Information Security Policy (Redacted)

12.07.2021

Alistair Farquharson

Vatom Inc

543 Broadway St

Venice, CA 90291

Introduction

Vatom Inc. is hereinafter referred to as "the Company."

Overview

This security policy was created to communicate the requirements for secure use of company resources, as they specifically relate to personnel or systems which contain Protected Data such as Personally Identifiable Information (PII), and represents the Company's strategy for how it will implement applicable Information Security principles and technologies. This security policy differs from security processes and procedures, in that the policy provides both high level and specific guidelines on how the Company is to protect its data, but does not specify exactly how that is to be accomplished. This provides leeway to choose which security devices and methods are best in consideration of all factors. This policy is technology and vendor independent, as its intent is to set policy only, which can then be implemented in any manner that accomplishes the specified goals.

Scope

The security policy covers the Company's information systems and resources specifically related to personnel or systems which contain Protected Data. Perhaps more importantly, it covers the Company data stored on these systems as well as any backups or hardcopies of this data.

As of the date of publication of this Policy, and unless otherwise narrowed in a specific policy herein, applies only to:

Vatom Inc – Los Angeles office
Amazon EC2 datacenters

Intent

It is the intent of this security policy to clearly communicate the requirements necessary for compliance with any applicable regulations, including alignment with ISO/IEC 27001.

Implementation

This policy requires the appointment of an Information Security Manager, who will be responsible for implementation and ongoing security administration. Specific

guidance on this position can be found within this document. The Information Security Manager doesn't necessarily need to be an independent position, but can be a designation fulfilled by an existing employee (i.e., the IT Manager) as long as that employee has the authority to hold a management role, and the resources and abilities to commit to the position. This policy must be implemented with full support of management and/or the executive team.

Roles and Responsibilities

The table below describes the roles and responsibilities associated with the the Company's systems:

Role	Responsibility
Information Security Officer	Establish, document, and distribute security policies and procedures
	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations
	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.
Platform Owner	Responsible for approving and scheduling changes within the environment
Platform Support	Responsible for troubleshooting application configuration and settings in the application database
Platform Administrator	Responsible for modifying application configuration and settings in the application database
System Administrator	Responsible for the logical management of all network components
	Monitor and analyze security alerts and information, and distribute to appropriate personnel
	Administer user accounts, including additions, deletions, and modifications
	Administer user accounts, including additions, deletions, and modifications
	Monitor and control all access to data.
IT	Tasked with employee systems and network security within corporate offices. This includes tasks such as wireless scans.

Daily, Monthly and Quarterly Processes

The following regularly scheduled processes need to be followed:

Schedule	Process	Role	Section
Daily	Log Review	System Administrator	Log Review
Monthly	Security Patch Validation	System Administrator	Security Testing
Quarterly	Physical Device Theft Audit	IT, System Administrator	Physical Incidents
	Wireless Encryption Key Refresh	IT	Security Testing
	Wireless Network Scans	IT	Wireless Scans
	Internal Vulnerability Scans	System Administrator	Internal Vulnerability Scans
	External Vulnerability Scans	System Administrator	External Vulnerability Scans
	Network Documentation Update	System Administrator	Network Documentation
	Update Information Security Policy	Information Security Officer	This document
Bi-Annual	Firewall and Route Rule Set Review	System Administrator	Network Configuration Review
	User Access Review	System Administrator	User Account Review
Annual	Backup Media Security Audit	System Administrator	Expiration of Backup Media
	Security Awareness Training	Information Security Officer	Security Awareness Training
	Risk Assessment	Information Security Officer	Risk Assessment
	Confidential Data Media Inventory	System Administrator	Inventory
	External Penetration Testing	3rd party	Penetration Testing

Reviews and Updates

Reviews of this policy must be conducted annually and the policy must be updated when the environment or business objectives change.

Enforcement

This policy will be enforced by the Information Security Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the Company may report such activities to the applicable authorities.

Revision History

Revision	Date	Notes
1	3/23/2017	First revision
2	5/9/2017	Added Vendor Management

Password Policy

Overview

A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

Purpose

The purpose of this policy is to specify guidelines for use of passwords. Most importantly, this policy will help users understand why strong passwords are a necessity, and help them create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

Scope

This policy only applies to people who have access to the Cloud Environment which is controlled via group membership to the 'Cloud Access' group.

Policies

Construction

The best security against a password incident is simple: following a sound password construction strategy. The organization mandates that users adhere to the following guidelines on password construction:

- Passwords must be at least 8 characters.
- Passwords must be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols).
- Passwords must be comprised of a mix of upper and lower case characters.
- Passwords must not be comprised of an obvious keyboard sequence (i.e., qwerty)
- Passwords must not be any of the previous 4 passwords used
- Passwords must not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Creating and remembering strong passwords does not have to be difficult.

Substituting numbers for letters is a common way to introduce extra characters - a '3' can be used for an 'E,' a '4' can be used for an 'A,' or a '0' for an 'O.' Symbols can be introduced this was as well: an 'S' can become a '$' or an 'i' can be changed to a '!.'

Another way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld!'. Of course, users may need to add additional characters and symbols required by the Password Policy, but this technique will help make strong passwords easier for users to remember.

Confidentiality

Passwords are considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of organization passwords:

- Users must not disclose their passwords to anyone.
- Users must not share their passwords with others (co-workers, supervisors, family, etc.).
- Users must not write down their passwords and leave them unsecured.
- Users must not check the "save password" box when authenticating to applications.
- Users must not send passwords via email.
- Users must not reuse passwords.

Change Frequency

In order to maintain good security, passwords must be periodically changed. This limits the damage an attacker can do as well as helps to frustrate and slow brute force attempts. At a minimum, users must change passwords every 90 days on any system that can access Credit Card holder data. The organization may use software that enforces this policy by expiring users' passwords after this time period. When selecting a new password, users must not select a password that is substantially the same as, or similar to, the previous password.

Incident Reporting

Since compromise of a single password can have a catastrophic impact on network security, it is the user’s responsibility to immediately report any suspicious activity involving his or her passwords to the Information Security Manager. Any request for

passwords over the phone or email, whether the request came from organization personnel or not, must be expediently reported. When a password is suspected to have been compromised the Information Security Manager will request that the user, or users, change all his or her passwords.

Remote Access Policy

Overview

It is often necessary to provide access to corporate information resources to employees or others working outside the Company's network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.

Purpose

This policy is provided to define standards for accessing technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium.

Scope

This policy only applies to employees and contractors who have access to the Cloud Environment which is controlled via group membership to the 'Cloud Access' group.

Policies

Remote Access Client Software

The Company will supply users with remote access software that allows for secure access and enforces the remote access policy. The software will provide strong traffic encryption in order to protect the data during transmission.
Further, the Company will provide remote users with client firewall software that will protect the remote computer when it connects directly to the Internet. This software will be configured in a consistent company-standard manner and will not be alterable by the user.

Remote Network Access

Users will only have access to the environment when using the following VPN Connection Profile:

XXXX REDACTED XXXX

XXXX REDACTED XXXX

This VPN Connection is the only one that will permit access to the cloud environment and only users who are members of the 'Cloud Access' group will be able to connect.

Employees

The Company will limit remote users' access privileges to only those information assets that are reasonable and necessary to perform his or her job function when working remotely (i.e., email). The entire network must not be exposed to remote access connections.

Administrators

Any non-console administrative access, such as remote management or web-based access, must be secured to prevent misuse. If such access is allowed, it must meet the following criteria:

- Remote administrative access must be encrypted using strong encryption that is initiated prior to the administrative password being requested.
- Insecure management protocols, such as telnet, must be disabled or prohibited in favor of more secure methods, such as SSH, or encrypted via a VPN or SSL/TLS.

Third Parties/Vendors

When non-employees are provided access to the network, such as vendors or service providers, their remote access account must be disabled when not in use. Further, accounts used for remote vendor access must be monitored when in use.

Idle Connections

Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to the Company's network must be timed out after 30 minutes of inactivity.

Prohibited Actions

Remote access to corporate systems is only to be offered through a company-provided means of remote access in a secure fashion. The following are specifically prohibited:

- Installing a modem, router, or other remote access device on a company system without the approval of the Information Security Manager.

- Remotely accessing corporate systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without the written approval from the Information Security Manager.
- Use of non-company-provided remote access software
  Split Tunneling to connect to an insecure network in addition to the corporate network, or in order to bypass security restrictions
- Copying, Moving and Storage of cardholder data onto local hard drives and removable electronic media

Confidential Data Policy

Overview

Confidential Data is valuable to the Company and others as well, and thus can carry greater risk than general company data. Also, certain regulations/industry standards specify how confidential data must be treated. For these reasons, it is good practice to dictate security standards that relate specifically to confidential data.

Purpose

The purpose of this policy is to detail how to identify and handle confidential data. This policy lays out standards for the classification and use of confidential data, and outlines specific security controls to protect this data.

Scope

The scope of this policy covers the confidential data stored in the database and backups.

Policies

Data Classification

Confidential data is classified as either:

- PCI data – this is protected data in accordance with PCI DSS 3.0
- PII data – this is any personally identifiable information such as email addresses, medical records, data as it relates to race, religion. This is identified by regulations such as the UK Data Protection Act.

Confidential data is segregated from the Company's non-confidential data by limiting It to the restricted Cloud environment. Access to it is tightly controlled and tracked.

Treatment of Confidential Data

The following sections detail company requirements on the storage, transmission, and destruction of confidential data:

Storage

Confidential data must be removed from desks, computer screens, and common areas unless it is currently in use.

Confidential data must be stored in encrypted form, using strong encryption, when storage of this data is necessary. Note that this requirement applies to backups containing confidential data as well.

Confidential data must be stored only when absolutely necessary. For example, when handling PCI data, the following must never be stored: the full contents of any track from a credit card magnetic stripe, the card verification code, and the personal identification number (PIN) or encrypted PIN block. The following data must be masked before being stored:

- All PII data as defined by the GDPR https://gdpr.eu/eu-gdpr-personal-data/
- PCI data, including
    - Cardholder name
    - Primary Account Number (PAN)
    - Expiration Date
    - Service Code

When credit card authentication data is received, the data must be securely deleted following authentication, using the guidelines in section 4.2.3. Processes must be implemented to ensure that this data is unrecoverable.

