(redpoint) SECURITY

code security by coders

REDPOINT SECURITY, INC.

INFORMATION SECURITY POLICY

Date July/24/2025

Version: 1.7

1. INFORMATION SECURITY POLICY

FOCUS

This policy addresses the requirement for an Information Security policy document to provide direction for the dissemination and implementation of Information Security policy across the organization. It includes who is responsible for the policy document and who must adhere to it.

POLICY

1.1 MAINTAIN THE INFORMATION SECURITY POLICY

The Information Security Policy must be reviewed and updated on a regular basis, no less than annually, and when major changes occur to the business that could impact the Redpoint Security, Inc.'s ("Company") security posture.

The Information Security Policy document will be approved by Company Management and published and communicated to all relevant personnel.

1.2 ENFORCEMENT OF POLICY

The Information Security Policy applies to everyone who accesses the Company's non-public information systems. This includes but is not limited to permanent, temporary and contract staff and staff working for other companies but operating on Company's premises.

Managers must ensure that security policies and standards relevant to their area of responsibility are adhered to and carried out correctly.

1.3 NON-COMPLIANCE WITH POLICY

In cases where Company personnel are found to be in non-compliance with this policy, internal disciplinary actions may be taken, including dismissal or legal action.

2. RISK ANALYSIS AND ASSESSMENT

FOCUS

This policy addresses the requirement for an Information Security risk management process to provide a sound basis for allocation of resources to control Information Security risks. It also assigns responsibilities for implementation and control of the Information Security risk management process.

POLICY

2.1 INFORMATION SECURITY RISK MANAGEMENT

Redpoint Security should continuously assess risk to its information systems that support business functions. Once identified, management should establish practical means to mitigate risk and codify these mitigations within this policy.

3. ASSET PROTECTION AND MANAGEMENT

FOCUS

This policy addresses the requirement for establishing an Information Security asset classification and control process to provide appropriate protection of IT resources. It also allocates the responsibilities for implementation and control of the Information Security asset classification and control process.

POLICY

3.1 INVENTORY OF IT INFORMATION ASSETS

To track IT assets, an inventory of IT information assets must be compiled and regularly maintained by IT and TechOps. Asset inventory should list the classification (see table in 3.3) of each asset or the highest level of classification of data processed or stored on that asset.

3.2 RESPONSIBILITY FOR ASSETS

IT asset inventory should identify the owner or person responsible for maintenance of IT security controls for each asset. Each Company asset must have a Company custodian.

Employees should only receive access to assets—and related information—that is necessary to perform their job functions. No employees should obtain access to information that exceeds their job duties as assigned.

3.3 CLASSIFICATION AND LABELING OF IT INFORMATION ASSETS

The originator of the information or the owner of the processing system is responsible for classifying the information or processing system. Classifications should be based on the level of sensitivity associated with the information.

When classifying information, employees should use the following protective markings:

Classification	Required protection	Description
RESTRICTED	High	Only authorized persons with a need to know have access. Unauthorized disclosure or loss of information could cause serious harm to the organization or individuals. **Examples**: personally-identifiable information, encryption keys, cardholder data.
CONFIDENTIAL	Medium	Only authorized persons with a need to know have access. Unauthorized disclosure or loss of information could cause harm to the organization or individuals or violate relevant government laws and regulations. **Examples**: configurations of infrastructure, personnel files.
INTERNAL	Low	Only employees and contractors of the Company have access. Unauthorized disclosure could cause embarrassment. **Examples**: Internal bulletins and information that should not be released to the public or partners.
PUBLIC	Integrity only	Employees and associated parties have access. Unauthorized disclosure would have little bearing on the business. Examples: Personal e-mails, information on the Company website.

All employees must ensure that information assets receive appropriate levels of protection for their classification.

3.4 RECLASSIFICATION OF IT INFORMATION ASSETS

Classifications and protective controls for Company information assets should be suited to business needs for sharing or restricting information and the business impacts associated with such needs.

The originator of information or owner of the processing system should reclassify assets they are responsible for to a lesser classification if they are no longer sensitive and to a higher classification if they have become more sensitive.

Company Management must ensure that all employees:

- Understand the classification system and their responsibilities for protecting Company assets
- Are provided the appropriate tools to handle Company information.

3.5 HANDLING OF INFORMATION ASSETS

3.5.1 STORAGE

All classified information must be stored in a secure manner to prevent access, disclosure, modification or destruction by non-authorized parties.

Digital information should be secured to the same extent that paper-based and physical information assets are secured.

Restricted information should be encrypted using approved encryption and key management methods.

