



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

INFINI SYSTEMS LIMITED

(a Veefin Group company)

CIN: [U72300MH2010PLC20509] | Registered Office: [Global One, 2nd Floor, Office 1, CTS No. 252/252-1, Opp. SBI, LBS Marg, Kurla (W), Mumbai, Maharashtra, 400070]

INFORMATION SECURITY POLICY

Document Title	Information Security Policy
Classification	Confidential — Internal Use Only
Version	1.0
Effective Date	01-08-2026
Next Review Date	01-08-2027
Approved By	Board of Directors, Infini Systems Limited



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

Table of Contents

1. Purpose and Scope.....	4
1.1 Scope.....	4
1.2 Internal Enforcement.....	4
2. Regulatory and Contractual Framework.....	4
2.1 Capacity in which Credit Information is Accessed	4
2.2 Legal and Regulatory Instruments	4
2.3 Data Localisation Position.....	4
3. Information Security Governance.....	5
3.1 Roles and Responsibilities.....	5
3.2 Board Approval	5
3.3 Risk Management	5
4. Overview of the Technical Environment.....	5
4.1 AWS Components	5
4.2 Environment Segregation	5
4.3 High-Level Data Flow (Bureau Integration).....	5
5. Asset Management and Data Classification.....	6
5.1 Asset Inventory	6
5.2 Data Classification and Handling.....	6
6. Access Control.....	6
6.1 Principles.....	6
6.2 Password and Credential Standard.....	7
6.3 Authentication to the Bureau API.....	7
6.4 Access Review, Joiner-Mover-Leaver and Revocation.....	8
7. Cloud Infrastructure Security.....	8
7.1 Shared Responsibility.....	8
7.2 Amazon EC2	8
7.3 AWS Lambda.....	8
7.4 Amazon API Gateway.....	9
7.5 Configuration Baselines	9
8. Network Security	9
9. Endpoint, Email and Remote Access Security.....	9
9.1 Endpoint Security.....	9
9.2 Bring Your Own Device	10
9.3 Email and Messaging Security.....	10
10. Data Security, Encryption and Retention.....	10



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

10.1 Encryption at Rest.....	10
10.2 Encryption in Transit	10
10.3 Data Minimization, Consent and Retention.....	10
10.4 Secure Disposal	11
10.5 Restriction on Use and Sharing of Credit Information	11
11. Application Security and Secure Development.....	11
12. Change Management.....	11
13. Logging, Monitoring and Audit	12
13.1 Log Generation and Content.....	12
13.2 Log Protection and Retention	12
14. Incident Response and Breach Notification.....	12
15. Human Resources Security	12



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

1. Purpose and Scope

This Information Security Policy (the “Policy”) sets out the administrative, technical and physical controls implemented by Infini Systems Limited (the “Company”) to protect the confidentiality, integrity and availability of information assets, including credit information obtained from, processed through, or transmitted to a Credit Information Company (the “Bureau”).

The Policy is the Company’s governing information security document. It is the parent document to the Company’s standards and procedures listed in Section 3.3, including the Information Security Incident Management Policy, which addresses incident detection and response procedures only.

1.1 Scope

This Policy applies to:

- **All personnel** — employees, interns, contractors, consultants and third-party personnel who design, develop, operate, support or administer systems in scope.
- **All systems** — the application layer, API integration layer, backend services, data stores, endpoints and cloud infrastructure described in Section 4 that request, receive, process, store or transmit credit information .
- **All environments** — Production, UAT and Development.
- **All information** — credit information, personal data, authentication secrets and supporting business data, classified in accordance with Section 5.

1.2 Internal Enforcement

Compliance with this Policy is mandatory. Non-compliance may result in withdrawal of system access and disciplinary action under the Company’s HR policy, up to and including termination of employment or contract, and, where applicable, civil or criminal proceedings.

2. Regulatory and Contractual Framework

2.1 Capacity in which Credit Information is Accessed

The Company accesses credit information in the capacity of **Specified User under Section 2(I)(i)(viii) of CICRA read with the applicable RBI notification**. The permitted purpose for which credit information is obtained is set out in the Company’s business-purpose note and is reflected in the technical controls described in Sections 6, 10 and 11.

