Information Security Plan (ISP)

Written guidelines and instructions approved by management, and published by security/legal committee and communicated to all workforce including employees and relevant external parties.

Version Revision

Date	Version	Description	Author(s)
July 1st 2017	1.0	Initial version	Irvin Tyan,
August 10th 2018	2.0	Added organization chart of information security Reviewed and updated policies	Trong Dong, Thien To, Long Nguyen, Minh Tong

Table of Content

I. Information Stewardship Policy

Scope and Applicability:

Policy: RAKUNA shall protect the security and privacy of all information entrusted to it.

Overview:

1. RAKUNA is committed to protecting the security and privacy of all information entrusted to it. Our services and internal operating processes and procedures will be in compliance with applicable laws and regulations, as well as established industry practices.

2. The purpose of this Written Information Security Plan and related policies (the "Plan") is to provide a framework for protecting information. Information is no longer simply something which supports the provision of a product or service. Information itself has become an asset.

3. The purpose of this Plan is to define and clarify policies, principles, standards, guidelines, and responsibilities related to the security of RAKUNA technology resources.

4. An information security management policy is necessary to serve goals pertaining to operations, records and facilities. Such goals include:

Ensuring continuity of operations.

Protecting the integrity of business records.

Preventing unauthorized access to records.

Protecting privacy and security of sensitive information.

5. The primary objectives of this Plan and its associated policies are:

To effectively manage the risk of security exposure or compromise within the systems.

To communicate the responsibilities for the protection of information.

To establish a secure processing base and a stable processing environment.

To promote understanding and compliance with all applicable laws and regulations.

To protect management and preserve management's options in the event of an information asset misuse, loss or unauthorized disclosure.

Procedures:

1. In accordance with other company policies and procedures, RAKUNA management is responsible for:

1.1 Ensuring a sufficient level of training takes place for people entering or modifying data in the company system(s).

1.2 Making decisions about the permissible uses of information.

1.3 Understanding the uses and risks associated with information. This means that they are responsible for the consequences associated with improper disclosure, insufficient maintenance, inaccurate classification labeling, and other security related control deficiencies pertaining to the information for which they have responsibility.

1.4 Protecting the information in their possession from unauthorized access, alteration, destruction, or usage.

1.5 Establishing, monitoring and operating information systems in a manner consistent with policies and standards.

2. In accordance with other company policies and procedures, employees, contractors, consultants, temporary workers, and other workers at RAKUNA are responsible for:

2.1 Using the information only for the purposes specifically approved by management.

2.2 Complying with all RAKUNA security measures.

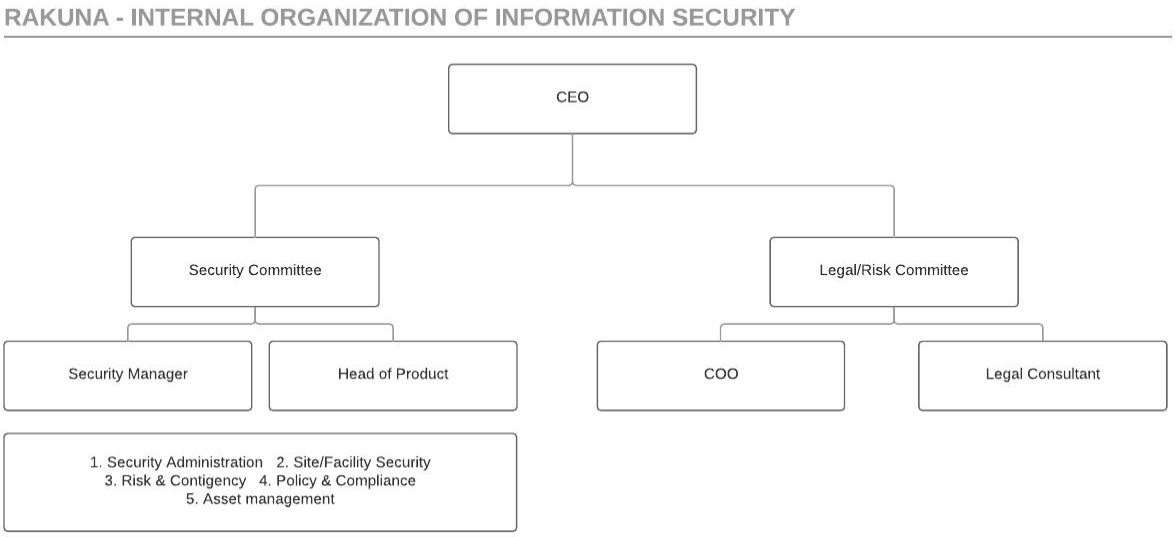
2.3 Refraining from unauthorized disclosure of information in their possession.