Confidential data must never be stored on non-company-provided systems (i.e., home computers).

Transmission

Strong encryption must be used when transmitting confidential data when such transmission takes place outside the Company's network. Confidential data must not be left on voicemail systems, either inside or outside the Company's network, or otherwise recorded.

With respect to confidential data the Company will:

- Only accept trusted keys and certificates. Ensure that processes are in place to verify that only trusted keys and certificates are accepted.
- Require the use of strong encryption by disabling support for weaker encryption schemes.
- Ensure that proper encryption strength is implemented for the encryption methodology in use per vendor specifications.

- If the transmission occurs as part of a web application, ensure that HTTPS is displayed in the browser URL bar whenever confidential information, such as cardholder data, is requested.
- Ensure that data is never sent via end-user messaging technologies.
- Log and audit all the transfers of confidential data.

Destruction

Media containing confidential data must be destroyed in a manner that makes recovery of the information impossible. Since the only media that is permitted to store confidential information in the scope of this policy is the database in the Cloud environment, the following guidelines apply:

- Database: a scheduled maintenance job must be run every night to delete data that exceeds the requirements of the retention policy.
- Database Backups: all database backups must be securely stored and destroyed as described in the Backup Policy.

Inventory

Media inventories must be conducted annually and a Media Inventory Log must be maintained.

Sharing Confidential Data with Third Parties

Confidential Data may not be shared with Third Parties.

Security Controls for Confidential Data

Confidential data requires the following controls in order to ensure its integrity. The Company requires that the following guidelines are followed:

Strong Encryption: Strong encryption must be used for confidential data transmitted external to the Company. Confidential data must always be stored in encrypted form, whether such storage occurs on a user system, server, laptop, or any other device that allows for data storage.

Network Segmentation: The Company must use firewalls, access control lists, or other security controls to separate the confidential data from the rest of the corporate network. More information about this can be found in the Network Security Policy.

Physical Security: Systems that contain confidential data, as well as confidential data in hardcopy form, must be stored in secured areas. Special thought should be given to the security of the keys and access controls that secure this data.

Printing: Confidential Information may not be printed.

Faxing: Confidential Information may not be faxed.

Emailing: Confidential data must not be emailed inside or outside the Company without the use of strong encryption. More information can be found in the Email Policy.

Mailing: Confidential Information may not be mailed.

Wireless Access: When confidential data is transmitted or accessed via wireless networks, the Company must use wireless industry best practices for encryption, such as IEEE 802.11i. Only the strongest encryption algorithms must be used to secure this data during transmission. Please note that the use of known insecure encryption methods, such as WEP, is expressly prohibited.

Discussion: When confidential information is discussed it must be done in non-public places, and where the discussion cannot be overheard.

Display: When confidential data is numerical, such as social security numbers or cardholder data, it must be removed if at all possible. If necessary for this information to be displayed, the number, such as a cardholder's Primary Account Number (PAN), it must be masked (i.e., such that only the last four digits displayed). Please note that this restriction does not apply to employees who must have access to this data to perform their job functions. Confidential data must be removed from documents unless its inclusion is absolutely necessary.

Confidential data may not be written on a whiteboard or other physical presentation tool.

Media: Confidential information may not be stored in any media other than the database and associated backups in the Cloud environment.

Retention Policy

Overview

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that the Company's guidelines on retention are consistently applied throughout the organization.

Purpose

Data is a valuable commodity, but when retained excessively it can become a liability. Without a clear retention policy, the volume of data steadily grows, placing an unnecessary burden on IT resources. The purpose of this policy is to specify the Company's guidelines for retaining different types of data.

Scope

The scope of this policy covers the retention of data in the Cloud environment only.

Policies

Reasons for Data Retention

The Company does not wish to simply adopt a "save everything" mentality. That is not practical or cost-effective, and would place an excessive burden on the IT Staff to manage the constantly-growing amount of data.

Some data, however, must be retained in order to protect the Company's interests, preserve evidence, and generally conform to good business practices. Some reasons for data retention include:

- Litigation
- Accident investigation
- Security incident investigation
- Regulatory requirements
- Intellectual property preservation

Data Duplication

As data storage increases in size and decreases in cost, companies often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's system, on a central file server, and again on a backup system. When identifying and classifying the Company's data, it is important to also understand where that data may be stored, particularly as duplicate copies, so that this policy may be applied to all duplicates of the information.

Retention Requirements

This section sets guidelines for retaining the different types of company data.

Operational Data

Operational Data includes data for basic business operations, communications with vendors, employees, device logs (if non-confidential), etc. The majority of data will fall into this category. Operational data must be retained for 1 year.

Personal Data (PII)

Personal Data includes non-company-related data, such as users' personal data, emails, documents, etc. See the Confidential Data Policy for more detailed information about how to handle this confidential data. There are no retention requirements for personal data. In fact, the Company requires that it be deleted or destroyed when it is no longer needed.

Retention of Encrypted Data

If any information retained under this policy is stored in an encrypted format, particularly confidential information, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that the Company will not get buried in data, making data management and data retrieval more complicated and expensive than it needs to be, and placing an unnecessary burden on IT Staff. Please note that exactly how confidential data should be destroyed is covered in the Confidential Data Policy.

When the retention timeframe expires, the Company must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term implications, exceptions

will be approved only by a member or members of the Company's executive team.

The Company specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself, or destroying data in an attempt to cover up a violation of law or company policy. Further, any data that may be subject to a subpoena or discovery request must not be destroyed.

Backup Policy

Overview

A backup policy is similar to an insurance policy - it provides the last line of defense against data loss and is sometimes the only way to recover from a hardware failure, data corruption, or a security incident. A backup policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in practice it will be used more frequently than a contingency planning document. A company's backup policy is among its most important policies.

Purpose

The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

Scope

The scope of this policy covers the backup of data in the Cloud environment.

The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

Policies

Identification of Critical Data

The Company must identify what data is most critical to its organization. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data must be identified so that it can be given the highest priority during the backup process.

Any data deemed confidential must be identified so that backups of this data are treated and secured accordingly. Further information about storing confidential data can be found in the Confidential Data and Retention Policies.

Data to be Backed Up

A backup policy must balance the importance of the data to be backed up with the

burden such backups place on the users, network resources, and the backup administrator. Data to be backed up includes:

- All data determined to be critical to company operation and/or employee job function.
- All information stored on the corporate file server(s) and email server(s). It is the user's responsibility to ensure any data of importance is moved to the file server.
- All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.
- Logs and configuration information from network devices such as switches, routers, IDS/IPS systems, etc.

The following table describes the systems that are backed up and the mechanisms used:

XXXX REDACTED XXXX

XXXX REDACTED XXXX

Backup Frequency

Backup frequency is critical to successful data recovery. The Company has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.

- Database:
  - Full: daily
- All other systems:
  - Incremental: daily
  - Full: weekly

Backup Retention

When determining the time required for backup retention, the Company must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. The Company has determined that the following will meet all requirements (note that the backup retention policy must conform to the Company's data retention policy and any applicable industry):

- Incremental Backups: must be saved for one month.
- Full Backups: must be saved for six months.

Note that backup retention requirements differ, in some cases, from data retention requirements. The Company must ensure that policies on data retention are followed. If the policies conflict, the greater retention time will apply.

Restoration Procedures & Documentation

The data restoration procedures must be tested and documented. Documentation must include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long the process should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not A) misinterpreted by readers other than the backup administrator, and B) confusing during a time of crisis. The procedure documentation can be found in TBD.

Restoration Testing

Since a backup policy does no good if the restoration process fails, it is important to periodically test the restore procedures to eliminate potential problems.

Backup restores must be tested when any change is made that may affect the backup system, as well as once every month.

Network Access and Authentication Policy

Overview

Consistent standards for network access and authentication are critical to the Company's information security and are often required by regulations or third-party agreements. Any user accessing the Company's computer systems has the ability to affect the security of all users of the network. An appropriate Network Access and Authentication Policy reduces risk of a security incident by requiring consistent application of authentication and access standards across the network.

Purpose

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the corporate network are authenticated in an appropriate manner, in compliance with company standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

Scope

The scope of this policy includes all users who have access to the Cloud Environment. It is controlled via group membership to the 'Cloud Access' group. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the Cloud Environment.

Policies

Account Setup

During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

- Positive ID and coordination with Human Resources is required.
- Users will be granted access only if he or she agrees to the applicable network use policies, such as the Acceptable Use Policy.
- Access to the network will only be granted in accordance with applicable policies, such as the Acceptable Use Policy.
- Creating an account, or change access right for an account requires approval by authorized parties and must follow the Network Security Change

Management Process described in TBD
- Creating an account, or changing access rights for an account requires approval by authorized parties and must follow the Network Security Change Management Process described in Error! Reference source not found..

Account Access Levels

It is company policy to follow the principle of least privilege, where employees will be provided the least amount of access required to perform their job functions. This is particularly important as it relates to high security zones, such as the Cardholder Data Environment. Any user account with access to these zones must be given the minimum amount of access possible.

Access levels must be assigned solely based on job classification or function (role-based access control). A list of roles may be found at the beginning of this document.

Account Use

Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

- Accounts must be created using the format [firstinitial][lastname] and must be unique
- Accounts must be password protected (refer to the Password Policy for more detailed information).
- Accounts must be for individuals only. Account sharing and group accounts are not permitted.
- User accounts must be granted membership to the ‘Cloud Access’ group to ensure that the Password Policies and Remote Access Policies are applied.
- User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function. All actions taken by individuals logged in with root or administrative privileges will be logged.
- Occasionally, guests will have a legitimate business need for access to the corporate network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time and disabled when the guest's work is completed. Refer to the Guest Access Policy for additional guidance.
- Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the Information Security Manager or executive team, or as required by applicable regulations or third-party agreements.

