Hit Labs Information Security Policy

Document History					
Revision Date	Revised By	Version	Description of Changes	Approval Date	Approved By
11/06/2020	Ben Dolman (CTO)	1	Initial Draft	11/06/2020	Zach Mangum (CEO)

1. Purpose and Overview

- The purpose of the document is to record policies and procedures for how Hit Labs plans to implement high level information security protections within the organization, including definitions, procedures, and responsibilities.

- This policy applies to all users of information systems within the organization, including employees and contractors, as well as any external parties that come into contact with systems and information controlled by the organization.

- This policy is intended to assist in the establishment of Hit Labs' information security program, in order to stay compliant with legal and regulatory requirements as well as with contractual obligations relevant to the organization.

- This policy, and all associated company policies, will be reviewed and updated at least annually.

2. Organizational Security

2.1 Security Roles and Responsibilities

All Hit Labs personnel are responsible for information security. Security must support business objectives and be built into the day to day activities of the company.

- The Chief Executive Officer (CEO) is responsible for:
    - *Managing the budget of the information security program*
    - *Overseeing and approving changes to policies*
    - *Ensuring proper oversight to information security throughout the company*
- The Chief Technology Officer (CTO) is responsible for:
    - *Creating and maintaining information security policies*
    - *Supervising roles supporting information security (engineering, IT)*

    - *Ensuring the coordination of all security related functions (e.g., physical security, personnel security, and the security of information stored in non-electronic form)*
    - *Conducting annual security awareness training*
    - *Investigating and documenting all security breaches/incidents*
    - *Assisting IT personnel in implementing security tools and procedures*
- System Engineers are responsible for:
    - *Administration of the network*
    - *Security patch management*
    - *System performance, security monitoring, and analyzing incidents*
    - *Application of necessary technical security controls*

2.2 Code of Conduct

Employees should fulfill their job duties with integrity and respect towards all individuals involved. Employees are further expected to be ethical and responsible when representing the company.

- *Discriminatory behavior, harassment, or victimization will not be tolerated.*
- *When in the workplace, employees must present themselves in an appropriate & professional manner.*
- *Employees are discouraged from accepting gifts from customers and other business partners and are always prohibited from accepting or offering bribes.*
- *Supervisors and managers may not abuse their authority.*
- *Employees should avoid any personal, financial, or other interests that might compete with their job duties.*
- *Employees are expected to not abuse their employment benefits.*
- *Disciplinary action may be taken for repeated or intentional violation of policies, ranging from reprimands to suspension or termination.*
- *Cases of corruption, theft, embezzlement, or other unlawful behavior may call for legal action.*

2.3 Acceptable Use Policy

Hit Labs has established criteria for determining acceptable use of its information assets. Each user is responsible for the appropriate collection, use, protection and disposal of information and assets to protect from unauthorized use.

- *Employees and Contractors are expected to be in compliance with applicable laws and regulations.*
- *Employees and Contractors are expected to act in an ethical and responsible manner when handing information assets and other company equipment.*

- *Employees and Contractors are subject to disciplinary actions in the event of policy violations, which include reprimands, suspension and termination, based on the severity of the violation at the discretion of company management.*
- *Employees and Contractors are expected to communicate information via authorized systems, including company email and shared drives.*
- *Employees and Contractors understand that their activities while accessing company information assets may be monitored.*
- *Limited personal use of company devices is acceptable as far as employee and contractor use does not interfere with job roles and responsibilities, nor does the personal activity imply company sponsorship or violate policies.*
- *Employees and Contractors are prohibited from performing any of the following activities when using or access company information assets:*
    - *Installing software that may compromise information assets*
    - *Engaging in other commercial activities*
    - *Unlawful or malicious use or behavior*
    - *Use of unlicensed software*
    - *Connecting to unauthorized communication networks*
- *Employees and Contractors access to all information assets are revoked and all physical devices must be returned to the company upon termination.*

2.4 Employee Communication and Training

Hit Labs has established procedures to ensure that employees are contractors are informed of their job roles and responsibilities, and up to date on the requirements of current policies.