2.4 Reporting all situations where they believe a privacy or security vulnerability or violation may exist.

3. Any member of the workforce found to have violated this Plan or its associated policies may be subject to disciplinary action, up to and including termination.

4. The Plan will be reviewed and updated as needed, but no less than every two (2) years.

II. Internal Organization of Information Security



SECURITY MANAGER

Authority and Reporting:

1. The Security Manager is appointed by management.
2. The Security Manager reports to CTO.
3. Whenever a policy or procedure related to Information Security Plan requires action or decision by a decision maker and the decision maker is not clearly identified in such policy or procedure, the Security Manager shall be the decision maker or shall designate the decision maker.

Responsibilities:

The Security Manager --

1. Exercises responsibility for the development and implementation of the information security plan.
2. Is responsible for implementing, managing, and enforcing information security directives as mandated by Federal, state or local law, regulation or statute (collectively "Law").
3. Reviews and recommends modification of Information Security Plan and all supporting policies and procedures in light of operating experience, changes in Law, and changes in available compliance tools.
4. Ensures the ongoing integration of information security with business strategies and requirements.
5. Ensures that the access control, incident response, and risk management needs of the organization are properly addressed.

6. Leads information security awareness and training initiatives to educate the Company's workforce about information risks and the policies and procedures of Information Security Plan.
7. Performs ongoing information risk assessments and audits to ensure that information systems are adequately protected and meet Law certification requirements.
8. Works with vendors, outside consultants, and other third parties to improve information security within the organization.
9. Leads an incident response team to contain, investigate, and prevent future computer security breaches.
10. Monitors the effectiveness of Information Security Plan and incorporates the results of monitoring into recommendations for amendment, sanction or other action.
11. Maintains working relationships with legal counsel and outside consultants and uses the services of such parties to assist with implementing, managing and enforcing Information Security Plan.
12. Assures timely and effective training and retraining of the Company's workforce with respect to Information Security Plan.
13. Uses judgment in assessing exposure, recommending solutions, and overseeing compliance with Information Security Plan.
14. Appropriately delegates responsibilities, as necessary.
15. Such other responsibilities as may be delegated to the Security Manager by the company's CTO

III. Risk Analysis and Management Policy

Scope and Applicability:

Policy: RAKUNA shall conduct an initial risk assessment and subsequent risk assessment(s), as appropriate, to identify the potential risks to and vulnerabilities of Non-Public Personal Information (as defined in the Gramm-Leach-Bliley Act), proprietary or confidential information or other protected information (collectively referred to as "Protected Information") possessed or maintained by RAKUNA. RAKUNA shall further adopt and implement reasonable and appropriate safeguards and security measures to protect against any reasonably foreseeable threats to the privacy, integrity and availability of the Protected Information and the information systems in which Protected Information is created, received, transmitted and maintained.

Procedures:

1. When evaluating, selecting, rejecting and implementing safeguards, the following factors should be considered:

1.1 Safeguards for the protection of the privacy and security of confidential information and Protected Information should be targeted to foreseeable threats to the privacy or security of such information. It is appropriate to consider RAKUNA's actual experience over the years with security and privacy of information when assessing risk or safeguards.