2.2 Legal and Regulatory Instruments

The Company’s information security programme is designed with reference to the applicable laws, to the extent relevant to the Company.

2.3 Data Localisation Position

Credit information and associated personal data obtained from the Bureau is processed and stored exclusively within Amazon Web Services (AWS) India regions.



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

3. Information Security Governance

3.1 Roles and Responsibilities

Role	Responsibility
Board of Directors	Approves this Policy and reviews the Company's risk posture at least annually.
Cloud / DevOps Lead	Manages AWS account security, IAM, network architecture, configuration baselines, and hardening of EC2, Lambda and API Gateway.
Internal Audit / Compliance	Conducts periodic control testing, tracks remediation to closure, and coordinates external VAPT, IS/CISA audits .
Human Resources	Owns background verification, confidentiality undertakings, training completion records and the joiner-mover-leaver process (Section 15).

3.2 Board Approval

This Policy has been reviewed and approved by the Board of Directors of Infini Systems Limited as the Company's governing Information Security Policy.

3.3 Risk Management

The Company maintains a record covering information security and privacy risks to systems in scope. Risks are assessed at least annually and on material change (new integration, new cloud service, significant incident, regulatory change), scored on likelihood and impact, and reported to the internal departments.

4. Overview of the Technical Environment

4.1 AWS Components

The Company's platform that consumes and processes bureau credit information is hosted entirely on Amazon Web Services.

4.2 Environment Segregation

Production, UAT and Development run within a single AWS account in separate, access-controlled **VPCs**, with no network path from lower environments into Production. Production credentials, production Bureau API keys and live credit information are never used, copied or replicated into non-production environments. Test data used in UAT and Development is synthetic or irreversibly masked.

4.3 High-Level Data Flow (Bureau Integration)

- An authenticated consuming application initiates a credit-report request through an internal API exposed via Amazon API Gateway, accompanied by a consent reference captured in accordance with Section 10.3.
- API Gateway authenticates the caller, validates the request schema, applies throttling, and invokes the AWS Lambda function that composes the outbound bureau request.



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

- The Lambda function retrieves the Bureau API key, API secret and admin code from AWS Secrets Manager at runtime, generates the HMAC-SHA256 signature, and calls the Bureau endpoint over TLS 1.2 or higher through a controlled NAT egress path with fixed IP addresses.
- The bureau response is processed in memory. Only the fields required for the permitted purpose are persisted, encrypted at rest using AWS KMS, in accordance with the retention limits in Section 10.3.
- The response is returned only to the entitled consuming entity that initiated the request, under the permitted purpose and consent recorded for that request (see Section 10.5).
- Request and response **metadata** — timestamp, caller identity, consent reference, purpose code and response status — is logged to CloudWatch and CloudTrail for audit. Full bureau payloads are excluded from general-purpose application logs (see Section 13).

5. Asset Management and Data Classification

5.1 Asset Inventory

The Company maintains an inventory of information assets covering AWS accounts and services, data stores, applications, third-party integrations, endpoints and source code repositories.

5.2 Data Classification and Handling

Classification	Examples	Handling Requirement
Restricted	bureau credit information, consumer personal data, KYC data, authentication secrets and API keys	Encrypted at rest and in transit; access on a named-user, least-privilege basis with documented approval; full audit logging; retention limits enforced; no storage on endpoints or removable media; no transmission over public channels such as personal email or consumer messaging apps.
Confidential	Internal system design, architecture documents, contracts, business and financial data	Encrypted at rest; access restricted to authorised roles; external sharing only on confidentiality basis.
Internal	Internal documentation, non-sensitive configuration, team process material	Access restricted to employees and contractors.
Public	Marketing material, published product documentation	No special handling; release subject to normal review.

All credit information sourced from the Bureau is classified **Restricted** by default, irrespective of the medium in which it is held.