3.5.2 ACCESS AND TRANSMISSION

All classified information must only be accessible by authorized parties. Data in transit between parties must be encrypted and secured from possible breaches of its confidentiality, integrity and availability.

3.5.3 DISPOSAL

Any media containing CONFIDENTIAL or higher data that should no longer be retained must be disposed of in a secure and safe manner as noted below:

- Hard disks: sanitize (7-pass binary wipe), degauss or shred platter.
- USB “thumb” drives, smart cards, and digital media: incinerate, pulverize, or melt.

Before computer or communications equipment can be sent to a vendor for trade-in, servicing, or disposal, all CONFIDENTIAL or higher data must be destroyed or concealed according to the approved methods in this policy.

3.6 HANDLING OF CLOUD-BASED INFORMATION ASSETS

This policy addresses the requirement for the safe, clear, and efficient management of data residing within cloud environments and controlled by the Company.

3.6.1 SANITIZATION PROCEDURES

At the conclusion of a client’s contract, the Company will purge all client-provided designs, code, users, records, data, and uploaded assets from cloud platforms that support the Company’s activities. The Company will not compile and transmit any data back to the client. Upon request, the Company will provide attestation to relevant members of the client team that all data has been sanitized.

3.7 HANDLING OF DEVICES/HARDWARE

3.7.1 STORAGE

All devices that store classified data must be housed in a secure manner to prevent access from non-authorized parties. All employees should take care to prevent theft of his or her IT assets.

3.7.2 ACCESS AND MAINTENANCE

All devices that enable access to classified data must only be accessible by authorized parties. Only authorized users, administrators and maintenance personnel are allowed access to these devices.

In the event that a device containing classified media requires to be returned to the manufacturer or other authorized repairer, the device should be sanitized before being sent.

In the event that a device containing RESTRICTED media needs to be returned to the manufacturer or other authorized repairer, the device must be sanitized before being sent.

If the RESTRICTED media cannot be removed or declassified, then the device must be repaired on site, or the repairer must sign a non-disclosure agreement regarding the contents of the media.

3.7.3 DISPOSAL

All hardware that has processed, transmitted or stored classified data must be sanitized using an approved method before being disposed of or reused.

Company must have a method of verifying that hardware has been appropriately sanitized before being disposed of.

3.8 OFF-SITE USAGE OF ASSETS

Company information and devices must be appropriately secured. Sensitive data should be encrypted on all devices, whether or not they are on Company premises. All encryption keys used to protect sensitive assets must adhere to the Key Management Policy.

4. PHYSICAL SECURITY

FOCUS

This policy addresses the requirement for establishment of a physically secure work and operational environment for staff and information assets. This is to prevent loss or compromise of equipment or information by theft, vandalism or environmental failure.

POLICY

4.1 PHYSICAL ACCESS

As a security service provider, Company does not maintain physical locations for computer equipment or hardware. Employee systems should adhere to all controls listed within this policy and employees should treat all Company devices as sensitive assets.

5. ACCESS CONTROL

FOCUS

This policy addresses the requirement for access control of information systems. The policy is primarily concerned with balancing the restrictions aimed at preventing unauthorized access against the need to provide unimpeded access in accordance with the needs of the business.

POLICY

5.1 ACCESS CONTROL

Access to the Company environments and assets is through appropriate authentication, such as username and password or encryption key. Each employee must have a unique username and password. Employees must keep their passwords private.

If the environment or asset supports multi-factor authentication (MFA), authentication using MFA should be required for access.

Where appropriate, administrators must have separate administrator accounts, which are separate from their user accounts.

5.2 REGISTRATION PROCESS

All account creation requests must go through a formal registration process. Users must have a clear business need to access any systems to which they request access.

All requests for new accounts and access to systems or secure areas must originate with the requestor's manager and be approved by the appropriate system or business owner. In sensitive cases approval from the CTO may be required.

5.3 USER ACCOUNT MANAGEMENT

All users should have a unique identification associated with them in order to access any Company systems and devices. Shared or group accounts must not have access to RESTRICTED information.

5.4 PRIVILEGED ACCESS MANAGEMENT

Administrators must have separate administrator accounts that will be used for administration purposes only.

5.5 USER RESPONSIBILITIES

Users are responsible for ensuring that their individual password remains a secret. Passwords must not be shared within teams or areas.

5.6 PASSWORDS

The allocation of passwords must be controlled through a formal registration and management process.

Company non-public systems must identify and authenticate users before any access is given.

Creation and maintenance of passwords must be based on the asset protected including l*ength, complexity, expiration, reuse following approved password standards, etc.*

5.7 SESSION TIMEOUT

All connections must be configured to timeout after a designated period of inactivity. Reconnection to the resource must be controlled through the use of an appropriate authentication method.