1.2 Safeguards should be reasonable. They should be designed to prevent improper access to, or use and disclosure of, confidential information or Protected Information by workforce and others, but they should not interfere with RAKUNA's ability to conduct its business. It is important to balance these objectives.

1.3 Safeguards should be reasonably affordable. It is appropriate to engage in cost benefit analysis. RAKUNA recognizes that it will not always be able to select the most effective solution in an area due to the cost of the solution or the potential detriment to other areas of compliance or operations that may result.

1.4 Safeguards must be evaluated within the resources and capabilities of the organization. These are RAKUNA's responses to perceived threats to the privacy and security of information at RAKUNA, and they should be tailored to fit RAKUNA's specific needs.

1.5 The selection of safeguards, such as the assessment of risk, is to be regarded as dynamic in light of RAKUNA's operating and compliance experience and understanding of applicable laws and regulations. All compliance steps should be open to reevaluation and change. Criticism and suggestions should be encouraged.

2. All software purchases, upgrades and development relative to Protected Information shall take into account the potential impact on applicable information security laws, statutes and regulations, including Law compliance. Hardware and software acquisitions and upgrades relative to Protected Information will be evaluated in light of RAKUNA's Plan.

3. The Security Manager shall conduct a risk assessment designed to:

3.1 Identify the potential risks and vulnerabilities to the confidentiality, integrity and availability of critical data and information technology.

3.2 Identify potential means to mitigate such risks and vulnerabilities.

3.3 Identify areas where RAKUNA's Plan fails to satisfy the requirements of the Law and other applicable information security laws, statutes and regulations.

3.4 The risk assessment will be conducted periodically and whenever significant changes occur in the RAKUNA information technology environment.

IV. Sanctions Policy

Scope and Applicability:

Policy: RAKUNA shall apply sanctions to workforce members who violate the Law or the policies and procedures of this Plan.

Procedures:

1. Examples of sanctions include, but are not limited to:

1.1 Verbal warnings.

1.2 Written warnings.

1.3 Employment suspension.

1.4 Termination of access to Protected Information.

1.5 Termination of employment.

2. Workforce members shall agree to comply with security policies and procedures and acknowledge this sanction policy by signing a NDA.

3. All sanctions will be applied to all workforce members consistent with existing personnel policies and procedures.

V. Information Systems Activity Review Policy

Scope and Applicability:

Policy: RAKUNA shall review information systems activity on a periodic basis to determine whether Protected Information is accessed or disclosed inappropriately.

Procedure:

1. Examples of information system activity records may include, but are not limited to, audit logs, access reports and Security Incident reports.
2. The Security Manager shall determine the records to be reviewed, the frequency of such review and the individual responsible.
3. Any Security Incidents identified as a result of information systems activity review shall be investigated as outlined in the Security Incident Policy and Procedures.

VI. Workforce Security Policy

Scope and Applicability:

Policy: RAKUNA shall ensure that workforce members requiring access to Protected Information have appropriate access while other workforce members who do not require Protected Information to perform their job duties re prevented from accessing such information.

Procedure:

AUTHORIZATION AND/OR SUSPENSION

1. All workforce members and others requiring access to Protected Information shall be identified.
2. Authorization to access Protected Information shall be granted as necessary based on job functions.
3. Access to Protected Information shall be periodically monitored by the Security Manager and any designees.

WORKFORCE CLEARANCE

1. All personnel having access to Protected Information shall undergo an appropriate background investigation prior to employment. Such check may include, but shall not be limited to, a credit check, verification of references and a criminal background check.
2. All personnel having access to Protected Information shall be subject to ongoing, periodic background checks.
3. Documentation regarding background checks, personnel actions, the levels of access granted to each individual, program and procedure should be maintained for at least six years.
4. Access levels shall be reviewed periodically and when the status of a workforce member changes.