Authentication Methods

Component	Authentication Methods	Comments
Remote Access	2-factor: • VPN with username/password • SSH with public key	
Web Console	Form-based over SSL	
Operating System	SSH with public key	
Database	Username/password	

Roles and Privileges

A list of roles can be found at the beginning of this document. The following table describes the privileges each role has for each system component:

XXXX REDACTED XXXX

XXXX REDACTED XXXX

Account Termination

When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at the Company, that employee's account can be disabled. Human Resources must create a process to notify the Information Security Manager in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.) that will result in changes in access levels.

Authentication

User systems must be configured to request authentication against a central network authentication manager, such as a domain, at startup. If this authentication mechanism is not available or authentication for some reason cannot occur, then the system must not be permitted to access the network.

Use of Passwords

When accessing the network locally, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to the Company's Password Policy.

Screensaver Passwords

Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason screensaver passwords are required, and must be configured to activate after 5 minutes of inactivity.

Minimum Configuration for Access

Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, users must strictly adhere to corporate standards with regard to antivirus software and patch levels on their systems. Users must not be permitted to access the network if these standards are not met. This policy will be enforced with a product that provides network admission control, or through other security controls that forbid access unless explicitly provided.

Encryption of Login Credentials

Industry best practices state that username and password combinations must never

be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to the Company network or across a public network such as the Internet. Username and passwords are considered confidential data, and further guidance regarding the treatment of this data can be found in the Confidential Data Policy.

First-time and Reset Passwords

When creating a user account for the first time, the first-time password must be set to a unique value that complies with the Password Policy.

When resetting the password for an existing user, the reset password must be set to a unique value that complies with the Password Policy.

First-time and reset passwords must be configured to expire immediately so that the user must change it after the first use.

First-time and reset passwords must have a minimum password age of one day.

Failed Login Attempts

Repeated login failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the Company must lock a user's account after 5 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the Information Security Manager.

In order to protect against account guessing, when login failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username login credentials you supplied were incorrect."

User Account Review

User accounts must be reviewed every month and all inactive user accounts are to be disabled. Additionally, the roles assigned to users must be reviewed bi-annually to ensure that the principles of least privilege are being followed. Over time, the roles assigned to an individual may change and the roles themselves may change, so it is important to review the user accounts and remove unused roles and privileges.

Access Reporting and Auditing

An access log must be maintained that records data, time and successful/rejected

logins. This audit log must be reviewed daily and kept for a period of 1 year.

Default System Accounts

All vendor default passwords must be immediately reset upon installation.

Root Access

All special access (e.g. root) access to servers must be limited to a segregated security role. Any use of this security role must be audited and the audit logs must be reviewed daily.

Applicability of Other Policies

This document is part of the Company's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary.

Incident Response Policy

Overview

A security incident can come in many forms: a malicious attacker gaining access to the network, a virus or other malware infecting computers, or even a stolen laptop containing confidential data. A well-thought-out Incident Response Policy is critical to successful recovery from an incident. This policy covers all incidents that may affect the security and integrity of the Company's information assets, and outlines steps to take in the event of such an incident.

Purpose

This policy is intended to ensure that the Company is prepared if a security incident were to occur. It details exactly what must occur if an incident is suspected, covering both electronic and physical security incidents. Note that this policy is not intended to provide a substitute for legal advice, and approaches the topic from an IT security practices perspective.

Scope

The scope of this policy covers all physical and information assets in the Cloud environment as well as physical and information assets used to access the Cloud environment. This is specifically laptops and computer systems used by employees in the 'Cloud Access' group as well as VPN devices and File Servers.

Policies

Types of Incidents

A security incident, as it relates to the Cloud environment, can take one of two forms. For the purposes of this policy a security incident is defined as one of the following:

Electronic

This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes, to a virus outbreak, to a suspected Trojan or malware infection. Also covered in this section is the discovery of unauthorized wireless access devices.

Physical

A physical IT security incident involves the loss or theft of a laptop, mobile device, tablet computer, smartphone, portable storage device, or other digital apparatus that may contain company information. A physical incident can also apply to the loss or theft of data in printed form.

Preparation

Work done prior to a security incident is arguably more important than work done after an incident is discovered. The most important preparation work, obviously, is maintaining good security controls that will prevent or limit damage in the event of an incident. This includes technical tools such as firewalls, intrusion detection systems, authentication, and encryption; and non-technical tools such as good physical security for laptops, mobile devices, and printed data.

All staff with responsibilities for security breach response must be trained on an annual basis.

Additionally, prior to an incident, the Company must ensure that the following is clear to System Administrators and IT personnel:

- What actions to take when an incident is suspected.
- Who is responsible for responding to an incident.

The Company should have discussions with an IT Security company that offers incident response services before such an incident occurs in order to prepare an emergency service contract. This will ensure that high-end resources are quickly available during an incident.

Finally, the Company must review any industry/governmental regulations or agreements with third parties that dictate how it must respond to a security incident (specifically, the loss of customer data), and ensure that its incident response strategies adhere to these regulations.

Confidentiality

All information related to an electronic or physical security incident must be treated as confidential information until the incident is fully contained and investigated. This will serve both to protect employees' reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the media and/or customers until the scope and damage of the incident can be assessed.

Electronic Incidents

When an electronic incident is suspected, the Company's goal is to recover as

quickly as possible, limit the damage done, secure the network, and preserve evidence of the incident. The following steps must be taken in order:

Remove the compromised or unauthorized device from the network by unplugging or disabling network connection. Do not power down the system.

- Immediately create an Emergency Response Ticket in Shortcut.io which will report the incident to the Information Security Manager
- Disable the compromised account(s) as appropriate.
- Physically secure the compromised system.
- Contact the security consultant for emergency response if the Information Security Manager deems this action necessary. If prosecution of the incident is desired, chain of custody and preservation of evidence are critical.
- Create a detailed event log documenting each step taken during this process, including chain of custody for the compromised system, hard drives, media, and/or logs.
- Determine how the attacker gained access and disable this access.
- Rebuild the system using new hardware, if applicable.
- Restore any needed data from the last known good and unaffected backup and put the system back online.
- Take actions, as possible, to ensure that the vulnerability (or similar vulnerabilities) will not reappear.
- Notify applicable authorities if prosecution is desired and possible based on the evidence collected.
- Refer to the “Notification” section for guidance on notifying any affected parties.
- Perform a vulnerability assessment as a way to spot any other vulnerabilities before they can be exploited.
- Reflect on the incident. What can be learned? How did the Incident Response team perform? Was the policy adequate? What could be done better?

Physical Incidents

Physical security incidents are challenging, since often the only actions that can be taken to mitigate the incident must be done in advance. This makes preparation critical. One of the best ways to prepare for an incident is to mandate the use of strong encryption to secure confidential data when stored on company systems, mobile or otherwise. Applicable policies, such as those covering encryption and confidential data, should be reviewed for guidance.

Physical security incidents are sometimes the result of a random theft or inadvertent loss by a user, but they must be treated as if they were targeted at the

Company.

The Company must assume that a physical loss or theft will occur at some point, and survey on a quarterly basis the Company's laptops and mobile devices to assess the Company's risk if one were to be lost or stolen. This survey can be done in conjunction with the quarterly audit required by the Mobile Device Policy.

Response

Establish the severity of the incident by determining the type of data stored on the missing device. This can often be done by referring to a recent backup of the device. If the type of data can't be determined, and there is a likely possibility that confidential data was involved, the Company must assume that confidential data was lost.

In responding to a physical security incident, two important questions must be answered:

1) Was confidential data involved?

   If not, refer to "Loss Contained" below.

   If confidential data was involved, refer to question 2 below.

2) Was strong encryption used?

   If strong encryption was used, refer to "Loss Contained" below.

   If not, refer to "Data Loss Suspected" below.

Loss Contained

First, change any usernames, passwords, account information, encryption keys, passphrases, etc., that were stored on, or used by, the system. Notify the Information Security Manager. Replace the lost hardware and restore data from the last known-good and unaffected backup. Notify the applicable authorities if a theft has occurred.

Data Loss Suspected

First, notify the executive team, legal counsel, and/or public relations group so that each team can evaluate and prepare a response in their area.

The Information Security Officer must report all incidents involving a loss or compromise of customer data must be reported to the customer or customers immediately.

The Information Security Officer must also ensure that all legal and regulatory obligations have been met in the event of an incident.

Change any usernames, passwords, account information, encryption keys,

passphrases, etc., that were stored on, or used by, the system. Replace the lost hardware and restore data from the last backup. Notify the applicable authorities as needed if a theft has occurred and follow disclosure guidelines specified in the notification section.

Review procedures to ensure that risk of future incidents is reduced by implementing stronger physical security controls.

Monitoring

All relevant systems must be monitored and incident response must be available on a 24/7 basis. Monitoring must include:

- Any evidence of unauthorized activity
- Detection of unauthorized wireless access points
- Critical IDS alerts
- Reports of unauthorized critical system or content file changes

Testing and Updating the Incident Response Plan

The incident response plan must be tested annually and the plan must be evaluated according to industry standards and lessons learned during that testing.

Notification

If an electronic or physical security incident is suspected to have resulted in the loss of third-party or customer data, follow applicable regulations and/or industry breach disclosure laws and append the applicable section(s) of the regulations to this policy. The Company's executive team will coordinate notification of impacted parties if such notification is needed.

Managing Risk

Managing risk of a security incident or data loss is the primary reason to create and maintain a comprehensive security policy. Risks can come in many forms: electronic risks like data corruption, computer viruses, hackers, or malicious users; or physical risks such as loss/theft of a device, hardware failure, fire, or a natural disaster. Protecting critical and confidential data and key systems from these risks is of paramount importance to the Company.