For systems that support it, screen savers should be active, timeout capability enabled after 10 minutes or less.

User authentication through passwords or other mechanisms (e.g. fingerprint, facial recognition) for all screen savers should be enabled.

5.8 MOBILE COMPUTING AND TELEWORKING

The use of mobile devices that access privileged Company resources is to be controlled and authorized by the Company.

Employees must ensure that Company resources and information is given adequate protection. Due care must be exercised that Company and client data is not compromised.

6. OPERATIONAL SECURITY

FOCUS

This policy addresses the correct operation and control of Company communications networks and business application systems to deliver services to Company's partners and clients. This objective will require a broad range of policy elements to ensure compliance with government or statutory regulations. This policy also ensures that appropriate controls are in place to protect against threats and that efficient use is made of available resources.

POLICY

6.1 THIRD PARTY SERVICE DELIVERY MANAGEMENT

Company should ensure that any operational services delivered by third parties are of a high standard and meet the expectations of the agreements.

6.2 SEPARATION OF ENVIRONMENTS

Company must ensure that development and testing of new systems are separated from the production areas of its cloud-based environments.

Company must document the process for transferring software and data between the development, testing and operational areas. Certain classified data should not be used in development and testing. If real life data is required, it must be properly sanitized before use.

The development and test environments should emulate the operational environment as closely as possible to avoid conflicts between different infrastructures.

6.3 EXCHANGE OF INFORMATION

Exchange of information to third parties is governed by the relationship between the parties and the sensitivity of the information. The level of protection should be formally defined and agreed upon before transmitting data to a third party.

6.4 MONITORING

The Company must monitor sensitive systems for usage and access. The Company should monitor for the following inappropriate and malicious content stored on Company devices, including electronic intrusions (worms, viruses and targeted attacks to the system).

6.5 MALICIOUS CODE AND ANTIVIRUS

Antivirus software should be installed on all Company workstations, laptops and servers that are commonly affected by malicious software. Incoming files should be screened for malicious code and viruses before being executed or accessed.

All files containing software or executable statements (including word processing and spreadsheet files) should be screened for viruses and shown to be virus free prior to being transmitted out of the Company network.

Virus checker applications should have automatic updating of signature files enabled and Company should be subscribed to an Antivirus alert and update service. Updates for virus definition and signature files should be on an ongoing basis.

7. AI TOOL USAGE AND DATA PROTECTION

FOCUS

Redpoint Security is committed to leveraging the power of Artificial Intelligence (AI) to enhance the speed, accuracy, and depth of our application security services, including dynamic web and mobile application pentests, secure-code reviews, and hybrid application security assessments. We recognize the immense potential of AI in information gathering, vulnerability identification, and even suggesting remediation strategies.

However, our paramount commitment is to the security and privacy of our customers' sensitive data. This policy outlines our approach to integrating AI tools while upholding the highest standards of data protection and ethical use.

POLICY

7.1 DATA MINIMIZATION AND ANONYMIZATION

- **Rule:** Company will only feed AI models the absolute minimum amount of data required for a given task. Wherever possible, sensitive customer data will be anonymized or de-identified before being used with AI tools, especially with external models.
- **Prohibited:** Inputting raw, unredacted sensitive customer data (e.g., personally identifiable information, financial data, health information, intellectual property) into any AI model, particularly cloud-based or publicly accessible models, without explicit, documented approval and stringent controls.

7.2 LOCALLY DEPLOYED MODELS FOR SENSITIVE DATA

- **Rule:** For tasks involving highly sensitive customer data (e.g., proprietary source code, critical infrastructure details, internal network configurations), Company will prioritize and, where feasible, mandate the use of AI models deployed and run entirely within our secure, on-premises infrastructure or private, dedicated cloud environments. This ensures data never leaves our controlled ecosystem.
- **Benefit:** Locally deployed models offer maximum data sovereignty, guaranteed privacy, and deterministic, versioned behavior, allowing us to maintain complete control and auditability over the AI's interaction with sensitive information.

7.3 STRICT DATA GOVERNANCE AND ACCESS CONTROLS

- **Rule:** All data used with AI tools, whether internal or external, will be subject to robust data governance framework and strict role-based access controls (RBAC). Only authorized personnel with a legitimate business need will have access to the AI tools and the data fed into them.
- **Prohibited:** Unauthorized access or use of AI tools for processing customer data or sharing AI-generated insights derived from sensitive data with unauthorized individuals or entities.