TERMINATION OF EMPLOYMENT

Upon termination of employment of any company employee, the following tasks will need to be completed:

1. Give the former member a copy of the employee's signed confidentiality statement and notify the former member of his or her ongoing confidentiality duties.
2. Recover from the former member all keys and access tokens for facilities, buildings, offices, desks and file cabinets.
3. Disable employee network access, e-mail accounts, and access to all other systems.
4. If the former member had system level or administrative access to systems containing sensitive information, change system passwords for all systems containing or allowing access to sensitive information.
5. If the former member had remote system access, all hardware, software and electronic information must be retrieved.
6. Change the former member's voice mail message to include directions regarding who or whom to contact.

7. Review computer files and forward or destroy, as appropriate.
8. As appropriate, notify customers and vendors with ongoing issues or projects involving the former member that such member is no longer employed.

VII. Information Access Management Policy:

Scope and Applicability:

Policy: RAKUNA shall grant workforce members access to Protected Information as required by their job duties. Such access will be limited to the minimum necessary amount of Protected Information as may be required for the workforce member to properly perform his or her job duties.

Procedure:

A. Access Authorization

1. The minimum amount of Protected Information required to perform the job duties shall be determined and documented.
2. Authorization to access Protected Information shall be based upon such documentation.

B. Access, Establishment and Modification

1. Unique usernames and passwords are created to authorize access to Protected Information.
2. A record of authorized users is maintained.
3. User records are reviewed periodically.
4. Access authorization is modified or terminated as necessary based on changes in job duties and changes in personnel.

VIII. Education, Training and Awareness Policy

Scope and Applicability:

Policy: The information security and privacy policies and procedures of RAKUNA will be communicated to all members of the workforce and a program to maintain effective awareness of information security policies and procedures will be implemented and maintained.

Procedure:

1. All workforce members of RAKUNA must be informed of security and privacy policies and procedures and their responsibilities in writing. All new workforce members of RAKUNA will sign a statement acknowledging they have received and read the policy and understand their responsibilities. This should include knowledge of the consequences of violations of security procedures.
2. All workforce members must be informed that any actions taken under their assigned identification, such as a user "ID," are their personal responsibility.
3. Important aspects of any information security and privacy policies and procedures will be communicated on a regular basis through postings, distributions, logon screens, meetings or other means that provide regular and useful reminders concerning information security and privacy policies and standards.
4. Persons responsible for information technology resources must be aware of the information security and privacy policies and procedures and must be knowledgeable about effective security practices for the technical environment under their control. In particular, such individuals shall be trained regarding password maintenance, incident reporting and viruses and other forms of malicious software.
5. Guidelines and examples for users will be developed and disseminated to assist in maintaining good security practices. This material may include brochures, electronic reminders, desk references, web sites, etc., and should include but not be limited to information on passwords and password protection, logon id, virus protection strategies, etc.

IX. Acceptable Use Policy

Scope and Applicability:

Policy: All use of RAKUNA's information technology is to be in compliance with this Plan, policies and procedures, and sound business judgment. RAKUNA shall monitor e-mail, Internet use, and other computer resources.

Procedure:

1. The Security Manager shall develop, implement and administer a procedure for restricting log-on access to individual terminals or workstations to only those members and authorized users that (i) follow the applicable log-on authorization procedure, and (ii) are actually authenticated as authorized users.

2. Use of the Internet, e-mail and other uses of computer resources must always be able to withstand public scrutiny and not cause legal liability or embarrassment to RAKUNA.

3. Workforce members shall be made aware that they should have no expectation of privacy when using RAKUNA resources or networks to access the Internet, e-mail or otherwise using RAKUNA computer and information resources.

4. E-mail.

4.1 RAKUNA shall employ virus protection software on workstations to prevent transmission of viruses in e-mail attachments and diskettes, as appropriate.

4.2 E-mail that is not secure or encrypted should not be used to send Protected Information.

5. Unacceptable Use. Unacceptable uses of RAKUNA's information technology include, but are not limited to:

5.1 Violation of the privacy of other users and their data.

5.2 Violation of the legal protection provided by copyright and licensing laws applied to programs and data.

5.3 Attempts by members to monitor or intercept the files or electronic communications of other members or third parties.