- *New Employees and Contractors are appropriately screened during the hiring process and are required to complete a background check.*
- *The company requires the completion of relevant new employee training upon hire.*
- *All employees and contractors are required to attend an annual security awareness training.*
- *Employees and contractors may be required to complete relevant job specific trainings, in order to stay current with product and industry standards and/or stay current with their certification training requirements.*
- *Employees and Contractors have access to the most current version of company policies and relevant procedures documents.*
- *Employees and Contractors are kept informed of key company updates via communications from company leadership.*
- *Employee performance reviews are performed periodically with team leaders or the employee's direct manager. Meetings are used to discuss performance around day-to-day and security-related activities and for managers to provide feedback for improvements.*

3. Classification of Data Types

Hit Labs has established criteria for determining how data sets and information within the environment should be used, handled and protected, based on its content and level of sensitivity to the business and the company's customers.

- *Management has identified the following data types:*
    - *Restricted - highly sensitive data that if compromised could put the company at financial or legal risk, may be subject to state/federal/international privacy regulations (PII, PHI, credit card information, IP, SSNs)*
    - *Confidential - sensitive data that if compromised would negatively affect the operations or reputation of the company (performance reviews, vendor contracts, trade secrets)*
    - *Private - data that should only be disclosed to employees and authorized vendors and third parties of the company, not appropriate for public disclosure (organizational charts, employee contact information, sales strategy, employee handbooks)*
    - *Public - data that may be freely disclosed to the public (approved marketing materials, contact information, product pricing details)*

4. Information Assets

Hit Labs maintains an inventory of critical information assets in the environment and assigns an owner. The inventory must be maintained and updated as needed and reviewed annually.

5. Data Storage and Encryption

Hit Labs has established means of securely storing data according to the classification.

- *Restricted, confidential and other sensitive data must be stored using at least AES 256-bit encryption when stored on any media type.*
- *Data containers (S3 buckets, RedShift clusters, etc.) should be secured using client-side and server-side encryption.*
- *Access to restricted, confidential and other sensitive data should be restricted to only those who need access for business purposes.*
- *Hard copies of restricted, confidential and other sensitive information must be secured in a locked drawer or file cabinet.*
- *All forms of removable media with production and customer data must be encrypted (disk, USB, hard drives).*
- *Monitoring and alerting should be configured to identify and respond to encryption failures or misconfigurations in a timely manner.*
- *Management must use cryptographic key management systems or procedures to ensure that access to keys is restricted, keys are rotated, and keys are generated and stored in a secure manner.*

6. Data Transmission and Encryption

Hit Labs has established means of securely transmitting data according to the classification using cryptography and other security protocols.

- *Management must use strong SSL or TLS settings for external web and email communications.*
- *Restricted information cannot be shared over open public wireless networks.*
- *Management should require that a minimum of AES 256-bit level encryption for data in transit.*
- *Management must require the use of an encrypted VPN for remote access.*
- *API calls must be encrypted with TLS/SSL for secure communications.*

7. Data Retention

Hit Labs has established a schedule to retain data according to legal and regulatory mandates, and to meet the company's service level agreements and commitments. Personal data shall be kept for no longer than is necessary for the purposes for which it is being processed.

- *Customer information is stored for the life of the contract.*
- *Internal financial data is retained for at least 7 years.*
- *The Data and Records retention schedule is reviewed annually for ongoing compliance.*
- *Exceptions to the retention policy must be requested by the relevant business unit and approved by management.*

8. Data Disposal

Hit Labs has established a schedule to dispose of data according to legal and regulatory mandates, and to meet the company's service level agreements and commitments.

