



Security Management ISO/IEC 27001:2013

Feb'1st, 2024

RAMTeCH Software Solutions, Inc.

6303 Osgood Ave North

Stillwater, MN 55082

P: 651.342.1780

F: 651.430.0201

www.ramtech-corp.com

Table of Contents

SECTION 1 – SECURITY MANAGEMENT POLICIES	3
1.1 Organization and Management	4
1.2 Information Classification	4
1.2.1 Connectivity and Data Transfer	5
1.2.2 Confidentiality Agreement	5
1.3 Personnel Security & Background Checks	5
1.4 Information Security – Internal Controls and Processes	6
1.5 IT Security – Network Connections (Internet, Firewalls, Intrusion Detection)	7
1.6 Physical Security	8
1.7 Information Back-up and Disaster Recovery	9
1.8 Privilege Management	10
1.9 Media Disposal	11
1.10 Backup Media Disposal	11
1.11 Employee Separation (Exit Process for Leavers)/Role Change	11
1.12 Incident Management	12
1.13 Antivirus policy	13
1.14 Business Continuity	14
1.15 System Audit and Logging Policy	15
1.16 Client Information Security	15
1.17 Operational Change Management	16
1.18 Risk Assessment Approach and Management	17
SECTION 2 – ISO CERTIFICATES	20
SECTION 3 – CYBER INSURANCE CERTIFICATE	22

Record of Revisions

Revision Number	Section	Revision Issued on (Date)	Revision Updated on (Date)	Revision Updated by (Name)
Rev1.1		September 30, 2021	September 30, 2021	Nagesh Kumar
Rev1.2a	2, 3	September 30, 2021	September 30, 2021	Nagesh Kumar
Rev1.3	3	January 27, 2022	January 27, 2022	Nagesh Kumar
Rev1.4	1	September 19, 2022	September 18, 2022	Nagesh Kumar
Rev1.5	Page 11	June' 28, 2023	June' 28, 2023	Nagesh Kumar
Rev1.6	Page 20	Sep' 28, 2023	Sep' 28, 2023	Nagesh Kumar
Rev1.7	Page 22	Feb' 1st, 2024	Feb' 1st, 2024	Nagesh Kumar
Rev1.8	Page 22	Mar' 9 th , 2025	Mar' 9 th , 2025	Nagesh Kumar

SECTION 1 – SECURITY MANAGEMENT POLICIES

As companies operate in increasingly competitive domestic and global markets, effective security policies are essential to protect both company and customer-related information. RAMTeCH has viewed this as a strategic focus for the company for many years and places particular importance upon the protection of information, which is increasingly stored and processed electronically. We recognize that an accredited security policy is necessary for securing compliances with relevant legislation, protecting customer confidentiality requirements, and maintaining customer confidence.



RAMTeCH's philosophy concerning client information security can be summed up as *"providing a secure platform for all RAMTeCH and customer data, protecting the company employees, assets, information, integrity, and reputation from potential threats."* RAMTeCH adheres to ISO standards and by virtue of it, ensures that this confidential information is not misused. The purpose of information security is to enable information to be shared between those who need to use it at the client's behest while protecting information from unauthorized access and loss. The basic principles of client information security that RAMTeCH always applies are:

- Confidentiality: Protect information from unauthorized access or use
- Integrity: Safeguard the accuracy and completeness of information and processes
- Accessibility: Ensure that information is available to authorized people when it is needed

RAMTeCH is certified for ISO/IEC 27001:2013, which is for Physical, Data, and IT Security and has stringent Information Security Management System Policy (ISMS) that are formal documented policies and procedures to provide secure platform and environment for all RAMTeCH and client data. Additionally, it protects data and information integrity and reputation from potential threats, while protecting all company employees and assets. This system also includes information back-up processes and procedures as well as a comprehensive business continuity strategy and plan.

Our security systems, protocols, policies have been audited on a regular basis by the ISO certifying organization, BSI Management Systems, as well as many of our customers and were found to comply – we have never failed an audit, nor have we ever had a security breach of any kind in the 29-year history of the company.

RAMTeCH's Information Security Management System (ISMS) consists of the following major components:

- Organization and Management
- Personnel Security
- Information Security – Internal Controls and Processes
- IT Security – Network Connections (Internet, Firewalls, Intrusion Detection)
- Physical Security
- Information Back-up and Disaster Recovery

- Business Continuity

Each of the components listed above are outlined in more detail below:


1.1 Organization and Management

Consists of the following organizational roles, responsibilities, and processes:

- Dedicated organization managed by Chief Information Security Officer (CISO)
- Core committee is responsible for management, performance, and review of all security systems every six months (or as required)
- Formal “Information Security Forum” (ISF) instituted with roles and responsibilities aligned to ISMS policies
- Forum reviews and discusses the overall security including risk analysis & assessment, mitigation planning and implementation
- Incident response team (IRT) in place
- Information, Asset Categorization & Control
- Regular reviews of information security function, policies, & procedures
- Periodic review of incidents by CISO

1.2 Information Classification

The classification of data and documents is essential to differentiate between the value of information and whether it is highly sensitive and confidential. Whenever data is received, stored, created, or amended they are always classified into appropriate sensitivity levels as detailed in the chart below.