5.4 Attempts by members to hack or obtain access to systems or accounts they are not authorized to use.

5.5 Use of other members' log-ins or passwords.

5.6 Use of electronic media in a manner that is likely to cause network congestion or significantly hamper the ability of other members to access and use RAKUNA's system.

5.7 Use inconsistent with laws, regulations or accepted community standards.

5.8 Transmission of material in violation of any local, state or federal law or regulation is prohibited. It is not acceptable to transmit or knowingly receive threatening, obscene or harassing material.

5.9 Intentionally or knowingly releasing a virus or other program that damages, harms, or disrupts a system or network.

5.10 Violation of the integrity of computing systems. For example, users shall not intentionally develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system.

5.11 Use of the RAKUNA computing facilities for fund-raising or public relations activities unrelated to an individual's employment by RAKUNA.

5.12 Malicious or disruptive use, including use of the RAKUNA facilities or any attached network in a manner that precludes or significantly hampers its use by others. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer worms or viruses, and use to make unauthorized entry to any other machine accessible via the network.

5.13 Using RAKUNA resources for unauthorized or illegal purposes or knowingly accepting or using information which has been obtained by illegal means.

5.14 Use in conjunction with for-profit or activities, unless such activities are stated as a specifically acceptable use.

5.15 Use for private or personal business, or other commercial activities not related to the Company's business.

5.16 Misrepresentation of one's self, an agency, or RAKUNA.

5.17 Accessing or attempting to access data or information without proper authorization even if it is not securely protected.

5.18 Obtaining, possessing, using or attempting to use someone else's password regardless of how the password was obtained.

5.19 Sending an overwhelming number of files across the network (e.g., spamming or e-mail bombing).

5.20 Preventing others from accessing services.

6. Users are not permitted to install any unapproved software or attach any device to their computer or workstation without specific approval.

7. Users are responsible for conducting routine backups, installing and using virus protection routines and installing patches and updates in accordance with RAKUNA procedures.

8. Users must ensure that computer repairs are undertaken in a manner that protects the confidentiality of data stored in the system.

9. Workstations and their disks, with critical and sensitive data stored on them or accessible through them, should be further secured (using software) against unauthorized use even by someone who has legitimate access to the physical space.

10. Equipment may not be removed from the office area without the department head's prior approval.

11. Virus Protection.

11.1 RAKUNA Users shall employ virus protection on all workstations connected to RAKUNA's networks, including those remotely accessing our network, as appropriate. Users shall not attempt to turn off the virus protection nor alter the antivirus settings on RAKUNA managed workstations.

11.2 Workstations using antivirus software that are not centrally managed must have the antivirus software set to scan all files before allowing them to be accessed or changed. Such antivirus software must be configured to update its virus definitions at least weekly.

11.3 Because computer viruses have become so complex, Users must not try to eradicate viruses without expert assistance. If a User suspects infection by a virus, they must immediately disconnect from the network or shut down their machine and then call the Help Desk.

11.4 NEVER open e-mail from an unknown, suspicious or untrustworthy source nor download any attachments from such e-mail.

11.5 Delete Spam, chain, and other junk e-mail without opening or forwarding such e-mail.

11.6 Do not forward virus warnings which you may receive via e-mail to friends or coworkers. Instead, forward such e-mail warnings to the Security Manager. Most of these warnings are hoaxes that accomplish the same results as actual viruses; they cause mass e-mailings.

12. Personal Use of RAKUNA's Information Resources.

12.1 RAKUNA's Information Resources are to be used primarily for business purposes only for the performance of one's job responsibilities.

12.2 Occasional and reasonable non-business usage of systems may be allowed at the discretion of management, provided that such usage:

(a) Does not interfere with work performance or productivity of oneself or others.

(b) Does not consume more than a trivial amount of resources that could otherwise be used for business purposes.

(c) Does not endanger the privacy or security of Protected Information.