- *Customer data is retained for at least 30 days after the termination of the contract or for the length of time determined by the customer.*
- *Restricted and/or Confidential customer data is to be permanently deleted within 60 days of the customer request.*
- *Internal financial data classified as either Confidential or Restricted is purged after 7 years.*

9. Use and Protection of Mobile Devices

Management must approve the use of cell phones, communication devices and laptops prior to use by an employee or contractor. Physical devices are expected to be protected and kept secure from unauthorized use.

- *Company management maintains a centralized list of approved devices to track authorized ownership and use.*
- *Devices are regularly updated with current security measures.*
- *Devices require appropriate authentication measures.*

- *Devices are not to be left unattended in public. Physical security devices such as a cable lock may be used on an unattended device when absolutely necessary.*
- *Screens must be locked at all times when not in use.*
- *Access to restricted information assets is prohibited from an employee's cell phone, unless authorized and properly secured.*
- *Company communications on personal mobile devices are restricted to secure company email and instant messaging.*
- *Damaged, lost, or stolen devices should be reported to management immediately.*

10. Physical Security

Hit Labs has established measures to protect the physical environment supporting information assets.

- *Management maintains a list of physical information assets, which includes a description, physical location and responsible parties.*
- *Physical access to information assets and company workspaces is restricted through the use of key cards, key codes and/or physical keys.*
- *Physical access to sensitive information assets (i.e. servers, distributable media, paper documents) is restricted to authorized individuals and reviewed periodically for continued appropriateness of access.*
- *Visitors to company workspaces must be accompanied at all times.*
- *Employee desks are expected to be clear of information assets when not present.*

11. Antivirus and Anti-Malware

Production and supporting environments are protected from malicious software to reduce the risk of disruption of service and loss of data. Software capable of preventing, detecting, and removing malicious software is required on all systems.

- *Antivirus software must be deployed on all company machines, including workstations and laptops, and kept up to date.*
- *Antivirus signatures should be updated at least every 24 hours.*
- *Anti-malware protection must be installed and appropriately configured on all installed company-owned servers.*
- *Access to update or edit locally installed antivirus agents must be limited to protect against unauthorized uninstallation.*
- *Antivirus software must be enabled for automatic updates.*
- *Antivirus software must be kept active and enabled for audit log generation.*
- *Systems must be configured to run anti-malware scans with actions to automatically remove any detected malware.*

12. Intrusion Detection Systems

Activity and event logging must be enabled in the environment to monitor for unusual activity, including intrusion detection and file integrity monitoring. Systems must be configured to automatically alert appropriate personnel and resolve identified issues.

- *Intrusion Detection System (IDS) signatures are kept up to date and configured to alert appropriate personnel in the event of suspected compromise or suspicious activity.*
- *IDS alerts must be investigated to determine if response is required.*
- *IDS logs should be reviewed periodically for suspicious activity to determine if response is required.*
- *File Integrity Monitoring (FIM) software should be installed to alert appropriate personnel to unauthorized or malicious changes to assets in the production environment. See Software Development Lifecycle for further details*
- *Additional Security Information and Event Management (SIEM) should be utilized to detect additional threats to relevant network hardware and applications.*
- *Logging should be enabled of activity by those with root or administrative privileges and the logs reviewed periodically to determine if response is required.*
- *Logs should be retained, reviewed and purged according to policy and access to logs should be limited to authorized individuals.*

13. Patching and Vulnerability Management

13.1 Patching

Hit Labs has established a periodic scheduled for patching various layers of systems and infrastructure in the environment. Further patching is performed as needed based on releases from vendors and events in the external environment.

- *Patching should be scheduled to be performed on a monthly basis as driven by releases of monthly security patches.*
- *Patches must be assessed for criticality and impact to prioritize resources during the patch deployment process.*
- *Patches should be evaluated to ensure they do not conflict with existing security configurations.*
- *Critical patches should be installed in a defined and timely manner.*
- *Application patches for vendor hosted systems should be performed on an as needed basis.*
- *Application patches must follow standard change management requirements for testing, approvals and deployment.*

13.2 Vulnerability Scanning

Hit Labs has implemented measures to detect security vulnerabilities in the environment using external tools and authoritative sources. Prioritized components of the environment are scanned periodically to identify vulnerabilities that present a threat to critical information assets.