7.4 MODEL SELECTION AND VETTING

- **Rule:** Before integrating any AI tool or model into our processes, a comprehensive security and privacy review will be conducted. This includes evaluating the model's architecture, data handling practices, security controls, and adherence to relevant industry standards and regulations (e.g., GDPR, HIPAA, ISO 27001). We will prioritize models with clear documentation on their data retention policies, security certifications, and auditability.
- **Prohibited Models:**
  - **Publicly accessible, general-purpose LLMs (Large Language Models) without specific, secure API integrations:** Unless a model is explicitly designed for secure enterprise use with robust data isolation and privacy guarantees (e.g., a private instance of a commercial LLM with a strict "no training on user data" policy), our employees are forbidden from inputting any customer data into them. This includes popular, free-tier conversational AI tools.
  - **Models with unclear or non-existent data retention/deletion policies:** We will not use models that do not provide transparent information about how data is processed, stored, and deleted.
  - **Models that explicitly state they use user input for continuous training without opt-out options:** This directly conflicts with our data privacy commitments.

7.5 EMPLOYEE TRAINING AND AWARENESS

- **Rule:** All employees utilizing AI tools will receive mandatory training on this policy, secure AI hygiene, data protection best practices, and the specific limitations and risks associated with different AI models. They will be educated on prompt engineering techniques that minimize sensitive data exposure.
- **Prohibited:** Bypassing security controls, attempting to "jailbreak" AI models, or knowingly inputting data into models that violate this policy.

7.6 CONTINUOUS MONITORING AND AUDITING

- **Rule:** Company's use of AI tools will be continuously monitored and audited to ensure compliance with this policy and to identify any potential data leakage or misuse. This includes logging AI tool usage, input data, and outputs.
- **Prohibited:** Disabling or circumventing monitoring and logging mechanisms for AI tool usage.

7.7 OUTPUT VALIDATION AND HUMAN OVERSIGHT

- **Rule:** AI-generated insights, findings, or code suggestions will always be validated and reviewed by a human expert. AI tools are considered assistants, not replacements for human judgment and expertise in security assessments.
- **Prohibited:** Blindly trusting or acting upon AI-generated outputs without thorough human review and validation, especially when those outputs pertain to vulnerability identification or remediation.

7.8 VENDOR AGREEMENTS AND DUE DILIGENCE

- **Rule:** For any third-party AI service or model, we will establish robust contractual agreements that explicitly outline data ownership, usage, security, and privacy obligations, ensuring alignment with our customer data protection commitments. This includes rigorous vendor due diligence.

7.8.1 SPECIFIC APPLICATIONS OF AI IN OUR SERVICES (WITH SECURITY CONSIDERATIONS)

Our goal is to incorporate LLM agents and AI tooling into our testing processes to deliver the best results possible to our clients. The following are the acceptable uses of AI tools as well as the processes we have in place to protect sensitive client data.

- **Speeding up Information Gathering:** AI can quickly process publicly available information, open-source intelligence (OSINT), and vast codebases to identify potential attack surface areas, dependencies, and configurations.
    - **Security Control:** When using external AI for OSINT, no customer-sensitive data is provided. When analyzing customer code for dependencies or configurations with AI, local or private cloud-deployed models are preferred, or strict anonymization/redaction is applied if external models are deemed necessary for specific tasks.
- **Identification of Potentially Sensitive Endpoints and Data Flows:** AI can analyze network traffic logs, Dynamic requests and responses acquired through a web proxy, API specifications, and application configurations to highlight endpoints that might process sensitive data or have exploitable access controls.
    - **Security Control:** This will primarily involve local analysis using our own tools and locally deployed AI models. If cloud-based AI is used for high-level pattern recognition on anonymized metadata, strict data ingress/egress controls and data minimization techniques will be enforced.
- **Automated Vulnerability Identification (Initial Triage):** AI can assist in rapidly scanning large codebases or application surfaces for common vulnerability patterns (e.g., OWASP Top 10, common misconfigurations).
    - **Security Control:** For static and dynamic analysis, our preference is for integrated AI capabilities within our licensed security tools that can operate locally or within our secure private cloud. When leveraging external AI services, only code snippets or non-sensitive, anonymized data will be used.
- **Suggesting Remediation Strategies:** AI can propose potential fixes or mitigation strategies based on identified vulnerabilities.
    - **Security Control:** These suggestions are always reviewed and refined by human experts before being presented to customers. No sensitive customer data is shared with external AI models for the purpose of generating remediation advice.