(d) Is not contrary to RAKUNA's Policies, standards or procedures.

12.3 Users are responsible for exercising good judgment regarding the reasonableness of personal use.

12.4 If there is any uncertainty on whether a use is appropriate or allowed, the User should consult their supervisor or manager. The supervisor or manager may consult the Security Manager for further guidance.

X. Passwords Policy

Scope and Applicability:

Policy: Strong passwords shall be used, changed frequently and protected.

Procedure:

1. Passwords are used for various purposes at RAKUNA. Some of the more common uses include: user level accounts, web accounts, e-mail accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

2. All user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least every 3 months.

3. All user-level and system-level passwords must conform to the guidelines described below.

3.1 Poor, weak passwords have the following characteristics:

(a) The password contains less than eight characters.

(b) The password is a word found in a dictionary (English or foreign).

(c) The password is a common usage word.

3.2 Strong passwords should be used wherever technically feasible.

3.3 Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase.

3.4 Do not use the same password for RAKUNA accounts as for other non-RAKUNA access (e.g., personal ISP account, option trading, benefits, etc.).

3.5 Here is a list of password "don'ts":

(a) Don't reveal a password over the phone to ANYONE.

(b) Don't reveal a password in an e-mail message.

(c) Don't talk about a password in front of others.

(d) Don't hint at the format of a password (e.g., "my family name").

(e) Don't reveal a password on questionnaires or security forms.

(f) Don't share a password with family members.

(g) Don't reveal a password to co-workers at any time, including when absent from RAKUNA.

3.6 Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

3.7 If an account or password is suspected to have been compromised, promptly report the incident to the Security Manager and change the password.

XI. Privacy and Security Incident Policy

Scope and Applicability:

Policy: All Privacy and Security Incidents shall be reported to the Security Manager who shall take appropriate steps to block further incidents, repair and restore service, and preserve evidence.

Procedure:

Any information concerning a known or suspected privacy or security breach (an "Incident") must be reported to the Security Manager without delay and in writing. In addition, the Security Manager may, after consultation with legal counsel, report the incident to outside authorities whenever this is required to comply with legal requirements, rules or regulations.

Response and reporting, investigation and Mitigation

1. The Security Manager is responsible for managing mitigation efforts. Specifically, the Security Manager shall:

1.1 Block or prevent continuation of the incident, if possible.

1.2 Repair the resulting damage and fix the root cause.

1.3 Restore service to its former level, if possible.

1.4 Preserve evidence, where appropriate.

2. Upon receipt of written notice, the Security Manager shall, without delay, identify and record any damage caused, and restoration or repair required, as well as gather all of the necessary information required to prosecute the reported issue if applicable. The Security Manager will develop a detailed plan to effectively remedy and respond to all reported incidents pursuant to this policy. Additionally, the Security Manager will develop, maintain and update a database of reported information Security Incidents with any effective remedies/responses in order to better protect RAKUNA from similar or future information Security Incidents.

3. The appropriate response to an Incident is determined by the Security Manager based on the potential and/or actual impact of the incident.

4. Any harmful effects of the Incident will be mitigated to the extent practical.

XII. Contingency Plan Policy

Scope and Applicability:

Policy: RAKUNA shall develop, implement and maintain appropriate procedures to respond to system emergencies or other occurrences (i.e., fire, vandalism, system failure, natural disaster, etc.). These procedures shall constitute RAKUNA's "Contingency Plan."

Procedure:

1. Data Back-up Plan.

1.1 Back-ups of critical information and/or Protected Information shall be conducted in a manner to allow timely recovery of information.

1.2 Administrators are responsible for backing up each system and required to implement a tested and auditable process.

1.3 As appropriate, centralized services back-ups will be stored on-site for quick recovery.

1.4 Critical business functions shall also have back-ups stored in an off-site, secured commercial facility.

1.5 Application software shall be copied to a separate back-up medium as new applications are added.

1.6 System software should be copied periodically and as major changes are made.

2. Disaster Recovery Plan.

2.1 In the event of an emergency, the Security Manager or a designee shall assess the impact to Protected Information and operations.