- *On a quarterly basis, the production environment is scanned for known vulnerabilities using an external scanning tool.*

- *Scheduling of scans takes into consideration the last timing of the patching cycle and the timing of least disruption to business operations.*

13.3 Reporting, Prioritization and Remediation

Results of scans are reviewed by management to prioritize the resolution of identified vulnerabilities against business objectives.

- *Results of scans are shared with appropriate business unit leaders for review.*
- *Management has established timelines for remediating vulnerabilities based on the criticality rating:*
    - *Critical - must be remediated within 14 business days*
    - *High - must be remediated within 30 business days*
    - *Medium - must be remediated within 90 business days*
    - *Low - must be remediated within 180 business days*
- *Exceptions for remediation within the established timeline must be documented and approved by management.*
- *Tickets are created to track the resolution of critical vulnerabilities that are to be remediated outside of the normal patching cycle.*
- *Evidence that vulnerabilities have been remediated shall be retained.*

14. Penetration Testing

Management should establish a schedule for performing penetration testing, both internally and by an outside party. Results of penetration tests are reported to appropriate levels of management and findings are resolved in a timely manner.

- *Internal and external penetration testing should be performed at least annually by qualified company personnel.*
- *Penetration testing should be performed after any significant infrastructure or application upgrade or implementation.*
- *Management should engage an outside service provider to perform penetration testing at least annually, if applicable.*
- *Findings from penetration testing must be prioritized and resolved according to their criticality rating.*
- *Results and findings from the penetration tests are reported to management and escalated to Board of Directors as necessary.*

15. Internal Risk Assessments

On an annual basis, or when a significant change occurs in the environment, management assesses the current risk landscape based on all facets of the business. Management considers

threats, vulnerabilities, weaknesses, and environmental impacts to the company to assist in the creation of objectives and goals and the allocation of resources.

- *Management identifies and documents valuable assets, potential threats, and vulnerabilities that could lead to threats materializing.*
- *Management identifies the likelihood and impact of identified threats to the company*
- *Management assigns a risk ranking to identified risks.*
- *Management determines and documents solutions, control measures and risk mitigation techniques for each identified risk to the environment based on their risk ranking.*
- *As needed, management updates policies and procedures based on the outcomes of the risk assessment.*
- *Results of the risk assessment are shared with stakeholders.*

16. External Risk and Control Assessments

At least annually, management engages an independent assessor to examine the effectiveness of controls in the environment and understand the company's state of compliance with internal policies and/or external frameworks.

- *Management should engage an independent assessor to review for gaps in the control environment when launch new products or implementing new systems.*
- *External audits must be performed to achieve compliance with financial and security reporting frameworks.*
- *Management must create remediation plans for any findings and monitor that plans are executed.*
- *Results of external assessments and audit must be presented to the relevant stakeholders (i.e. Board of Directors) and members of management.*

17. Third Party and Vendor Management

17.1 New Vendor Set Up

All new vendors and third parties must be thoroughly screened before entering into a business relationship. Prior to entering into service agreements or contracts, Hit Labs performs a risk assessment over the prospective vendor's ability to abide by applicable policies and procedures related to security.

- *The new vendor risk assessment includes the following requirements:*
  - *Identification of the relationship owners for both the company and the prospective vendor.*
  - *Documentation of the services provided by the vendor.*
  - *Documentation of risks associated with the use of the vendors.*
  - *Review and document findings from any available compliance reports (SOC 1, SOC 2, PCI, etc) or, if unavailable, have the vendor complete an IT Questionnaire to provide the relevant information.*

- *When available, Hit Labs completes a trial period to test the features of the product to meet business needs.*

17.2 Service Level Agreements

Upon successful completion of new vendor assessments, Hit Labs and their vendors agree to service level agreements to ensure that applicable policies and procedures are followed.