8. DEVELOPMENT AND MAINTENANCE

FOCUS

This policy addresses the requirement for consideration of security in the development and maintenance phases of system lifecycles. In order to build security into Company information systems a broad range of policy elements need to be specified so that appropriate controls are in place during these phases.

POLICY

8.1 CORRECT PROCESSING IN APPLICATIONS

To prevent errors, loss, unauthorized modification or misuse of information in applications, input and output data validation and internal processing validation must be performed by all applications processing Company data.

Input data should be checked for at least the following conditions:

- Out of range values
- Invalid characters in data fields
- Missing or incomplete data
- Exceeding upper and lower data volume limits
- Unauthorized or inconsistent control data.

Output data should be checked for at least the following conditions:

- Plausibility checks (e.g. requests for single items should not return multiple responses)
- Provide sufficient information for the requestor to determine the accuracy, completeness and classification of the information (the information returned should be readable to the requestor and should only be information that the requestor is authorized to access).
- Dynamic data should be treated as untrusted and therefore protections employed to prevent against rendering potentially unsafe data.
- Errors in the processing of data should never be shown client-side (examples – stack traces, server errors). We should always handle this safely
- Comments should not be overly verbose as to describe the inner-workings or application functionality to the user.

Database queries follow these guidelines:

- Parameterize queries
- Data should never be concatenated within the query
- Parameterized queries should not be concatenated with other parameterized queries or data.
- Treat all dynamic content as untrusted

8.2 CRYPTOGRAPHIC KEY MANAGEMENT

A cryptographic key management policy (*in development)* must be created that covers protection of keys, generation of keys and the use of cryptography in Company.

The cryptographic key management policy must detail the methods used to protect the cryptographic keys in case of theft, loss, damage or other compromise. It should also identify roles and responsibilities of individuals and areas for key management including generation, storage, modification, replacement and disposal.

8.3 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES

Controls must be applied to secure outsourced software development.

Implementation of any application code changes should be controlled by the use of a formal change control procedure to minimize the corruption of information systems.

Access to application source code and libraries should be strictly controlled.

8.3.1 ACQUIRE AND MAINTAIN APPLICATION SOFTWARE

Information Security requirements must be taken into account when acquiring application software through purchasing of off-the-shelf products, customized products, third-party developed products and internally developed products.

8.4 VULNERABILITY MANAGEMENT

To reduce the risks resulting from exploitation of published technical vulnerabilities, configuration management, patch management and operation system and application version control should be established at Company.

8.5 MANAGE CHANGES

All new implementations and major changes to Company applications and systems must undergo a formal change control procedure.

8.5.1 CHANGE CONTROL

All changes to the Company systems are required to go through a formal change control and approval process. This should include but is not limited to

- Installation of application and system revisions and patches
- Promoting code from testing to production
- Problem tracking and resolution
- Introducing new systems or system functionality.

9. ORGANIZATION AND CONTRACTUAL SECURITY

FOCUS

This policy addresses the requirement for the establishment of an Information Security organization within Company to provide a sound basis for allocation of resources to control implementation and operation of Information Security policies and systems across the Company organization.

POLICY

9.1 INTERNAL ORGANIZATION

Company Management should actively support security within Company through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of Information Security responsibilities.

9.2 EXTERNAL AND THIRD-PARTY COMMUNICATIONS

The Company should ensure that all third-party service providers follow reasonable Information Security policies.

The Company must ensure that appropriate data-sharing, nondisclosure agreements are in place for any service providers that access Company sensitive information.

Information sharing between parties should be controlled with documented processes for protection of information prior to, during, and after data transmission to the third-party.

Company should be aware of all information assets that are accessed by a third-party. The risks associated with access to organizational information processing facilities by third parties must be assessed and appropriate security controls implemented prior to granting that access.

9.3 SERVICE PROVIDER OVERSIGHT

Before entering into a contract for services with an external party accessing Company sensitive systems or information, Company must assess the Information Security policies of the external party.

10. INCIDENT MANAGEMENT AND BUSINESS CONTINUITY

FOCUS

This policy addresses the requirement for incident management and business continuity management. These processes are essential in reducing situations caused by disruptive and unforeseen events. These may be the result of human error, accidents or equipment failures, deliberate actions of attackers over internal or external channels, or natural and man-made disasters. If an incident does occur, all staff must not only report the incident as quickly as possible but also be able to implement the appropriate responsive action to limit the impact of the incident.

POLICY

10.1 INCIDENT RESPONSE PLAN

Company must develop appropriate response plans to ensure the appropriate handling of information security incidents.

10.2 BUSINESS CONTINUITY PLAN

A managed process must be in place for developing and maintaining business continuity throughout the organization. This process should include consideration of information assets and the risks associated with them in the event of their compromise or destruction.