6. Access Control

6.1 Principles



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

- Access to AWS accounts, source code, and any system that can reach the bureau integration is granted on a least-privilege, need-to-know basis, and requires documented approval from the relevant Application or System Owner.
- Access is granted against named individual identities. Shared, generic or group accounts are prohibited; where a technical account is unavoidable, it is documented, its credentials are vaulted, and its use is attributable through logging.
- Role-based access control is implemented through IAM roles and policies federated through single sign-on, rather than long-lived individual IAM user credentials. Programmatic access from Lambda and EC2 uses IAM roles with scoped permissions, not static access keys.
- Multi-factor authentication is mandatory for the AWS root account (which is not used for operational tasks and whose credentials are sealed and stored securely), for all console and API access, for VPN and remote access, and for source control and CI/CD tooling.
- Privileged and administrative access, including access to the Bureau API secret in AWS Secrets Manager, is restricted to a small named group, granted just-in-time where technically feasible, and logged with alerting on use.
- Segregation of duties is maintained between development, QA and production deployment; no single individual can both author and independently release a change to Production.

6.2 Password and Credential Standard

Control	Requirement
Composition	A mix of upper case, lower case, numeric and special characters; dictionary words, sequences and user-identifiable strings are rejected.
Reuse and history	The previous 5 passwords cannot be reused.
Rotation	Rotation on suspected compromise, on role change, and on exit of any individual who knew the credential. Time-based rotation is applied where mandated by a system or by contract.
Failed attempts	Account lockout after 5 consecutive failed attempts, with lockout duration and reset defined in the Access Control Standard.
Session controls	Idle session timeout of 15 minutes for administrative consoles; re-authentication required for privileged operations.
Storage	Passwords are stored only as salted hashes using an approved algorithm. Credentials are never stored in plaintext, in source code, in configuration files, in tickets or in chat.
Initial and temporary credentials	Issued out-of-band, single-use, and forced to change on first login.

6.3 Authentication to the Bureau API

Outbound calls to the Bureau are authenticated using the API key, API secret and admin code issued during onboarding, with each request signed using HMAC-SHA256 in accordance with the Bureau's integration specification. These credentials are held only in AWS Secrets Manager, encrypted with a dedicated KMS key, retrieved at runtime by the Lambda execution role, and are never embedded in application code, container images, environment variables, logs or support tickets. Read access to the



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

secret is limited to the Lambda execution role and to a named break-glass group, and every retrieval outside the execution role generates an alert.

6.4 Access Review, Joiner-Mover-Leaver and Revocation

- Access to all systems in scope is reviewed periodically by the relevant System Owner, with the review evidenced and retained for audit. Privileged access and access to the bureau integration are reviewed as well.
- Access changes on internal transfer are processed within 2 working days, and access no longer required is removed rather than accumulated.
- Access for departing employees and contractors is revoked within **24 hours** of exit, and immediately on involuntary termination, including AWS, SSO, VPN, source control, CI/CD, email and physical access.
- Dormant accounts with no activity for 90 days are disabled automatically pending review.

7. Cloud Infrastructure Security

7.1 Shared Responsibility

The Company operates under the AWS Shared Responsibility Model. AWS is responsible for security **of** the cloud — physical data centers, host infrastructure and the hypervisor. The Company is responsible for security **in** the cloud — configuration of EC2, Lambda, API Gateway, IAM and networking, data encryption, identity management, and patching of guest operating systems and application code.

7.2 Amazon EC2

- Instances are built from hardened, patched golden AMIs derived from a documented configuration baseline (CIS Benchmark aligned); unnecessary services and ports are disabled.
- Instances run in private subnets without public IP addresses. Administrative access is via AWS Systems Manager Session Manager rather than open SSH; where a bastion is used, it is restricted by Security Group to named source addresses and requires MFA.
- Security Groups follow default-deny with explicit least-privilege inbound rules. Changes are made through the change management process in Section 12.
- EBS volumes are encrypted with AWS KMS, with EBS encryption-by-default enabled at account level.
- Patches are applied on a risk-prioritized basis following vendor release, tracked through AWS Systems Manager Patch Manager and reported to the IT Steering Committee.

7.3 AWS Lambda

- Each function is assigned a dedicated IAM execution role scoped only to the resources it requires, such as a specific secret or a specific table.
- Functions handling bureau requests run inside the VPC, with outbound bureau calls traversing a controlled NAT egress path with fixed Elastic IP addresses, enabling IP allow-listing on the Bureau side.
- Environment variables containing sensitive configuration are encrypted with KMS; secrets are fetched at runtime from Secrets Manager rather than stored as plaintext environment variables.