- *For self-subscription products, Hit Labs management reviews terms of service to ensure that vendor products align with Hit Labs requirements.*
- *Service Level Agreements should include provisions for, but not limited to, roles and responsibilities, incident reporting and resolution, data classification and handling, customer support and communication requirements, renewal and termination.*
- *Service Level Agreements or other contracts should include access to compliance reports or a right to audit.*
- *Service Level Agreements should include key performance indicators such as uptime, availability and capacity.*
- *Provisions for a Non-Disclosure Agreement (NDA) must be included for instances where the company chooses to share customer or PII confidential data with a vendor or third party.*

17.3 Third Party Risk Management

Hit Labs has established a program to monitor and ensure service levels and ongoing compliance of existing vendors and third parties. Based on their risk ranking, vendors and third parties must be periodically reviewed for adherence to applicable security policies, as well as legal, regulatory and contractual obligations.

- *Management must maintain a centralized list of all third parties and vendors.*
- *Management must classify each vendor according to the risk ranking system (e.g. based on access to information, access to facilities, criticality of the service provided, etc.).*
- *Management must perform periodic due diligence of vendors and third parties including the collection of compliance reports, collection of a completed security questionnaire, and analyze reports (complementary controls, impacts of control failures reported, assess service levels, etc.).*
- *Management must report findings and outcomes of periodic due diligence to stakeholder, including the board of directors.*

18. Access Control Policy

18.1 New or Modified Access

Any new instance of access within the environment must be authorized prior to accessing information assets.

- *Authorization for access must be granted by the information asset owner or the user's direct manager. Users may not authorize their own access.*
- *Authorization for access must be documented and granted prior to the provisioning of access.*

- *Access to information assets are authorized based on business need according to the user's job roles and responsibilities.*
- *Users must meet all requirements prior to obtaining access to sensitive information assets (i.e. users must have passed a background check prior to accessing customer information).*
- *The authorized approver considers segregation of duties prior to approving access.*
- *The authorized approver considers business justifications for granting vendors and third parties' access to information assets.*
- *New credentials and temporary passwords are shared with the user in a secured manner.*

18.2 Authentication

Hit Labs requires that users authenticate to networks, operating systems, databases, applications and tools in the environment using unique IDs and strong passwords in order to access information assets.

- *Usernames must be unique to identify users' activity in the environment.*
- *Passwords must contain 8 characters.*
- *Passwords must meet complexity requirements (combination of upper- and lower-case letters, numbers and special characters).*
- *Passwords must be changed at least every 180 days.*
- *Passwords cannot be reused and should not contain the users' account name.*
- *Account lockout thresholds must be enforced for invalid password attempts.*
- *Remote access must be secured through the use of a virtual private network and multi-factor authentication requirements.*
- *Failed logon attempts and account lockouts must be logged and monitored.*
- *Credentials must be shared during initial set up in a secure manner and users are required to change passwords at first login.*
- *Single sign-on and password vault software should be used where available.*

18.3 User Access Reviews

Access to information attests is reviewed periodically to ensure ongoing compliance with access policies. Users are reviewed for continued appropriateness of access rights and segregation of duties, and to ensure that access is removed timely for terminated employees or changes in job roles and responsibilities.

- *Hit Labs maintains a list of access roles that grant users access to the production environment.*
- *Access to production systems (OS/DB/App) is reviewed quarterly for continued appropriateness.*
- *Action items resulting from the review are documented and completed in a timely manner.*
- *The results of the review are approved by an individual other than the reviewer.*

18.4 Deprovisioning

Access to information assets is removed in a timely manner for users no longer requiring access to perform their job responsibilities.

