, report suspected incidents, and handle information according to its sensitivity.

- Managers shall ensure that personnel understand role-specific security duties and that access is updated when roles change or employment ends.

15. Privacy and Legal Compliance

RampedUp shall maintain security and privacy controls designed to support compliance with applicable privacy and data-protection requirements, including applicable EU and UK data-protection laws and U.S. state privacy laws such as the CCPA/CPRA. The Data Protection Officer function shall advise on privacy obligations and coordinate relevant governance activities.

This policy does not replace legal analysis. Where law, regulation, or contract imposes a stricter requirement, the stricter requirement shall control.

16. Assurance and External Reports

RampedUp may rely on independent assurance reports and control documentation from service providers as part of its vendor and infrastructure oversight. AWS provides third-party System and Organization Controls reports, including a publicly available AWS SOC 3 report. AWS assurance reports shall not be represented as certifications held by RampedUp.

17. Exceptions

Exceptions to this policy require documented business justification, a risk assessment, compensating controls where appropriate, approval by the responsible system or data owner and the Security & Compliance function, and an expiration or review date. Exceptions that create material legal, contractual, or customer risk require senior-management approval.

18. Enforcement

Violations of this policy may result in access restriction or removal, disciplinary action up to and including termination of employment or contract, contractual remedies, and referral for legal action. Enforcement shall be consistent with applicable law and contractual obligations.

19. Review and Maintenance

This policy shall be reviewed at least annually and after material changes to RampedUp's services, infrastructure, threat environment, legal obligations, or following a significant security incident. Changes must be documented and approved by senior management. Superseded versions shall be retained in accordance with document-retention requirements.

20. Related Documents and References

- RampedUp Data Security: https://rampedup.io/data-security
- RampedUp Sub-Processors: https://rampedup.io/sub-processors
- RampedUp Incident Response Plan
- RampedUp Business Continuity Plan
- RampedUp Retention Policy
- RampedUp Acceptable Use Policy
- RampedUp BYOD Policy
- RampedUp Employee Code of Conduct

- RampedUp Privacy Policy and Information Security documentation

Approval

Approved by	Scott Miller
Title	CEO
Signature	
Date	09-16-2026

CERTIFICATE *of* SIGNATURE

REF. NUMBER
5DWPE-3HEJT-BEH26-BP7QS

DOCUMENT COMPLETED BY ALL PARTIES ON
16 SEP 2026 23:54:58
UTC

SIGNER	TIMESTAMP	SIGNATURE
SCOTT MILLER EMAIL SCOTT.MILLER@RAMPEDUP.IO	SENT 16 SEP 2026 23:54:58 SIGNED 16 SEP 2026 23:54:58	 IP ADDRESS 99.34.61.134 LOCATION ATLANTA, UNITED STATES