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

-
- Function code and dependencies are deployed only through the CI/CD pipeline; direct console edits to Production function code are disabled by IAM policy.
 - Dependencies are scanned for known vulnerabilities in the pipeline before deployment, per Section 11.

7.4 Amazon API Gateway

- All internal APIs are exposed only through API Gateway, never directly from EC2 or Lambda.
- Authentication and authorization are enforced through IAM authorizers, OAuth 2.0 / JWT authorizers, or mutual TLS as appropriate to the consumer. Anonymous access is not permitted for any endpoint that touches credit information. API keys are used for identification and throttling only, never as the sole authentication mechanism.
- Throttling and usage plans limit request rates and burst per client, protecting both the platform and the upstream bureau relationship from excessive call volumes.
- Request schema validation is enabled to reject malformed input before it reaches backend logic.
- TLS 1.2 or higher is enforced on all endpoints, with a minimum TLS security policy configured on custom domains. AWS WAF is attached to public-facing APIs with managed rule groups covering injection, cross-site scripting, bad inputs and bot traffic, plus rate-based rules.
- Access logging and execution logging are enabled on all stages and shipped to the central log store.

7.5 Configuration Baselines

- AWS Config rules and conformance packs continuously evaluate the account against the configuration baseline; drift generates an alert and a remediation ticket.
- S3 Block Public Access is enabled at account level; public exposure of any resource holding Restricted data is prohibited.

8. Network Security

- Network segmentation places data-tier resources (RDS and ElastiCache) in private subnets with no route to the internet.
- Security Groups and Network ACLs implement default-deny inbound. Outbound traffic to the Bureau is restricted to the documented bureau endpoints, and egress is routed through controlled NAT gateways with fixed IP addresses registered with the Bureau.
- VPC Flow Logs are enabled on all VPCs and retained per Section 13 for audit and forensic purposes.
- Remote access to Production networks is only via **VPN** with MFA; split tunnelling is disabled and access is limited to named personnel.
- Wireless networks at Company premises use WPA2-Enterprise or stronger, with guest networks logically separated from corporate networks.

9. Endpoint, Email and Remote Access Security

9.1 Endpoint Security



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

-
- All Company-issued laptops and workstations used to access systems in scope have enabled endpoint protection / EDR installed and centrally monitored, automatic screen lock after 5 minutes of inactivity, and host firewalls enabled.
 - Operating system and application patches are applied on a risk-prioritized basis, consistent with Section 7.2; endpoints out of compliance are blocked from corporate resources.
 - Local administrator rights are restricted; software installation is limited to an approved list.
 - Removable media is disabled by default. Any exception is approved under Section 22 and requires encryption of the media.
 - Credit information and other Restricted data are not downloaded to, or stored on, endpoints. Where a download is unavoidable for an approved operational purpose, it is time-limited, logged and securely deleted on completion.

9.2 Bring Your Own Device

Personal devices are **not permitted** to access restricted Company systems. Personal devices may not be used to access Restricted data.

9.3 Email and Messaging Security

- Corporate email is protected by anti-malware and anti-phishing filtering, with SPF, DKIM and DMARC published for Company domains.
- External-sender warning banners are applied, and known-malicious attachment types are blocked.
- Credit information and other Restricted data must not be sent over email, personal email accounts, or consumer messaging applications. Where a transfer to an external party is approved, it uses an approved encrypted channel with access controls and expiry.
- Personnel are trained on phishing and social engineering, and simulated phishing exercises are conducted periodically.

10. Data Security, Encryption and Retention

10.1 Encryption at Rest

All Restricted and Confidential data is encrypted at rest using AES-256 through AWS KMS, covering EBS volumes, RDS instances and snapshots, S3 buckets, backups and AWS Secrets Manager. Customer-managed KMS keys are used for data stores holding credit information, with key policies restricted to a named group of key administrators who are separate from the personnel with data-plane access to the underlying data.

10.2 Encryption in Transit

TLS 1.2 or higher is enforced for all traffic, including traffic between internal services, administrative access, and the outbound HMAC-signed calls to the Bureau API. Protocols and cipher suites below TLS 1.2 are disabled. Certificates are managed through AWS Certificate Manager with automated renewal and expiry monitoring.