- *Access to the production environment must be deprovisioned within 3 days of termination. Business justification must be documented for any access roles extended beyond employment.*
- *Access updates required based on changes in job roles and responsibilities for existing employees are completed within 5 business days.*
- *Access to the network and other internal resources are deprovisioned within 5 business days of termination.*

18.5 Administrative and Privilege Access

Access to sensitive information and administrative access to systems and tools is restricted to authorized individuals and limited to as few individuals as necessary to perform relevant functions.

- *Administrative access to systems is restricted through the use of multifactor authentication tools.*
- *Access to administer firewalls and VPNs must be restricted.*
- *Access to update domain and operating systems configurations must be restricted.*
- *Hit Labs has implemented code approvals and pull requests to prevent unauthorized code from being deployed to production.*
- *Activity by those with access to deploy code should be logged and monitored.*
- *Administrative access must not be granted until the user has successfully completed a background check and/or completed required trainings.*
- *Administrative access is subject to all controls required for non-administrative access.*

18.6 Shared and Generic Accounts

Users are required to use individual accounts when accessing information assets. Hit Labs restricts the use of shared and generic accounts, and limits users with access to these accounts to only those required for the functions of the accounts.

- *Generic and shared accounts are subject to the same controls as individual accounts, including approval for access and periodic reviews.*
- *Passwords to shared accounts are maintained in a password vault.*
- *Management authorizes the use of shared and generic accounts in the environment.*

19. Incident Management

19.1 Incident Monitoring and Identification

Hit Labs has implemented an entity wide security program to identify incidents and issues occurring in the environment through monitoring and reporting.

- *The company has established the Security team as responsible for overseeing the implementation of the security incident response program.*
- *Management has communicated employee and contractor responsibilities regarding security through policies and trainings.*
- *Employees are required to report any system vulnerability, incident, or event pointing to a possible incident.*
- *The company has established channels for customers to report issues or suspected incidents.*
- *The company has established an on-call schedule to respond to urgent issues in the environment in a timely manner.*
- *Activity and event logging enabled in the environment are monitored for unusual activity and are configured to alert appropriate personnel.*

19.2 Incident Tracking and Classification

Hit Labs has established tracking and classifying methods for reported incidents. The Security team ensures that relevant information is collected in the tracking system to inform the classification of the incident and require resources for resolution.

- *The company has established the internal ticketing systems for tracking incidents.*
- *Reported incident tickets should include the following details:*
    - *Description of the incident*
    - *Date/time/location of the incident*
    - *Person who discovered and reported the incident*
    - *How the incident was identified (customer reported, automated alert, internal, etc.)*
    - *Affected systems and/or individuals*
- *The company has established a prioritization system to classify tickets based on their impact and severity:*
    - *Critical - PII/PHI impacts, service disruptions affecting SLAs, violates legal or compliance obligations, etc.*
    - *High - Impacts customers or disrupts important internal operations*
    - *Medium - impacts internal business unit activities*
    - *Low - no or little impact to customers or business operations*
- *The company has established timelines for acknowledgement and resolution based on the classification of the incident:*
    - *Critical - Assigned/Acknowledged within 4 hours, contained within 24 hours, resolved within 3 business days*
    - *High - Assigned/Acknowledged within 1 business day, contained within 3 business days, resolved within 5 business days*
    - *Medium - Assigned/Acknowledged within 3 business days, contained within 10 business days, resolved within 15 business days*

    - *Low - Assigned/Acknowledged within 10 business days, contained within 30 business days, resolved within 90 business days.*
- *Any evidence, screenshots, documents, and communication pertaining to the incident is attached to the ticket as support.*

19.3 Containment, Eradication and Recovery

Incidents that have been identified and entered into the tracking system, are assigned to the appropriate owners for resolution. Responsible parties document activities associated with the containment, resolution and other recovery efforts associated with the incident.