2.2 The Security Manager or a designee shall activate the disaster recovery plan by notifying the appropriate personnel.

2.3 The Security Manager shall identify an alternate location if necessary.

2.4 The Security Manager shall arrange for replacement equipment if necessary.

2.5 Back-up shall be retrieved from cloud storage and restored.

3. Emergency Mode Operation.

3.1 The Security Manager shall ensure the physical security of Protected Information during emergency mode operations limiting physical access to the extent practicable.

3.2 The Security Manager shall ensure the technical security of Protected Information via user identification codes and passwords to the extent practicable.

4. Contingency Operations.

4.1 The Security Manager shall grant temporary access as necessary to replace equipment and restore lost data.

4.2 The Security Manager shall grant access to workforce members as required for contingency operations.

5. Testing and Revision.

RAKUNA's Contingency Plan shall be tested (and revised as appropriate) periodically and whenever significant changes occur in the RAKUNA information technology environment. Copies of the contingency plan shall be maintained in multiple off-site locations. Workforce members who deem to be suitable shall receive training in contingency plan procedures.

6. Applications and Data Criticality Analysis.

6.1 The Security Manager shall determine the Protected Information most critical in the event of an emergency.

6.2 The systems and software used to access such Protected Information shall be prioritized for restoration.

XIII. Evaluation Policy

Scope and Applicability:

Policy: RAKUNA shall perform a periodic technical and non-technical evaluation to make certain that RAKUNA's security policies and procedures continue to comply with the Law.

Procedure:

1. The Security Manager, with the assistance of technical specialists, shall determine the frequency and scope of each evaluation.

2. The evaluation shall consider:

2.1 For the initial evaluation, the standards under the Law.

2.2 For all subsequent evaluations, environmental and operational changes affecting the security of Protected Information.

3. Documentation of evaluations shall be maintained as a Law record.

XIV. Back-Ups and Recovery Policy

Scope and Applicability:

Policy: Back-ups of critical information shall be conducted in a manner to allow timely recovery of information.

Procedure:

1. Administrators are responsible for backing up each system and required to implement a tested and auditable process.
2. Centralized services back-ups will be stored on-site for quick recovery.
3. Critical business functions shall also have their back-ups stored off-site.
4. RAKUNA will implement information resource security precautions to ensure the timely recovery of data and provide appropriate back-up processing capabilities in the event of a loss.
5. Application software shall be copied to a separate back-up medium as new applications are added to or on a daily basis, depending on site requirements.
6. System software should be copied weekly and as major changes are made to system software.

XV. Workstation Administration Policy

Scope and Applicability: This policy covers any and all workstations owned or operated by RAKUNA.

Policy: Workstations shall be used in a manner to safeguard the confidentiality and integrity of Protected Information.

Procedure:

1. A workstation administrator shall be responsible for the following activities:

1.1 Maintaining a record of to whom each workstation is assigned.

1.2 Maintaining an inventory of all workstation hardware components, including serial numbers.

1.3 Maintaining a log of the physical location of all hardware components.

1.4 Distributing software to each workstation.

1.5 Maintaining an inventory of all software loaded.

1.6 Ensuring all software used at a workstation is licensed.

1.7 Retaining custody of keys to locks on workstations.

1.8 Ensuring that all hardware components are physically marked for ease of identification.

2. Workstation users shall signoff of their workstation at the end of the day or their shift.

3. All workstations shall automatically lock or logoff the network after a predefined period of inactivity. The timeframe is 10 minutes

3.1 All workstations shall also have an easily accessible way to lock the workstation at will. (Example: Icon on Windows desktop to engage the password-protected screensaver.)

4. All workstations shall maintain a log of all system access, including attempted log-ins.

XVI. Destruction of Protected Information Policy

Scope and Applicability: This policy covers any and all media containing Protected Information.