Risk Assessment

As part of the risk management process, the Company must conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the Company's critical or confidential

information. The process must include the following steps:

- Scope the assessment. Determine both the physical and logical boundaries of the assessment.
- Gather information. Determine what confidential or critical information is maintained by the Company. Determine how this information is secured.
- Identify threats. Determine what man-made and natural events could affect the Company's electronic information.
- Identify vulnerabilities. After threats have been identified, determine the Company's exposure to each threat. Security assessments may be useful here, as covered in the Network Security Policy.
- Assess security controls. After vulnerabilities have been cataloged, determine the efficacy of the Company's security controls in mitigating that vulnerability.
- Determine the potential impact of each vulnerability being exploited. Would the event result in loss of confidentiality, loss of integrity, or loss of availability of the information?
- Determine the Company's level of risk. Based on the information gathered in the previous steps, make a determination to the Company's level of risk of each event.
- Recommend security controls. Security controls that will mitigate the identified risks are evaluated during this step. Consider cost, operational impact, and effectiveness of each control.
- Document the risk assessment results. The final step is to document the risk assessment, including the results of each step.

Risk Management Program

The Company must conduct an annual risk assessment based on ISO 27005 (see http://www.27000.org/iso-27005.htm). To simplify this, the Company uses an online risk assessment tool from Smart (http://www.smart-ra.com). The tool contains the current risk assessment profile and a methodology for quantifying risk.

The Information Security Manager administers the system and run the annual audit.

Wireless Access Policy

Overview

Wireless communication often plays an important role in the workplace. In the past, some type of wireless access was the exception; it has now become the norm in most companies. However, while wireless access can increase mobility and productivity of users, it can also introduce significant security risks to the network. These risks can be mitigated with a sound Wireless Access Policy.

Purpose

The purpose of this policy is to state the standards for allowing wireless access to the Company's network. Wireless access can be provided securely if certain steps are taken to mitigate known risks. This policy outlines the steps the Company wishes to take to secure its wireless infrastructure.

Scope

This policy covers the wireless infrastructure of the network, including access points, routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless signal.

Policies

Physical Guidelines

Unless a directional antenna is used, a wireless access point typically broadcasts its signal in all directions. For this reason, access points must be located central to the office space rather than along exterior walls. Technology must be used to control the signal broadcast strength so that it is reduced to only what is necessary to cover the office space. Directional antennas should be used as necessary to focus the signal to areas where it is needed.

Physical security of access points must be considered. Access points must be placed in secured areas of the office. Cabling to and from access points must be secured so that it cannot be easily accessed.

Configuration and Installation

The following guidelines apply to the configuration and installation of wireless networks on Company premises:

Security Configuration

The Service Set Identifier (SSID) of the access point must be changed from the factory default. The SSID must be changed to something completely nondescript. Specifically, the SSID must not identify the Company, the location of the access point, or anything else that may allow a third party to associate the access point's signal to the Company.

The SSID must not be broadcast. This adds a layer of security by requiring wireless users to know the SSID in order to connect to the network.

If possible, though not required, the wireless access point should utilize MAC address filtering so that only known wireless NICs are able to connect to the wireless network.

The wireless access point must not connect to the Company's trusted network without a firewall or other form of access control separating the two networks. Refer to the Network Security Policy for firewall configuration standards.

Encryption must be used to secure communications on wireless networks. The strongest available algorithm must be used (insecure standards, such as WEP, are specifically banned). Encryption keys must be changed and redistributed quarterly.

Administrative access to wireless access points must utilize strong passwords or two-factor authentication.

All logging features must be enabled on the Company's access points.

Wireless networking must require users to authenticate against a centralized server. These connections must be logged, with IT staff reviewing the log regularly for unusual or unauthorized connections.

Wireless LAN management software may be used to enforce wireless security policies. The software must have the capability to detect rogue access points. Refer to the Company’s Incident Response Policy if an unexpected wireless device is discovered.

Installation

Software and/or firmware on the wireless access points and wireless network interface cards (NICs) must be updated prior to deployment.

Wireless networking must not be deployed in a manner that will circumvent the

Company's security controls.

Wireless devices on Company premises must be installed only by, or approved by, the Company's IT department.

Channels used by wireless devices must be evaluated to ensure that they do not interfere with company equipment.

Accessing Confidential Data

When confidential data, such as cardholder information, is transmitted or accessed via wireless networks, the Company must use wireless industry best practices for encryption, such as IEEE 802.11i. Only the strongest encryption algorithms must be used to secure this data during transmission. Please note that the use of known insecure encryption methods, such as WEP, is expressly prohibited. Refer to the Confidential Data Policy for additional information.

Inactivity

Inactive wireless access points must be disabled. If not regularly used and maintained, inactive access points represent an unacceptable risk to the Company (such as those that are accessible overnight or when the office is empty). This should be accomplished with management software or access point settings if it isn't feasible to do manually.

Wireless Scans

Please refer to the Network Security Policy Section 0 for information regarding wireless scans.

Audits

The wireless network must be audited quarterly to ensure that this policy is being followed. Specific audit points should be: location of access points, signal strength, SSID, SSID broadcast, and use of strong encryption.

Network Security Policy

Overview

The Company wishes to provide a secure network infrastructure in order to protect the integrity of corporate data and mitigate risk of a security incident. While security policies typically avoid providing overly-technical guidelines, this policy is necessarily a more technical document than most.

Purpose

The purpose of this policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support the Company's comprehensive set of security policies.

Scope

This policy covers all IT systems and devices that comprise the Cloud environment and supporting corporate systems including VPN and Wireless networks.

Policies

Network Device Authentication

A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches, and servers, must be held to higher standards than user-level or desktop system passwords.

Network Device Password Construction

Passwords can be a weak link in a security infrastructure. Because of this, the organization specifies that two-factor authentication be used for network devices. This may be in the form of a smart card, hardware or software token, biometrics, or another method that greatly enhances security.

The organization recognizes, however, that not every system (internal and external) is compatible with two-factor authentication, or that two-factor authentication isn't practical. In these situations management must be notified and a strong password selected. Where a password must be used, the organization mandates that users

adhere to the Company's Password Policy.

Failed Logins to Network Devices

Repeated login failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the Company must lock a user's account after 3 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the Information Security Manager.

In order to protect against account guessing, when login failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the login credentials you supplied were incorrect."

Network Device Default Value Change Requirements

Passwords must be changed according to the Company's Password Policy. Additionally, the following requirements apply to changing network device defaults:

- Vendor defaults are easy for an attacker to guess and can lead to a major security incident. For this reason the Company requires that all vendor default values be changed prior to a new device being installed on the network. This includes but is not limited to:
    - Encryption keys
    - SNMP Strings
    - Passwords/passphrases
- Additionally, these values must be changed when someone who has knowledge of the existing values leaves the Company, changes position, or any time there is a suspected security incident relating to these devices, even peripherally. This statement also applies to any consultant or contractor who has access to administrative passwords.
- If any network device password is suspected to have been compromised, all network device passwords must be changed immediately.

Password Policy Enforcement

Where passwords are used, technology must be implemented that enforces the Company's password policies on construction, changes, re-use, lockout, etc.

Administrative Password Guidelines

As a general rule, administrative (also known as "root") access to systems must be limited to only those who have a legitimate business need for this type of access. This is particularly important for network devices, since administrative changes can

have a major effect on the network, and, as such, network security. Additionally, administrative access to network devices must be logged.

Logging

The logging of certain events is an important component of good network management practices. Logs contained on application servers, network devices, and critical systems may all contain different data, but all contain valuable information that the Company must record. Thus, the Company requires that logging on network-level devices must be enabled to the fullest degree possible.

The following statements apply to the Company's implementation of logging:

- No passwords must be contained in logs.
- All security events must be logged
- All system components that store, process, or transmit Cardholder Data (CHD) and/or Sensitive Authentication Data (SAD), or that could impact the security of CHD and/or SAD must be logged
- All critical system components must be logged
- All servers and system components that perform security functions must be logged

Log Management

While logging is important to the Company's network security, log management can become burdensome if not implemented appropriately. As logs grow, so does the time required to review and manage the logs. For this reason, the Company recommends that a log management application be considered.

Log Review

Device logs do little good if they are not reviewed on a regular basis. Log management applications can assist in highlighting important events, however, these must be regularly reviewed. In addition:

- A System Administrator must review the events and logs on all system components on a daily basis.
- All exceptions must be entered into JIRA and assigned to the appropriate person for resolution.

Log Retention

Logs must be retained in accordance with the Company's Retention Policy. Unless known to contain non-proprietary or public data, the Company must classify network device logs as confidential data.

Firewalls

Firewalls are arguably the most important component of a sound security strategy. Internet connections and other unsecured networks must be separated from the Company network through the use of a firewall.

Configuration

The following statements apply to the Company's implementation of firewall technology:

- A firewall or firewalls must be configured by default to block inbound access to the network from external sources.
- Firewall rules must be as restrictive as possible while still providing the necessary access required for business operations.
- Firewalls must provide secure administrative access (through the use of strong encryption) with management access limited to only networks where management connections would be expected to originate.
- No unnecessary services or applications can be enabled on firewalls. The Company must use 'hardened' systems for firewall platforms, or use pre-hardened appliances.
- Clocks on firewalls must be synchronized with the Company's other networking hardware using NTP or other means. This should be done by either synchronizing directly to an external time server or by synchronizing to an internal time server which itself is synchronized to an external time server. Regardless of the architecture, the Company must ensure that its systems are synchronized to UTC (Coordinated Universal Time), which is received from reliable, industry-accepted time sources. Among other benefits, this will aid in problem resolution and security incident investigation.
- Firewall rules that allow access to high security zones or confidential information, regardless of the type of access, must be approved by management and documented accordingly. Documentation must include port, level and type of access, business reason for access, and proof of management approval for access.
- The firewall ruleset must be documented and audited every six months. Audits must cover each rule, what it is for, if it is still necessary, and if it can be improved.
- For its own protection, the firewall ruleset must include a "stealth rule," which forbids connections to the firewall itself.
- The firewall must log dropped or rejected packets.

Outbound Traffic Filtering

Firewalls are often configured to block only inbound connections from external sources; however, by filtering outbound connections from the network, security can be greatly improved. This practice is also referred to as "Egress Traffic Filtering."