- *Responsible parties work with associated business units and other stakeholders to determine the appropriate response to the incident.*
- *All documentation associated with the triage and resolution of the incident must be preserved.*
- *Notice of the incident must be given to affected internal and external parties as required. Such disclosures, along with the time, date and method of disclosure, is documented in the ticket.*
- *Status of the incident is tracked in the ticket (Open, Closed, Cancelled, Archived, etc).*

19.4 Root Cause Analysis

After an incident has been resolved and appropriate parties notified of the occurrence, a postmortem that includes root cause analysis is performed, along with the documentation of any lessons learned.

- *Root Cause Analysis details are documented within the tracking ticket.*
- *Policies and procedures are reassessed and updated as needed in the event of a major or pervasive incident.*
- *Additional training is performed to prevent future occurrences of similar incidents.*
- *Periodically, incidents are reviewed for the recurrence of similar root causes.*

20. Business Continuity and Disaster Recovery

20.1 Backups, Restores and Availability of Data

To ensure the ongoing availability of critical data, management has established a schedule of backups and data redundancy. Backups and replications are monitored for failures and resolved in a timely manner.

- *Backups of production database are performed on a nightly basis.*
- *Data is replicated across geographically separate availability zones.*

- *Backups and replications are monitored for failures. In the event of three successive nightly failures, IT will open an incident ticket to investigate the issue.*
- *IT performs restorations of data per customer or business requests.*
- *System restore capabilities are tested at least annually.*

20.2 Business Continuity Planning

To ensure continued business operations during and following any critical incidents that results in a disruption to normal operational capabilities, management has developed a plan to address scenarios that may arise from the occurrence of such disruptive events and incidents.

- *Management has identified critical assets in the environment and has assessed the associated threats and vulnerabilities. See the Information Risk Management section above.*
- *Management has considered customer service level agreements in defining critical services and technologies for recovery.*
- *A team has been designated with specific roles and responsibilities to manage crisis scenarios and recovery processes.*
- *Recovery procedures for critical assets and functions are documented and shared with respective teams and members of leadership. Procedures include steps for notification of relevant staff and vendors, critical items to be recovered from each department, and lists of key requirements to move to an alternate worksite.*

- *Specific plan procedures are documented in the Hit Labs Business Continuity Plan.*

20.3 Annual Testing

To ensure that the business continuity and disaster recovery plan is effective for meeting recovery time objectives, management conducts an annual test of the plan. The results of the test are reported to stakeholders and analyzed to make improvements to the existing plan. In the event of an actual live event scenario that requires the plan to be used, no testing is required.

- *Roles and responsibilities for the annual testing of the BCDR plan are defined, including the individual responsible for selecting the test scenario or parameters.*
- *Scenarios tested are documented and outcomes are evaluated against the existing plan.*
- *Management reviews the results of the test to assess readiness in the event of an actual event. Updates are made to the plan based on the test results.*

21. Software Development Lifecycle

21.1 Design and Development

To ensure that significant updates to software are designed and developed according to management's intentions, the company must establish a process to obtain necessary inputs, documentation and approvals for the creation of updates.

- *The design and details of all changes to the software must be documented, proposed and signed off prior to initiating development processes.*
- *Change specifications must be documented to record necessary information including critical issues, system impairments, customer impacts, rollback/backout plans, etc.*
- *Security and data handling considerations must be documented, including for the use of any confidential or personal information.*
- *Features, tasks and development checklists must be tracked in the ticketing systems in order to record responsible parties, change types and priority.*
- *Customer data and other live production data must not be used in development activities.*
- *Development environments must be logically segregated from the production environment.*
- *Software development guidelines and policies must be documented, reviewed at least annually and made available to all relevant parties.*

21.2 Release Testing

To ensure that new features are created in accordance with the approved design, management must develop processes to test new changes for functionality, alignment with management's intentions and impact to customers prior to release.