Policy: Media shall be wiped or destroyed in a manner to safeguard the confidentiality of Protected Information.

Procedure:

1. Protected Information must not be discarded in trash bins, unsecured recycle bags or other publicly-accessible locations. Instead this information must be personally shredded or placed in a secured recycling bag.

2. Printed material and electronic data containing Protected Information shall be disposed of in a manner that ensures confidentiality.

3. It is the individual's responsibility to ensure that the document has been secured or destroyed. And it is the supervisor's responsibility to ensure that their employees are adhering to the policy.

4. Electronic Copies. Secure methods will be used to dispose of electronic data and output. The IT department is responsible for the destruction of electronic copies containing Protected Information. However, employees may dispose of the electronic data themselves using the following methods:

4.1 "Degaussing" computer tapes to prevent recovery of data;

4.2 Deleting on-line data using the appropriate utilities;

4.3 Removing Protected Information from mainframe disk drives being sold or replaced, using the appropriate initialization utilities;

4.4 Erasing diskettes to be re-used using a special utility to prevent recovery of data; or

4.5 Destroying discarded diskettes.

5. Hardcopy (Bulk Destruction). Secure methods will be used to dispose of hardcopy data and output.

5.1 Protected Information printed material shall be shredded and recycled by a firm specializing in the disposal of confidential records or be shredded by an employee of RAKUNA authorized to handle and personally shred the Protected Information.

5.2 Microfilm or microfiche must be cut into pieces or chemically destroyed.

5.3 After documents have reached their retention period, all Protected Information must be securely destroyed using the record retention process governing destruction of records.

5.4 If hardcopy Protected Information (paper, microfilm, microfiche, etc.) cannot be shredded, it must be incinerated.

6. Documentation of Destruction

6.1 To ensure that it is in fact performed, RAKUNA personnel or a bonded destruction service must carry out the destruction of Protected Information.

6.2 If COMPANY personnel undertake the destruction of the records, the RAKUNA personnel must use the RAKUNA records destruction form provided by the IT department, if the record is found on the record retention schedule for the department destroying the record.

If a bonded shredding company undertakes the destruction, the bonded shredding company must provide RAKUNA with the document of destruction that contains the following information: Date of destruction Method of destruction; description of the disposed records; inclusive dates covered; a statement that the records have been destroyed in the normal course of business; and the signatures of the individuals supervising and witnessing the destruction.

XVII. Email Policy

Scope and Applicability: This policy covers appropriate use of any email sent from a Rakuna email address and applies to all employees, consultants, contractors, vendors, and agents operating on behalf of Rakuna.

Policy: Ensure the proper use of email system and make users aware of what deems as acceptable and unacceptable use of Rakuna's email system

Procedures:

1. All use of email must be consistent with policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
2. Email account should be used primarily for business related purposes; personal communication is permitted on a limited basis, but non- related commercial uses are prohibited.
3. All sensitive data contained within an email message or an attachment must be secured and encrypted.
4. Email should be retained only if it qualifies as a business record. Email is a business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
5. The Rakuna email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Rakuna employee should report the matter to their supervisor immediately.
6. Users are prohibited from automatically forwarding Rakuna email to a third party email system or personal email. Individual messages which are forwarded by the user must not contain Rakuna confidential or above information.
7. Users are prohibited from using third-party email systems and storage servers to conduct Rakuna business, to create or memorialize any binding transactions, or to store or retain email on behalf of . Such communications and transactions should be conducted through proper channels using Rakuna-approved documentation.
8. Using a reasonable amount of Rakuna resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email.
9. Users are strictly prohibited from:
    - 9.1. Sending unsolicited email messages such as chain mail or spam.
    - 9.2. Forging or attempting to forge email messages, or disguising or attempting to disguise your identity when sending mail.
    - 9.3. Giving out a password for any type of Rakuna account via email.
10. Rakuna employees shall have no expectation of privacy in anything they store, send or receive on the company's email system.
11. Rakuna may monitor messages without prior notice.