These plans should be tested regularly and maintained through recurrent reviews to ensure that they are up to date, effective and adequately consider current IT assets. The plans should be updated as part of the formal change management process.

The key human resources that will manage a Business Continuity event must be identified, accessible and trained in what is required of the position.

10.3 INCIDENT DETECTION

10.3.1 ACTIVITY LOGGING AND MONITORING

Authorized Company personnel have the legal and technical authority to monitor user activity and network traffic on Company systems.

Company implements a risk-based approach to determine which systems require logging and monitoring and the appropriate method to utilize.

Designated Company systems should generate audit logs for recording the details of user interaction, exceptions and other security related events.

Systems should be monitored to detect deviation from access control policy and to ensure events are logged to provide evidence in case of security incidents.

10.3.2 INTRUSION DETECTION SYSTEMS

Mechanisms should be established to detect incidents that may impact the secure and effective operation of Company's cloud-based systems. This capability includes logging from Intrusion Detection Systems provided by various cloud providers.

10.3.3 ANTIVIRUS AND MALICIOUS CODE

Users should be made aware of the dangers of unauthorized or malicious software. Company should introduce special controls to detect and/or prevent the introduction of malicious code onto the Company network.

10.4 INCIDENT RESPONSE

10.4.1 INCIDENT RESPONSE TEAM

Company must have a response team who will be the first point of call in the event of an incident.

10.4.2 EVENT REPORTING

Information Security events should be reported through appropriate channels and to appropriate personnel as quickly as possible to enable optimal investigation of the event. At a minimum, security events for Company should be reported as an email to security@redpointsecurity.com.

All employees, contractors and third-party users should be aware of the reporting procedures for the assets within Company.

Company must identify events that need to be reported to a statutory authority and have procedures in place to do so.

Any security related events or problems detected by logging and monitoring should be dealt with according to appropriate incident reporting procedures.

10.4.3 INCIDENT INVESTIGATING

Audit logs recording exceptions and other security-relevant events must be produced and kept for one year to assist in incident investigations and access control intrusions.

10.4.4 DISCIPLINARY PROCEDURES

Any Company staff found to have caused an incident that has impact on Company business will face disciplinary action as outlined in the Code of Conduct.

11. HUMAN RESOURCE SECURITY

FOCUS

This policy addresses the requirement for human resource security. Company relies on its personnel to be honest and vigilant to help protect Company information and systems from compromise. In order to do this, all information system users and support personnel must be aware of the potential security threats and concerns and be properly trained in the correct procedures for use of the information and systems.

POLICY

11.1 PRIOR TO EMPLOYMENT

11.1.1 SECURITY CLEARANCE AND POLICE CHECK

All eligible potential employees of Company should undergo appropriate checks as a condition of employment. Examples of such checks may include reference checks, criminal background checks, and credit checks.

11.1.2 POSITION SENSITIVITY

All employees must have successfully passed a background check performed prior to access being granted to sensitive information.

11.2 DURING EMPLOYMENT

Employees must abide by the policies stipulated in this Information Security policy.

11.2.1 DISCIPLINARY ACTION

Disciplinary action should include but not be limited to training, temporary suspension of duties, termination of employment, reporting to law enforcement, or legal action.

11.2.2 EDUCATE AND TRAIN USERS

Company employees must receive appropriate training and regular updates of Company Information Security policies and procedures.

All users must acknowledge that they are aware of the Information Security policies and their requirements, and the consequences of not adhering to them.

11.2.3 ANNUAL SECURITY AWARENESS TRAINING

All Company employees, contractors, and third-party personnel with access to the organization's information systems or sensitive data are required to complete security awareness training annually. This training will cover key topics such as phishing prevention, password management, secure data handling, and recognizing social engineering tactics. Non-compliance may result in pause of system access until training is completed.

11.2.4 ROLE-SPECIFIC SECURITY TRAINING REQUIREMENTS

The organization will provide annual security awareness training tailored to the specific roles and responsibilities of employees. This includes additional training for high-risk roles such as testers with access to sensitive client data, developers, and customer fulfillment personnel. Training completion will be documented, and refresher courses will be offered periodically to address emerging threats.

11.2.5 TRACKING AND REPORTING OF TRAINING COMPLIANCE

Redpoint management will track participation in and keep logs of the annual security awareness training program and report compliance. Employees who fail to complete the training by the specified deadline will be notified and required to attend a remedial session within 30 days to ensure compliance with the Company's security policies.

11.2.6 SEGREGATION OF DUTIES

Requests for administrative changes to duties or access control cannot be approved by the same person who requested the change.