- *All changes and new features must be tested by a different individual than the developer of the change.*
- *Testing requirements should vary based on the complexity of the release (e.g. limited testing for routine maintenance, UAT/QAT for major releases).*
- *The change tester must provide approval that the update has completed testing.*
- *Testing must be performed in a logically segregated environment from the production environment. The testing environment should be similar to the production environment to ensure the integrity of the testing.*
- *Customer data and other live production data must not be used in testing activities.*
- *Test data and accounts must be removed prior to testing sign off.*

21.3 Release Approvals

Management must implement a series of required approvals for any changes to the production environment supporting products and services.

- *In addition to design and quality assurance approvals, deployment approvals must be required by relevant stakeholders and recorded in the ticketing system prior to deployment.*

- *Relevant stakeholders for production approval should include representatives from both IT and the business where applicable.*
- *Final release approval should be granted by individuals other than the tester and/or developer.*
- *No further changes to the release can be made after approved.*

21.4 Release Deployment

To ensure that updates and new features are appropriately deployed to the production environment according to management's intentions, the company has implemented measures to ensure the integrity of the deployment, minimal impact to customers and segregation of duties between the environments.

- *Upon receipt of deployment approvals, the change is passed to the individual/team responsible for deployment. Access to deploy to production is restricted to appropriate and designated members.*
- *Segregation of duties must be automatically enforced through the deployment software and network segregation to ensure that a single individual cannot build and release code and avoid or skip testing and approval requirements.*
- *The deployment team should monitor the success of the deployment. Failures that require new development and testing must also obtain a new release approval.*
- *Success of deployments should be recorded in the ticketing/tracking system.*

21.5 Change Detection and Monitoring

In order to ensure the ongoing integrity of deployment code, management must implement measures to ensure that no unauthorized changes have been made to the production environment.

- *File integrity monitoring (FIM) software should be used to automatically alert appropriate individuals in the event of any changes to critical software, executables and files in the environment.*
- *FIM logs should be reviewed periodically to ensure that all changes made in the environment tie out to appropriate documentation and approvals.*
- *Software should be configured to log the individual making changes to any critical systems and files.*
- *Access to edit FIM logs should be limited and restricted to only authorized individuals. Segregation of duties between individuals who can make changes in the environment and who can access logs should be enforced where possible.*
- *Management should perform periodic code/config reviews for any instances in the environment where FIM software is not available.*

21.6 Emergency Change Procedures

To ensure that processes are in place to quickly respond to customer or internal incidents that require updates to product code or other production environments, management must establish procedures for alternative change controls when individuals or teams are not immediately available for timely response.

- *Emergency changes must be appropriately classified as such within the ticketing system.*
- *Deployment approvals must be collected within 2 business days of deployment.*
- *All documentation and assessments required for planned releases must be required for emergency changes.*

Information Security Policy Receipt and Acknowledgement

Hit Labs employees and contractors must comply with all applicable parts of this security policy. Compliance is necessary to ensure the confidentiality, integrity and availability of Hit Labs information systems, data and network resources.

Hit Labs employees and contractors who do not comply with all applicable Hit Labs security policies may be subject to disciplinary actions, up to and including termination of employment.

Third party persons (i.e. vendors, service providers) who do not comply with this policy may be subject to appropriate actions as defined in contractual agreements.

I _____ have received a copy of the Information Security Policy (the Policy) and have been given the opportunity to ask questions about it. I understand that the Policy outlines Hit Labs' policies, procedures, and user responsibilities for the protection of critical information assets. I agree to familiarize myself with the information in this Policy, will ask questions of my Manager, Human Resources, or IT when necessary, and will comply with the policies and procedures summarized

As required, Hit Labs, at its complete discretion, may modify or eliminate these summarized policies and procedures or any policy, procedure, standard, or guideline at any time without notice. I realize I will be responsible for complying with future changes in Hit Labs policies, procedures, standards, and guidelines. I also acknowledge that no user has the authority to allow me to engage in any conduct or behavior that is inconsistent with the Policy.

Please sign and date this receipt and return it to Hit Labs for placement in the users file.

Print Name: _____

Signature: _____

Date: _____