Blocking outbound traffic prevents users from accessing unnecessary, and many times, dangerous services. By specifying exactly what outbound traffic to allow, all other outbound traffic is blocked. This type of filtering would block root kits, viruses, and other malicious tools if a host were to become compromised.

The Company requires that permitted outbound traffic be limited to only known 'good' services, which are the following ports: 22, 25, 53, 80, 143, 443, 465, 585, 993 and 995. All other outbound traffic must be blocked at the firewall unless an exception is granted from the Information Security Manager.

Networking Hardware

Networking hardware, such as routers, switches, bridges, and access points, must be implemented in a consistent manner. The following statements apply to the Company's implementation of networking hardware:

- Networking hardware must provide secure administrative access (through the use of strong encryption) with management access limited to only networks where management connections would be expected to originate.
- Clocks on networking hardware must be synchronized with the Company's other networking hardware using NTP or other means. This should be done by either synchronizing directly to an external time server or by synchronizing to an internal time server which itself is synchronized to an external time server. Regardless of the architecture, the Company must ensure that its systems are synchronized to UTC (Coordinated Universal Time), which is received from reliable, industry-accepted time sources. Among other benefits, this will aid in problem resolution and security incident investigation.
- Switches must be used instead of hubs. Hubs are not to be used without the specific permission of the Information Security Manager. When using switches the Company must use VLANs to separate networks if it is reasonable and possible to do so.
- Access control lists must be implemented on network devices that prohibit direct connections to the devices. Connections to routers must be limited to the greatest extent possible. Exceptions to this are management connections that can be limited to known sources.
- Only services, daemons, and protocols necessary for the system to perform the intended business functions are to be enabled on any system. All other

services, daemons, protocols must be disabled.
- Access to administrative ports on networking hardware must be restricted to known management hosts and otherwise blocked with a firewall or access control list.

Network Servers

Servers typically accept connections from a number of sources, both internal and external. As a general rule, the more sources that connect to a system, the more risk that is associated with that system, so it is particularly important to secure network servers. The following statements apply to the Company's use of network servers:

- Only services, daemons, and protocols necessary for the system to perform the intended business functions are to be enabled on any system. All other services, daemons, protocols must be disabled.
- Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.
- Clocks on network servers must be synchronized with the Company's other networking hardware using NTP or other means. This should be done by either synchronizing directly to an external time server or by synchronizing to an internal time server which itself is synchronized to an external time server. Regardless of the architecture, the Company must ensure that its systems are synchronized to UTC (Coordinated Universal Time), which is received from reliable, industry-accepted time sources. Among other benefits, this will aid in problem resolution and security incident investigation.
- A standard installation and hardening process has been developed for the Company's network servers. Refer to the system hardening process in the Vatom Inc Cloud System Configuration' document.
- Only one primary function may be implemented on each server (or virtual server) to ensure that different security levels do not coexist on the same server.
- Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers from each server. A list of enabled functions can be found in the 'Vatom Inc Cloud System Configuration' document.
- Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. A list of approved protocols can be found in the Vatom Inc Cloud System Configuration' document.

Intrusion Detection/Intrusion Prevention

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology can be useful in network monitoring and security. The tools differ in that an IDS alerts to suspicious activity whereas an IPS blocks the activity. When tuned correctly, IDSs are useful but can generate a large amount of data that must be evaluated for the system to be of any use. IPSs automatically take action when they see suspicious events, which can be both good and bad, since legitimate network traffic can be blocked along with malicious traffic.

The Company requires the use an IDS within the Cloud environment. All alerts from the IDS system must be analyzed for validity. If any intrusion is deemed to be a risk should be immediately remediated by following the Incident Response policy in Section **TBD**

Security Testing

Security testing is an important part of maintaining the Company's network security. Security testing can sometimes be provided by IT Staff members, but is often more effective when performed by a third party with no connection to the Company's day-to-day Information Technology activities, which is why the Company requires a mix of both strategies be used.

A risk rating must also be assigned to any vulnerability found:

Risk Rating	Criteria
Low	A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service attack
Medium	A vulnerability that allow local or remote users to increase their privileges on a system or access confidential information
High	A vulnerability that could potentially allow a user to gain privileged access to a system

Security testing must be performed as follows:

- At least quarterly by vAtomic staff
- At least annually by a third-party that specializes in application security
- After any changes to the environment.

Security testing must include, at a minimum, the following vulnerabilities:

- Injection flaws, particularly SQL injection
- Buffer overflow
- Insecure cryptographic storage
- Insecure communications
- Improper error handling
- All “high risk” vulnerabilities identified in the vulnerability identification process
- Cross-site scripting (XSS)
- Improper access control
- Cross-site request forgery (CSRF)
- Broken authentication and session management

If any vulnerabilities are detected they must be logged in JIRA, corrected, and the application must be reevaluated after the corrections.

As part of security testing, vulnerability testing must be performed that is based on industry-accepted penetration testing approaches and includes:

- Coverage for the entire CDE perimeter and critical systems.
- Testing from both inside and outside the network.
- Testing to validate any segmentation and scope reduction controls.
- Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed above.
- Defines network-layer penetration tests to include components that support network functions as well as operating systems.
- Review and consideration of threats and vulnerabilities experienced in the last 12 months.
- Retention of penetration testing results and remediation activities results.

Wireless Scans

The Company must evaluate the network for unauthorized wireless access devices connected to the network, such as wireless access points, wireless cards, and portable wireless devices (such as USB-connectable devices).

This analysis must be performed at least quarterly via physical and wireless spectrum analysis.

Refer to the Company’s Incident Response Plan for specific actions to take if an unauthorized wireless device is discovered, either during a manual scan or discovered via automated analysis.

The process to detect and identify wireless access points is as follows:

- The IT department must perform a scan around the same time every quarter.
- A physical inspection must be conducted by looking in each office and workspace for unauthorized wireless and other network devices.
- A complete network scan for unauthorized wireless access points must be done using the Kismet tool combined with any wireless card which supports raw monitoring (rfmon) mode.
- All discovered networks should be correlated to known networks. Any unknown networks should be tested to ensure that they belong to neighboring offices and are not connected to the internal network.
- The results of the scan must be documented and any unauthorized wireless devices should be found, disabled and reported to the Information Security Officer.

Security Patch Validation

The Company must evaluate all software installed in the Cloud environment for new security patches. The external sites listed below must be used to validate the current security vulnerabilities, and patches available. This should be compared to the current patch levels in the environment and all new "High" security patches must be installed within one month.

- http://linux.web.cern.ch
- http://www.gnu.org
- http://www.linuxquestions.org

Internal Vulnerability Scans

Internal Vulnerability Scans, that is, vulnerability scans that test systems from a point internal to the network perimeter, must be performed quarterly in the Cloud environment. At a minimum, all systems in the cardholder data environment or high security zones must be included in the scope of the internal scans. The purpose of these scans is to locate any vulnerabilities that exist on the local network, that are either exploitable by local access or that may be hidden by firewalls or other access controls.

Internal scans can be performed by qualified company personnel who are reasonably independent of the systems being tested. Alternatively, the Company may engage a third party to conduct the internal scans. Any third party company selected must be recognized as an Approved Scanning Vendor (ASV) by the PCI SSC.

The Company must put a process in place to quickly remediate any vulnerabilities discovered that are rated "high-risk" vulnerabilities. After remediation activities, the

Company must rescan the network until no high-risk vulnerabilities are found.

In addition to the regularly scheduled quarterly scans, the Company must re-scan the network after any significant change to the network, such as: new component installations, changes in network topology, firewall rule changes, product upgrades, etc. These scans can be performed by internal company personnel as qualified above.

External Vulnerability Scans

External Vulnerability Scans, that is, vulnerability scans that test systems from a point external to the network perimeter, must be performed quarterly in the Cloud environment. External scans must test the Company's security posture from a public perspective (the internet). The purpose of these scans is to locate any vulnerabilities that exist and can be accessed from external sources.

External scans must be performed by an Approved Scanning Vendor (ASV) with organizational independence of the Company's systems and security configuration. The Company must put a process in place to quickly remediate any vulnerabilities discovered that are rated "high-risk" vulnerabilities. After remediation activities, the Company must rescan the network until no high-risk vulnerabilities are found, such as those rated higher than 4.0 by the Common Vulnerability Scoring System (CVSS).

In addition to the regularly scheduled quarterly scans, the Company must re-scan the network after any significant change to the network, such as: new component installations, changes in network topology, firewall rule changes, product upgrades, etc. These scans can be performed by internal company personnel who are reasonably independent of the systems being tested.

Penetration Testing

In addition to vulnerability scans, both external and internal penetration testing must be performed in the Cloud environment at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).

These penetration tests must include the following:

- Network-layer penetration tests
- Application-layer penetration tests

Disposal of Information Technology Assets

IT assets, such as network servers and routers, often contain sensitive data about the Company's network communications. When such assets are decommissioned, the following guidelines must be followed:

- Any asset tags or stickers that identify the Company must be removed before disposal.
- Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.
- At a minimum, data wiping must be used. Simply reformatting a drive or deleting data does not make the data unrecoverable. If wiping is used, the Company must use the most secure commercially-available methods for data wiping. Alternatively, the Company has the option of physically destroying the data storage mechanism from the device (such as its hard drive or solid state memory).

Network Compartmentalization

Good network design is integral to network security. By implementing network compartmentalization, which is separating the network into different segments based on their security classification, the Company will reduce its network-wide risk from an attack, virus outbreak, or unauthorized disclosure of confidential information. Firewalls and routers must be configured to seriously restrict or block connections between trusted and untrusted networks. Further, security can be increased if traffic must traverse additional enforcement/inspection points. The Company requires the following with regard to network compartmentalization:

High Risk Networks and High Security Zones

Network/Zone:

XXX REDACTED XXXX

Requirements:

Access must be restricted to only those services and ports that are absolutely necessary for business operations and separate the network with a firewall. Direct access to or from these networks is prohibited. This includes both inbound and outbound traffic. Initially an implicit “deny all” rule must be implemented and then specific, limited access opened as necessary. The firewall must support dynamic packet filtering, such that only established connections are allowed through. Management approval must be obtained for any rule or configuration change that

provides access at any level to high security zones. Any ports opened to high security zones must be documented (inbound or outbound). Documentation must include: the port, the level and type of access, the necessary business reason for the access, and management approval for such access. Access must only be granted when there is no other viable way to meet the business need.