11.3 TERMINATION OR CHANGE OF EMPLOYMENT

Upon termination of employment staff must return any Company issued devices.

Access to all Company systems must be revoked within 24 hours of employment being terminated.

12. COMPLIANCE

FOCUS

This policy addresses the requirement for Company systems and processes to be compliant with applicable regulations, legislation and standards. The design, operation, use and management of information systems are subject to numerous statutory, regulatory and contractual security requirements. Company has established Information Security controls to protect Company information systems and to comply with these obligations. This Information Security Compliance policy has been established to verify that appropriate controls are in place and that they are working effectively.

POLICY

12.1 COMPLIANCE WITH LEGAL REQUIREMENTS

Company must identify, define and document all relevant statutory, regulatory and contractual requirements relating to its information systems.

Company must define and implement appropriate procedures to ensure Company's compliance with legal restrictions regarding intellectual property rights and the use of proprietary software products.

Company must apply controls to protect personal information in accordance with the applicable privacy legislation.

When Company has a need to collect evidence in connection with a legal action, it will follow the aforementioned procedures to protect the integrity of the evidence.

12.2 RETENTION OF ORGANIZATIONAL RECORDS

Except as required by law, business needs, or contractual obligations with third parties, Company will ordinarily retain all organizational records for a period of seven (7) years.

12.3 TECHNICAL COMPLIANCE

Information system owners should ensure that their systems comply with security implementation standards by checking the systems on a regular basis.

Vulnerability and penetration testing should only be conducted after thorough planning and should be documented and repeatable. Testing of this nature should only be performed by fully competent staff members.

12.4 INFORMATION SYSTEMS AUDIT CONSIDERATIONS

Company must establish and regularly review procedures for monitoring the use of Company information processing facilities. The level of monitoring will be determined by Security, according to risk management principles.

Company monitoring should include all privileged operations, unauthorized access attempts and system alerts or failures.

Company must have a procedure for archiving raw and processed audit trail data regularly.

12.4.1 EVENT LOGGING

Company must produce and maintain audit logs recording exceptions and other security-relevant events for a minimum period of one (1) year to assist in future investigations and access control monitoring. Such logs should be maintained for more than one year if they are part of an existing investigation or subject to specific disposal authorities issued by the local regulatory archiving authority.

Audit logs of systems that perform security functions for the cardholder environment must be reviewed daily.

TERMS AND DEFINITIONS

Term	Definition
Access Control	*The process of allowing authorized usage of resources and disallowing unauthorized access. Relies on the validity of the identification and authentication process.*
Accountability	*The ability to hold people responsible for their actions.*
Application	*A program that has been created to perform a specific task that is useful to the user - unlike the operating system which is a program that controls the system.*
Artificial Intelligence (AI)	*A broad field of computer science focused on creating machines that can perform tasks typically requiring human intelligence. This includes learning, problem-solving, perception, and decision-making. In the context of application security, AI can assist with tasks such as data analysis, pattern recognition, vulnerability identification, and information gathering to augment human expertise.*
Auditing	*Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.*
Authentication	*Is closely related to identification, but refers to the ongoing process of validating a user based on their presented credentials prior to allowing access to a resource.*
Availability	*Ensuring that information is available in a timely manner to authorized parties.*
Business Continuity Planning	*The process of planning a response or containment strategy in the event of a system failure, emergency or security incident to ensure business operations are either maintained or returned to operation promptly.*
Compromise	*The disclosure of information or data to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.*
Confidentiality	*Ensuring that information is not disclosed to an unauthorized party.*
Configuration Management	*Refers to the process of maintaining a secure baseline and ensuring that changes to the baseline are evaluated, tested, approved and managed in a way that new vulnerabilities are not introduced with the change.*
Data	*Representation of facts, concepts or instructions in a formalized manner suitable for communication, interpretation or processing by humans or by automatic means. Any representations such as characters or analogue quantities to which meaning is or might be assigned.*
Exception	*The process to formally request and review a deviation to a specific policy or standard.*
Identification	*Refers to the process of verifying the identity of a user prior to granting access to a resource. This process requires documents to be provided which form Evidence of Identity.*
Information	*The meaning that a human assigns to data by means of the known conventions used in their representation.*
Integrity	*Ensuring that data has not been modified by unauthorized parties.*
Intrusion Detection	*Is the process of ensuring that the actions of unauthorized users are readily identified, possibly in real-time.*