10.3 Data Minimization, Consent and Retention



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

-
- Consumer consent for accessing credit information is captured **before** any bureau call is made, recorded with a unique consent reference, the purpose, the timestamp, the channel and the identifier of the consumer, and is linked to every resulting bureau request in the audit log.
 - Only the bureau data fields required for the permitted purpose are persisted. Full raw bureau responses are not retained beyond the period operationally necessary to complete the transaction.
 - Personal data is deleted or irreversibly anonymized once the purpose is served and no legal, regulatory or contractual retention obligation remains, consistent with the DPDPA principle of storage limitation.

10.4 Secure Disposal

Decommissioned storage (EBS volumes, RDS snapshots, S3 objects) is deleted through AWS-native secure deletion. Because encryption keys are Company-managed, scheduled deletion of the applicable KMS key or revocation of its grants renders residual ciphertext cryptographically inaccessible in addition to logical deletion. Physical media held at Company premises is wiped to an approved standard or physically destroyed. Paper records containing Restricted data are shredded.

10.5 Restriction on Use and Sharing of Credit Information

Credit information obtained from the Bureau is used for the specific permitted purposes including purpose disclosed to the consumer at the time consent was obtained.

11. Application Security and Secure Development

- A documented secure software development lifecycle is followed, covering design, development, testing, release and decommissioning. Security requirements are considered at design stage for features that handle credit information.
- Access to source code repositories is role-based.
- Application code and third-party dependencies are subject to security testing as part of the development and release process, and identified issues are addressed on a risk-prioritised basis.
- Testing is performed in a non-production environment before releases.
- Segregation of duties is maintained between development, testing and production deployment, and deployment to Production follows a controlled, approved release process.
- Production data is never used for development or testing.

12. Change Management

- All changes to Production systems, infrastructure, network configuration, IAM policies and application code follow a documented Change Management Procedure with a raised, reviewed and approved change record.
- Changes affecting the bureau integration, authentication, encryption, logging or data retention require explicit CISO review.



Infini Systems limited

(Formerly Known as Infini Systems Private Limited)

CIN: U72300MH2010PTC205096

-
- Post-implementation review is performed for major and emergency changes, and failed changes are analyzed and reported to internally.

13. Logging, Monitoring and Audit

13.1 Log Generation and Content

- AWS CloudTrail records all management-plane API activity across every account, with data-plane events enabled for data stores holding credit information. CloudTrail is enabled in all regions and cannot be disabled by operational roles.
- Application logs, API Gateway access and execution logs, Lambda execution logs, VPC Flow Logs, database audit logs, endpoint/EDR logs and GuardDuty findings are collected centrally.
- Security-relevant events are logged with, at minimum: timestamp, event type, source address, user or role identity, target resource and outcome.
- Logs exclude full bureau payloads, authentication secrets, tokens and unmasked personal data. Where a personal identifier must appear for traceability, it is masked or tokenised.

13.2 Log Protection and Retention

- Logs are shipped to a centralised, access-restricted, tamper-evident store — a dedicated logging account with an S3 bucket using versioning, Object Lock and a restrictive bucket policy. Operational roles have write-only access; deletion rights are held by a separate named group.

14. Incident Response and Breach Notification

Incident detection, response, escalation and breach notification (including statutory and contractual notification timelines) are followed as per the Company's Policy.

15. Human Resources Security

- **Pre-employment.** Background verification is conducted for all employees and contractors with access to restricted systems in scope, proportionate to the role, covering identity, address, education, prior employment and, where permitted by law, criminal record checks. Access is not granted until verification is complete or an approved interim risk decision is recorded.
- **Terms of engagement.** All personnel are bound by a confidentiality / non-disclosure undertaking and an acceptable use acknowledgement covering credit information and bureau-related data.
- **During employment.** Personnel complete the training in Section 18 and are subject to the disciplinary process for policy violations.
- **Exit.** A documented exit checklist covers revocation of all access within 24 hours (Section 6.4), return of assets, revocation of physical access, and reminder of continuing confidentiality obligations.
- **Contractors and interns.** Personnel who are not permanent employees are subject to the same background verification, confidentiality, training and access-control requirements, with access time-bound to the engagement period.