Externally-Accessible Systems

Network/Zone:

XX REDACTED XXXX

Requirements:

Segmentation of externally-accessible systems from the Company's internal network is required, and must be enforced with a firewall or router that provides granular access controls (source, destination, service, port, etc.).

Internal Networks

Network/Zone:

XX REDACTED XXXX

Requirements:

Segmentation of internal networks from one another can improve security as well as reduce chances that a user will access data that he or she has no right to access. The Company requires that networks be segmented to the fullest reasonable extent. If the internal network is also considered a high risk or high security zone, then the more restrictive policy will apply.

Network Documentation

Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network ensures that the Company's IT Staff has a firm understanding of the network architecture at any given time. The intangible benefits of this are immeasurable.

The Company requires a formal network documentation process. At a minimum, network documentation must include:

- Network diagram(s), including any wireless networks

- System configurations
- Firewall ruleset
- IP Addresses
- Access Control Lists
- Details of rule changes as specified in section 4.9.1

The Company requires that network documentation be updated on a quarterly basis.

Sharing of network documentation, including private IP addresses and routing information, must be authorized by the Information Security Officer.

Antivirus/Anti-Malware

Computer viruses and malware are pressing concerns in today's threat landscape. If a system or network is not properly protected, a virus outbreak can have devastating effects on the system, the network, and the entire company. The Company provides the following guidelines on the use of antivirus/anti-malware software:

- All company-provided user workstations and servers must have antivirus/anti-malware software installed.
- Workstation software must maintain a current "subscription" to receive patches and virus signature/definition file updates.
- Patches, updates, and antivirus signature file updates must be installed in a timely manner, either automatically or manually. Software must be set to automatically install updates whenever practical.
- Antivirus solution must be capable of detecting and removing all known threats. In addition to viruses, the software must eradicate threats from all known malware, adware, spyware, Trojans, rootkits, worms, or any other known malicious virus-like software.
- Antivirus software must automatically run periodic scans with no user intervention required to initiate the scan.
- Antivirus software must be able and configured to generate audit logs that are retained for at least one year. A minimum of three months' logs are required to be available for immediate restoration and/or analysis.

Software Use Policy

Software applications can create risk in a number of ways, and thus certain aspects of software use must be covered by this policy. The Company provides the following requirements for the use of software applications with the Cloud environment:

- Only legally licensed software may be used. Licenses for the Company's software must be stored in a secure location.

- Open source and/or public domain software can only be used with the permission of the Information Security Manager.
- Software must be kept reasonably up-to-date by installing new patches and releases from the manufacturer.
- Vulnerability alerts must be monitored for all software products that the Company uses. Any patches deemed critical, in that they fix vulnerabilities or security holes, must be installed within one month of the patch release.

Maintenance Windows and Scheduled Downtime

Certain tasks require that network devices be taken offline, either for a simple reboot, an upgrade, or other maintenance. When this occurs, the IT Staff must perform the tasks during a scheduled weekly or monthly maintenance window. Tasks that are deemed "emergency support," or tasks required to close discovered vulnerabilities, as determined by the Information Security Manager, must be done with one hour's notice to users or immediately if the situation dictates.

Change Management

Documenting changes to network devices is a good management practice and can help speed resolution in the event of an incident. The IT Staff must document and implement hardware and/or configuration changes to network devices as per the following Change Management Process that has been codified in JIRA.

Change Management Process

Note: No changes can be applied to the environment that are not submitted through JIRA

The JIRA process must include:

- Documentation of impact.
- Documented change approval by authorized parties.
- Functionality testing to verify that the change does not adversely impact the security of the system.
- Back-out procedures.

Device Labeling

Network devices must bear a sticker or tag indicating essential information, such as the device name, IP address, asset information, and any additional data that may be helpful, such as information about cabling.

Documentation Requirements

As stated in 4.9.1, any ports opened to high security zones must be documented (inbound or outbound). Documentation must include: the port, the level and type of

access, the necessary business reason for the access, and management approval for such access. Granular documentation for all firewall rule changes, not just those that fall under the requirement above, is recommended.

Suspected Security Incidents

When a security incident is suspected that may impact a network device, the IT Staff must refer to the Company's Incident Response policy for guidance.

Redundancy

Redundancy can be implemented on many levels, from redundancy of individual components to full site-redundancy. As a general rule, the more redundancy implemented, the higher the availability of the device or network, and the higher the associated cost. The Company wishes to provide the IT Manager and/or Information Security Manager, as appropriate, with latitude to determine the appropriate level of redundancy for critical systems and network devices. Redundancy should be implemented where it is needed, and should include some or all of the following:

- Hard drive redundancy, such as mirroring or RAID
- Server level redundancy, such as clustering or high availability
- Component level redundancy, such as redundant power supplies or redundant NICs
- Keeping hot or cold spares onsite

Manufacturer Support Contracts

Outdated products can result in a serious security breach. When purchasing critical hardware or software, the Company must purchase a maintenance plan, support agreement, or software subscription that will allow the Company to receive updates to the software and/or firmware for a specified period of time. The plan must meet the following minimum requirements:

Hardware: The arrangement must allow for repair/replacement of the device within an acceptable time period, as determined by the Information Security Manager, as well as firmware or embedded software updates.

Software: The arrangement must allow for access to updates, upgrades, and hotfixes for a specified period of time.

Security Policy Management

It is the Company's intention to comply with this policy not just on paper but in its everyday processes as well. With that goal in mind the Company requires the following:

Information Security Officer

An employee must be designated as the manager of the Company's security program. He or she will be responsible for the Company's compliance with this security policy and any applicable security regulations. This employee must be responsible for A) the initial implementation of the security policies, B) ensuring that the policies are disseminated to employees, C) training and retraining of employees on the Company's information security program (as detailed below), D) any ongoing testing or analysis of the Company's security in compliance with this policy, E) updating the policy as needed to adhere with applicable regulations and the changing information security landscape.

The Information Security Manager must maintain a list or database of all critical technologies (such as remote access technologies, wireless technologies, laptops, tablets, email, and the Internet) and the users that have access to these technologies. The list must include all devices and personnel with access to the technologies, the approval of the relevant authorized parties to use the technologies, the authentication methods for the use of the technologies, and acceptable network locations for the devices.

Additional employees can be included in the Company's security program as deemed necessary. All security roles and responsibilities must be clearly defined, with appropriate escalation paths. Further, an employee (can be the Information Security Manager) or team must be specifically designated as the contact in the event of a suspected security incident.

Security Awareness Training

A security awareness program must be implemented that will detail the Company's information security program to all users and/or employees covered by the policy, as well as the importance of data security. The training program must cover, among other topics, the appropriate handling of Protected Data. Employees must sign off on the receipt of, and in agreement to, the user-oriented policies upon hire and at least annually. Likewise, security awareness training must be performed upon hire and at least annually.

The following Topics are covered by the training:

Topic	Audience	Provider	Occurrence
Cybersecurity in the Workplace	All	ADP	Annual

Cybersecurity Foundations	IT Managers	LinkedIn	On demand
Learning Security Frameworks	IT Staff	LinkedIn	On demand
Programming Foundations: Web Security	Developers	LinkedIn	On demand
JavaScript: Security Essentials	Developers	LinkedIn	On demand

Security Policy Review

The Company's security policies must be reviewed at least annually. Additionally, the policies must be reviewed when there is an information security incident or a material change to the Company's security policies or network. As part of this evaluation the Company must review:

- Any applicable regulations for changes that would affect the Company's compliance or the effectiveness of any deployed security controls.
- If the Company's deployed security controls are still capable of performing their intended functions.
- If technology or other changes may have an effect on the Company's security strategy.
- If any changes need to be made to accommodate future IT security needs.

Network Configuration Review

The Company's network configuration must be reviewed regularly. The following table describes the specific components, review period and actions that must be taken upon each review:

XX REDACTED XXXX

Time Synchronization Policy

Overview

Time synchronization ensures that all systems securely and reliably acquire time to synchronize log events and other application events across servers and the supporting infrastructure.

Purpose

The purpose of this policy is to outline the Company's standards for synchronizing time across systems so that it is used securely and managed appropriately.

Scope

This policy covers all time synchronization in the Cloud environment.

Policies

Updates

All time synchronization systems and services must have the latest vendor-supplied security patches installed within one month of release.

Please refer to the Network Security Policy Section Error! Reference source not found. for more information regarding security testing and patch updates.

Time Sources

Please refer to the 'Vatom Inc Enterprise API Platform System Configuration' document for an overview of the time synchronization architecture.

Time settings may only be received from industry-accepted time sources

Only designated central time servers may receive time signals from external sources.

Time signals from external sources must be based on International Atomic Time or UTC.

Time Distribution

The designated central time servers must peer with each other to keep accurate

time.

Other internal servers may only receive time from the central time servers.

Access Control

Access to time data is restricted to the System Administrator.

Change Management

All changes to the time settings are subject to the change management process described in the Network Security Policy Section Error! Reference source not found..

Encryption Policy

Overview

Encryption, also known as cryptography, can be used to secure data while it is stored or being transmitted. It is a powerful tool when applied and managed correctly. As the amount of data the Company must digitally store increases, the use of encryption must be defined and consistently implemented in order ensure that the security potential of this technology is realized.

Purpose

The purpose of this policy is to outline the Company's standards for the use of encryption technology so that it is used securely and managed appropriately.

Scope

This policy covers all data stored on or transmitted across the Cloud Environment.