Intrusion Prevention	*Is the process of ensuring that the actions of unauthorized users are prevented from causing harm to the system.*
Key	*A data element used to encrypt or decrypt a message - includes both Public Keys and Private Keys.*
Large-Language Models (LLMs)	*A type of artificial intelligence program designed to understand and generate human-like text. LLMs are trained on vast amounts of text data, enabling them to perform a wide range of language-based tasks, including translation, summarization, question answering, and content creation.*
General-Purpose LLMs	*These are publicly accessible LLMs (often offered as free-tier or widely available services) that are not specifically designed for enterprise or secure data handling. They are typically cloud-based and may involve the processing of user input for continuous model improvement, which can pose significant data privacy risks if sensitive information is provided.* Our policy restricts the use of general-purpose LLMs with any sensitive customer data due to inherent data privacy and control concerns.
Cloud-Hosted LLMs (Secure/Private Instance)	*These are LLMs offered by cloud service providers but configured specifically for enterprise use with robust data isolation, strict privacy guarantees, and contractual agreements that prevent the service provider from using customer data for their own model training. Data processing typically occurs within a dedicated or highly secure environment.*
Locally Hosted LLMs	*These are LLMs deployed and run entirely within an organization's own secure, on-premises infrastructure or private, dedicated cloud environment. This setup provides maximum control over data, security, and the model's operation, as sensitive information never leaves the organization's controlled ecosystem. Our policy prioritizes and, where feasible, mandates the use of locally hosted LLMs for tasks involving highly sensitive customer data.*
Monitoring	*The process of reviewing audit trails and collection agents to detect anomalies or system misuse.*
Must	*The item is mandatory. See "Exception" in relation to non-compliance.*
must not	*Non-use of the item is mandatory. See "Exception" in relation to non-compliance.*
Policy Compliance	*Refers to the appointment responsible for ensuring all IT environments adhere with the policy.*
Registration Information	*Information about users, which is reasonably required for the issue and use of authentication credentials.*
Responsibility	*Defines obligations and expected actions.*
Role-Based Access Control (RBAC)	*A method of restricting network access based on the roles of individual users within an organization. In an RBAC model, users are assigned specific roles, and these roles are granted permissions to access certain resources or perform specific operations. This ensures that employees can only access the information and tools necessary for their job functions, significantly enhancing data security and preventing unauthorized access.*
Security Management	*Refers to the policies and procedures associated with implementing, enforcing and reviewing security controls.*
Secure Authentication Data	*Refers to the verification information held on credit cards which could be used to duplicate the "magnetic stripe", or be used to verify the credit card in any other way. This is commonly referred to as the CVV, CVV2, CVC, or CVC2 numbers, or "Track Data".*
Should	*Valid reasons to deviate from the item may exist in particular circumstances but the full implications need to be considered before choosing this course.*

System	*Generally used as an abbreviation for 'automated information system', which is defined as an organized assembly of resources and procedures i.e., computing and communications equipment and services, with their supporting facilities and personnel--that collect, record, process, store, transport, retrieve, or display information to accomplish a specified set of functions.*
UPS	*Uninterrupted Power Supply – A system that provides power for a limited time to allow operation of critical systems and /or orderly shutdown of systems.*

DOCUMENT CONTROL

Title	*Redpoint Security, Inc. Information Security Policy*
Contents	*Company Information Security Policy*

Date	Version	Author	Details of Change
1/6/2019	*0.1*	*Seth Law*	*Initial Draft*
2/15/2019	*1.0*	*Seth Law*	*Release*
2/24/2020	*1.1*	*Seth Law*	*Updated for yearly review (2020)*
9/9/2020	*1.2*	*Seth Law*	*Formatting changes*
2/1/2021	*1.3*	*Seth Law*	*Yearly Review update (2021)*
3/23/2022	*1.4*	*Seth Law*	*Yearly Review update (2022)*
6/26/2023	*1.5*	*Seth Law*	*Yearly Review update (2023)*
6/14/2024	*1.6*	*Seth Law*	*Yearly Review update (2024)*
7/23/2025	*1.7*	*Aaron Law*	*Yearly Review update (2025) – AI section added, formatting*

Name	Position	Date
Seth Law	*Founder, Principal Consultant*	*2/15/2019*
Seth Law	*Founder, Principal Consultant*	*2/24/2020*
Seth Law	*Founder, Principal Consultant*	*9/9/2020*
Seth Law	*Founder, Principal Consultant*	*2/1/2021*
Seth Law	*Founder, Principal Consultant*	*3/23/2022*
Seth Law	*Founder, Principal Consultant*	*6/26/2023*
Seth Law	*Founder, Principal Consultant*	*6/14/2024*
Seth Law	*Founder, Principal Consultant*	*7/23/2025*