Policies

Applicability of Encryption

Encryption plays a versatile role in the Company's data security. Since many policies contain requirements pertaining to encryption, this section summarizes those requirements from other policies:

Remote Access

The Company requires that remote access to the network be secured with strong encryption for both users and administrators. Encryption must be initiated prior to the administrative password being changed.

Mobile Devices

Mobile devices, such as laptops, mobile computers, removable storage media, and tablets, must, at minimum, use an encrypted partition to store company data. Whole disk encryption should be considered if the data on the device is especially sensitive.

Email and Instant Messaging

Confidential information must never be sent via email or any other end-user

messaging technologies without the use of strong encryption, regardless of recipient. Credit Card Primary Account Numbers (PANs) must never be sent via end-user messaging, regardless of encryption.

Backups

Confidential data must be stored in encrypted form using industry-standard strong encryption algorithms to protect the Company against data loss.

Authentication

Authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to the Company network or across a public network such as the Internet.

Site-to-site VPNs

Site-to-site VPNs must utilize strong encryption to protect data during transmission. Encryption algorithms must meet or exceed current minimum industry standards.

Confidential Data

Strong encryption must be used for confidential data transmitted external to the Company. Confidential data must always be stored in encrypted form, whether such storage occurs on a user system, server, laptop, or any other device that allows for data storage.

When confidential data, such as cardholder information, is transmitted via wireless networks, the Company must use wireless industry best practices for encryption, such as IEEE 802.11i. Only the strongest encryption algorithms must be used to secure this data during transmission. Please note that the use of known insecure encryption methods, such as WEP, is expressly prohibited.

Firewall Configuration

Firewalls must provide secure administrative access (through the use of strong encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.

Network Hardware

Networking hardware must provide secure administrative access (through the use of strong encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.

Encryption Key Management

Key management is critical to the success of an implementation of encryption technology. The following guidelines apply to the Company's encryption keys and

key management:

Management of keys must ensure that data is available for decryption when needed, including the retention of keys necessary to decrypt encrypted backups.

- Keys must be backed up.
- Keys must be locked up.
- Keys must never be transmitted in clear text.
- Keys are considered confidential data.
- Keys must not be shared.
- Keys must not be stored on the same media as the encrypted information, and must be stored in the fewest locations possible.
- Physical key generation materials must be destroyed immediately upon generation.
- Keys must be used and changed in accordance with the password policy.
- When user encryption is employed, minimum key length is 12 characters.
- Keys must be known or accessed by the fewest number of employees necessary.
- The Company must perform background checks on the persons in charge of encryption keys.
- For secure key storage the Company must use split knowledge or dual control (for example, requiring two or three people, each knowing only their key component, to reconstruct the whole key).

Acceptable Encryption Algorithms

Only the strongest types of generally-accepted, non-proprietary encryption algorithms are allowed, as dictated by industry best practices on encryption. Use of proprietary encryption is specifically forbidden since it has not been subjected to public inspection and its security cannot be assured. The length of encryption keys should meet the following guidelines:

- 128 bits for SSL and TLS ciphers
- 2048 bits for public key algorithms based on factorization (i.e., RSA)
- 160 bits for elliptic curve cryptography (i.e., ECDSA)

Acceptable algorithms should be reevaluated as encryption technology changes.

Key Generation

The system uses different keys for different purposes as follows:

XXXX REDACTED XXXX

SSH Key Generation

To configure SSH on the system, you require a configuration for each user. This is described in detail in the following reference:

https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/s1-ssh-configuration.html

The process for user key generation is:

- The user uses a tool such as ssh-keygen to generate their public and private keys
- The user securely transmits the public key to the System Administrator
- The System Administrator updates the user's SSH configuration

Note: The system-wide configuration is automatically done as part of the server installation

Remote access for the root user must be disabled after the System Administrator account has been created and a private key established for SSH. This is described as part of the hardening process in the 'Cloud Platform System Configuration' guide.

SSL Key Generation

SSL keys are generated using the Java Keytool to generate a Java Keystore containing the private and public keypair and signed certificate.

Note: Key Generation requires 2 people: Platform Owner and System Administrator. System Administrator secures the keystore using their password while the Platform Owner secures the private key using their password.

The process to follow is:

- Generate a Java keystore and key pair

keytool -genkey -alias mydomain -keyalg RSA -keystore keystore.jks -keysize 2048

- The system will prompt for the keystore password, which must be provided by the System Administrator
- The system will then prompt for all the certificate information which is provided by the System Administrator (eg. CN=*.vatom.com, OU=Cloud Platform, O=VatomInc, L=Los Angeles, ST=California, C=US)
- The system will then prompt for the key password, which must be provided by the Platform Owner
- Generate a certificate signing request (CSR) for the alias

keytool -certreq -alias mydomain -keystore keystore.jks -file mydomain.csr

- Import a root or intermediate CA certificate to an existing Java keystore

keytool -import -trustcacerts -alias root -file Thawte.crt -keystore keystore.jks

- Import a signed primary certificate to an existing Java keystore

keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore keystore.jks

Disk Encryption Key Generation

Disk encryption is used on both server and laptop systems:

- Disks within the Cloud environment is provided by Amazon EC2.
- Laptop and desktop disk encryption keys are generated by Bitlocker (Windows) and File Vault (Mac)

Each encrypted volume gets a new, unique key at creation time

Key Distribution

Keys may only be distributed over a secure network using SSL or SSH.

SSH Key Distribution

Only the public SSH keys should be distributed and must be distributed over a secure connection

SSL Key Distribution

To configure SSL, the listeners on the server must be updated with the keys and cert in the keystore created above in section 4.4.2.

The System Administrator must use an existing SSL connection or SSH tunnel to connect to the web console and configure the listener keys.

The web console will prompt the use for the keystore password and the key password which must be entered by the System Administrator and Platform Owner respectively.

Disk Encryption Key Distribution

Keys are not distributed.

Key Storage

SSH Key Storage

The user's SSH keys must be stored on password protected systems and protected using a keyphrase. Both password and keyphrase must comply with the password construction policy in the Password Policy.

SSL Key Storage

The SSL keys are stored in two places:

1. The original keystore used in key generation

2. The encrypted disk within the environment

The original keystore is stored within the corporate private network and protected by a dual-password which must be entered by the System Administrator and Platform Owner.

The disk is encrypted with dm-crypt as mentioned above.

Disk Encryption Key Storage

Disk encryption is used on both server and laptop systems:

- Server disk encryption keys are kept in the Agility database. The keys are encrypted at rest, at a field level, using symmetric AES-encryption.
- Laptop disk encryption keys are stored on the disk and recovery keys are securely stored by the IT Systems Administrators.

Key Expiry

The system must be configured to notify the System Administrator two week before an SSL certificate expiry deadline. The System Administrator must then generate a new a new key pair, CSR and obtain a new certificate as described in Section 4.4.2.

Key Retirement

In the event that the integrity of the key has been weakened, a new key must be generated and installed. The process differs depending on the system:

SSH Key Retirement

The user's account must be suspended immediately.

A new public and private key must be generated and stored by following the process in Section 4.4.1.

The retired keys must be destroyed.

Once the new public key has been associated with the user account, it can be reopened.

SSL Key Retirement

Access to the site must be suspended.

The System Administrator must generate a new a new key pair, CSR and obtain a new certificate as described in Section 4.4.2.

The retired keys must be destroyed.

After the installation of the new certificate, access to the site can be allowed

Disk Encryption Key Retirement

External access to the system must be suspended.

The System Administrator must create a new volume that is encrypted with a new key and copy all the content from the compromised volume to the new volume and mount it appropriately.

The retired keys may be used to decrypt already archived data and must be stored in such a way that they are no longer usable for encrypting data.

Once the old volume has been destroyed, the system can be made available again.

Assignment of Key Custodians

All employees that manage keys as described in the previous section must accept their responsibilities as Key Custodians. See Appendix D.

Legal Use

Some governments have regulations applying to the use and import/export of encryption technology. The Company must conform with encryption regulations of the local or applicable government.

The Company specifically forbids the use of encryption to hide illegal, immoral, or unethical acts. Anyone doing so is in violation of this policy and will face immediate consequences per the Enforcement section of this document.

Trusted Keys/Certificates

Only certificates issued by recognized providers such as Versign may be used in the environment or accepted when connecting into the environment to transmit protected data or provide authentication within the environment. The Information Security Officer must maintain a list of trusted certificates in the Policy Manager system.

Secure Protocols

Many protocols or configurations have both secure and non-secure versions. When transmitting Confidential Data, only the secure version of the protocol (e.g. HTTPS versus HTTP) or configuration must be used.

Software Development Policy

Overview

This policy describes the Software Development Policies used by the Company.

Purpose

The purpose of this policy is to list and state the software-development policies and procedures that must be in place to protect applications from a range of vulnerabilities

Scope

This policy applies to the applications that are leveraged within the Cloud environment and the Company's information systems that handle confidential data.

Policies

Source Code Analysis

The software must be regularly scanned using a source code analysis tool that identifies common vulnerabilities. Scans must be performed at least on a monthly basis, ideally daily. The list of vulnerabilities must include, at a minimum:

- Injection flaws, particularly SQL injection
- Buffer overflow
- Insecure cryptographic storage
- Insecure communications
- Improper error handling
- All “high risk” vulnerabilities identified in the vulnerability identification process
- Cross-site scripting (XSS)
- Improper access control
- Cross-site request forgery (CSRF)
- Broken authentication and session management

Vendor Management Policy

Overview

The vendors and 3rd party Service Providers used by the Company are subject to the following general principles:

1. A smaller number of proven vendors who are responsive, thoughtful.
2. Vendors who understand the mission, challenges and limitations of SaaS companies.
3. Long-term relationships.
4. Pursuit of the lowest price is not the primary purpose.
5. Vatom Inc will challenge prices from vendors when prices deviate significantly and consistently from past patterns.

Purpose

The purpose of this policy is to list and state the compliance of the Service Providers used by the Company.

Scope

This policy applies to the service providers that are leveraged within the Cloud environment and the Company's information systems that handle confidential data.

Policies

Due Diligence

Prior to engaging vendors or service providers, they must be subjected to a due diligence process as follows:

- They must comply with any applicable laws regarding the protection of confidential data
- They must have appropriately up-to-date certifications
- They must acknowledge in a written agreement that they will maintain all applicable requirements as it relates to confidential data
- They must be approved by the Information Security Officer

Statements of Work

- A Statement of Work (SOW) must clearly state the security requirements for the vendors to ensure that their work is consistent with the Company's security requirements.
- In general, contracts for software and other services delivered from cloud vendors are reviewed by the Information Security Officer for security compliance.
- Statement of Works must include a clear description of the scope of services provided under the contract or purchase order.
- Statement of Works must clearly identify any and all types of sensitive data to be exchanged and managed by the vendor. Sensitive data is defined as either regulated or confidential.
- Statement of Works and contracts must contain a documented System Security Plan which describes all existing and planned security controls.

Contracts

Reporting Requirements

- Contracts must clearly identify security reporting requirements that stipulate that the vendor is responsible for maintaining the security of sensitive data, regardless of ownership.
- In event of a breach of the security of the sensitive data, the vendor is responsible for immediately notifying the Company and working with the both regarding recovery and remediation.
- Security reporting requirements in the contract must also require the vendor to report all suspected loss or compromise of sensitive data exchanged pursuant to the contract within 24 hours of the suspected loss or compromise.

Breach Notification

The vendor is responsible for notifying all persons whose sensitive data may have been compromised as a result of the breach as required by law.

Sanctions

Contracts must include formal sanctions or penalties for failure to meet the security requirements in the contract or purchase document.

Termination of Service

- Upon termination of vendor services, contracts must require the return or destruction of all Company systems' data in accordance with Access Control

Policy.
- Procurement and contract managers are to immediately ensure termination of all access to information systems and, if applicable, facilities housing these systems.

Management and Oversight

Policy Compliance

Vendors are required to comply with all the applicable Company Information Security Policies.

Contract Maintenance

Departments that have implemented contracts shall ensure all contracts being renewed are updated with provisions supporting the requirements of this policy.

Reporting and Monitoring

Communications

Departments shall provide the appropriate security reporting contact information to each vendor upon contract initiation, along with any reporting instruction specific to the respective public agency.

Inspection and Review

The Company shall have the ability to inspect and review vendor operations for potential risks to operations or data. This review may include a planned and unplanned physical site inspection, technical vulnerabilities testing, and an inspection of documentation, such as security test results, IT audits, and disaster recovery plans.

Risk Reporting

All contracts shall require the vendor to produce regular reports focusing on four primary potential risk areas:

- Unauthorized Systems Access
- Compromised Data
- Loss of Data Integrity
- Inability to Transmit or Process Data
- Exception Reporting

Any exceptions from normal activity are to be noted in the reports, reviewed, and the appropriate responses determined.

Service Provider List

- A list of service providers must be maintained and kept up to date. For convenience, the following list of service providers are used by the Company, must be updated annually:

Name	Description	Type	Confidential Data Policy
Amazon AWS	Datacenter provider - has physical custody of the Company systems and the data on them but no access to confidential data. They cannot login to the Company systems.	Datacenter provider	(SOC 1), Type II

- Service providers' data confidentiality compliance status must be verified at least annually.
- A record must be kept describing which data confidentiality requirements are managed by each service provider, and which are managed by the Company. For convenience, this list is maintained here:

Name	Data Confidentiality Requirement	Description

Appendix A: Assignment as Information Security Officer

The signer of this document is an employee with the Company on the date shown below and hereby acknowledges that I have read and understand the Information Security Policy and accept responsibility for performing the Information Security Officer duties laid out therein, including but not limited to:

- Creating and distributing security policies and procedures
- Creating and distributing security incident response and escalation
- Quarterly reviews of the Information Security Policy
- Managing Security Awareness Training
- Performing the annual Risk Assessment

I agree to the above in full and understand my responsibilities as indicated above.

Signed: _____

Printed Name: _____

Date: _____

Witnessed: _____

Printed Name: _____

Appendix B: Policy Acceptance Form

The signer of this document is an employee with Vatom Inc on the date shown below, with access to computer systems and company information, and hereby agrees that he/she:

- Has read and understood the Information Security Policy and agrees to comply with them.
- He/she has had the opportunity to ask questions regarding this policy, and has had those questions answered to their satisfaction.
- Agrees to promptly report to management any suspicious activity, including but not limited to system or key compromise or theft.

I agree to the above in full and understand my responsibilities as indicated above.

Signed: _____

Printed Name: _____

Date: _____

Witnessed: _____

Printed Name: _____

Appendix C: Key Custodian Form

The signer of this document is an employee with Vatom Inc on the date shown below, with access to key management devices, software, and/or equipment, and hereby agrees that he/she:

- Has read and understood the policies and procedures associated with key management and agrees to comply with them to the best of their ability.
- He/she has had the opportunity to ask questions regarding this policy, and has had those questions answered to their satisfaction.
- Agrees to never divulge to any unauthorized party the key management practices or any related security systems, passwords, processes, or other secrets associated with the company's systems.
- Agrees to promptly report to management any suspicious activity, including but not limited to system or key compromise or theft.

I agree to the above in full and understand my responsibilities as indicated above.

Signed: _____

Printed Name: _____

Date: _____

Witnessed: _____

Printed Name: _____

Appendix D: Assignment as System Administrator

The signer of this document is an employee with Vatom Inc on the date shown below and hereby acknowledges responsibility for performing the System Administrator duties laid out in the Information Security Policy, including but not limited to:

- Daily log reviews of all system components, including those that perform security functions
- Monthly reviews to ensure that the latest vendor-supplied security patches are installed
- Internal Vulnerability Scans both quarterly and after any significant change in the network
- Quarterly reviews of the network documentation to ensure that it remains current
- Bi-annual reviews of the firewall and router rule sets
- Annual inventories of the media containing confidential data
- Annual audits to confirm that the backup media is secure
- Monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel
- Administering user account and authentication management
- Monitoring and controlling all access to data
- Performing a quarterly audit of physical and information assets in the EAPaaS environment to assess the Company's risk if one were to be lost or stolen
- Following the appropriate Incident Response policy in the case of theft of a physical or information asset in EAPaaS environment

I agree to the above in full and understand my responsibilities as indicated above.

Signed: _____

Printed Name: _____

Date: _____

Witnessed: _____

Printed Name: _____

Appendix E: Acceptable Use Policy

1. Computer Access Control – Individual's Responsibility

Access to Vatom Inc's IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on Vatom Inc's IT systems.

Individuals must not:

- Allow anyone else to use their user ID/token and password on any Vatom Inc IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Vatom Inc's IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorized changes to Vatom Inc's IT systems or information.
- Attempt to access data that they are not authorized to use or access.
- Exceed the limits of their authorization or specific business need to interrogate the system or data.
- Connect any non- Vatom Inc authorized device to the Vatom Inc network or IT systems.
- Store Vatom Inc data on any non-authorized Vatom Inc equipment.
- Give or transfer Vatom Inc data or software to any person or organization outside Vatom Inc without the authority of Vatom Inc.

Line managers must:

- Ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.
- Maintain, and keep current, a list of company-approved products
- Maintain, and keep current, a list of all devices and personnel authorized to use them
- Provide a method to accurately and readily determine owner, contact information, and purpose for all devices

2. Internet and Email Conditions of Use

Use of Vatom Inc Internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Vatom Inc in any way, not in breach of any term and condition of employment and does not place the individual or Vatom Inc in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the Internet and email systems.

Individuals must not:

- Use the Internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Vatom Inc considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
- Use the Internet or email to make personal gains or conduct a personal business.
- Use the Internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to Vatom Inc, alter any information about it, or express any opinion about Vatom Inc, unless they are specifically authorized to do this.
- Send unprotected sensitive or confidential information externally.
- Forward Vatom Inc mail to personal (non-Vatom Inc) email accounts (for example a personal Hotmail account).
- Make official commitments through the Internet or email on behalf of Vatom Inc unless authorized to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect Vatom Inc devices to the internet using non-standard connections.

3. Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorized access or loss of information, Vatom Inc enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

4. Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with Vatom Inc remote working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

5. Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Vatom Inc authorized mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

6. Software

Employees must use only software that is authorized by Vatom Inc on Vatom Inc's computers. Authorized software must be used in accordance with the software supplier's licensing agreements. All software on Vatom Inc computers must be approved and installed by the Vatom Inc IT department.

Individuals must not:

- Store personal files such as music, video, photographs or games on Vatom Inc IT equipment.

7. Viruses

The IT department has implemented centralized, automated virus detection and virus software updates within Vatom Inc. All laptops and desktops have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Vatom Inc anti-virus software and procedures.

8. Telephony (Voice) Equipment Conditions of Use

Use of Vatom Inc voice equipment is intended for business use. Individuals must not use Vatom Inc's voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances.

All non-urgent personal communications should be made at an individual's own expense using alternative means of communications

Individuals must not:

- Use Vatom Inc's voice facilities for conducting private business.
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators, unless it is for business use.

9. Actions upon Termination of Contract

All Vatom Inc equipment and data, for example laptops and mobile devices

including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Vatom Inc at termination of contract.

All Vatom Inc data or intellectual property developed or gained during the period of employment remains the property of Vatom Inc and must not be retained beyond termination or reused for any other purpose.

10.Monitoring and Filtering

All data that is created and stored on Vatom Inc computers is the property of Vatom Inc and there is no official provision for individual data privacy, however wherever possible Vatom Inc will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Vatom Inc has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, the UK Data Protection Act 1998, the Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000.

This policy must be read in conjunction with:

- Computer Misuse Act 1990
- Data Protection Act 1998

It is your responsibility to report suspected breaches of security policy without delay to your line management, the IT department, the information security department or the IT helpdesk.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Vatom Inc disciplinary procedures.

Appendix F: InfoSec Organization Chart

XXX REDACTED XXXX