	Company Confidential	<ul style="list-style-type: none"> • Request for Proposals • Client Contacts • Employee Personal Details • Financials • System and Data Backups • Intellectual Property and Software • Security Protocols and Audits • Infrastructure and IT Administration • Processed Data
	Client Confidential	<ul style="list-style-type: none"> • Request for Proposals • Source Data, Documents, and Samples • Specifications and Requirements • Technical, Procedural, and Standard Documentation • Tools • Project and Data Deliverables • Pricing • Communications and Reporting
	Internal	<ul style="list-style-type: none"> • Internal Communications • Project Reports • Shift Schedules • Holidays List • Standard Operating Procedures • Presentations
	General	<ul style="list-style-type: none"> • RAMTeCH Website • Recruitment Advertisements • Press Releases • Media Content and Conference Presentations • Blogs • Marketing Brochures • Social Media

Company Confidential: Highly sensitive assets and documents related to RAMTeCH e.g., investment strategies, business plans, sensitive customer information, Intellectual Property, Employee information, finished proposals, etc. are classified under this category. Disclosure or loss of this information could seriously affect the organization. The company's confidential information has very restricted access and is kept secure. Such information is not copied or removed from the organization's operational control without specific authorization.

Client Confidential: Information related to clients (past or present), but under the custody of RAMTeCH e.g., their test data, programs, project artifacts, legacy source data & databases, and client information are shared among cross-functional departments or project execution groups are classified under this category. Disclosure of this information could seriously affect the reputation and image of the organization. This information is made accessible based on a need-to-know basis only. This information is shared with the employees after relevant authorization from the project heads.

Internal: Information approved for internal circulation within the organization such as internal communications, Project Reports, shift schedules, presentations, job vacancies, quality reports, etc. are classified under this category. Disclosure of this information would inconvenience the organization or management but does not affect the reputation and image of the organization. Security at this level is controlled at normal.

General: Information in the public domain, annual reports, RAMTeCH website, press releases, media content and conference presentations, brochures, etc. is classified under this category. This information has been approved by the Executive Management for public use. Security at this level is minimal.

1.2.1 Connectivity and Data Transfer

We have point-to-point links between our office in India and Client locations across the globe with security and encryption. All our FTP/sFTP servers are behind the firewall. We have secure FTP /sFTP servers for hosting the project data. RAMTeCH will carry out FTP/sFTP transfers using these links. In addition, we can also transfer the data through VPN as per Client requirements.

1.2.2 Confidentiality Agreement

All RAMTeCH staff sign a confidentiality agreement (proprietary information agreement) as part of their initial conditions of employment. This may be included in the Code of Ethics and Acceptable Use Policy Agreement that establishes the principles of conduct that all employees are expected to observe. Contract personnel and other staff such as maintenance staff, security etc., who are not already covered by an existing confidentiality agreement are required to sign the Non-Disclosure Agreement prior to being granted access to any Information Processing areas. The agreement is reviewed when there are changes to the terms of employment or contract.

1.3 Personnel Security & Background Checks

Consists of the processes and policies employed for hiring, onboarding, and managing personnel:

- Comprehensive reference and background check and verification for each new employee
- Required security training for all new employees
- Mandatory security awareness training at least once every six months for all employees
- Competency tests are conducted to evaluate the effectiveness of training
- Non-disclosure & confidentiality agreements signed by employees

- Client specific agreements signed by individuals as required
- Security briefing and consequences for non-compliance
- Security permanent ID card badge & photo ID for all employees
- Address verification of employees every six months
- Visitor sign-in and photo ID verification
- Visitors must be accompanied by manager as well as Visitor & House Logs are maintained
- Since many of RAMTeCH employees hold Indian Passports, we rely upon the Indian Government for the verification process. The following is an overview of the processes used by
- RAMTeCH for background investigation:
 - An employee, who is issued an Indian passport which is issued by the Regional Passport Authority, Government of India, is a through criminal background check. The passport issue process involves police verification and hence is considered as a valid criminal check record. The police clearance certificate is taken from the Regional Passport Office. Alternatively,
 - A Police Verification Certificate can be taken from the police department if the employee does not hold a valid passport.
 - (or) In the case where the passport and/or police clearance certificates are not available in a timely manner, RAMTeCH performs background checks through a private security agency who will certify the individuals

Disciplinary process in place and communicated to employees during induction, security awareness programs. Whilst focused here for disciplinary action following security breaches, it can also be dovetailed with other disciplinary reasons. Hence HR disciplinary process covers information security in the manner required for the ISO 27001:2013 standard. Formal disciplinary process in place for any type of information security breach, as you would expect it needs you to clearly communicate to the employees (think inductions, reviews, team meetings etc). There are three levels in the formal disciplinary procedure depending upon the gravity of the case and/or the on-going nature of the misconduct.

- Level One –Verbal warning
- Level Two - Written warning
- Level Three Formal – Termination

Acceptable use Policy: All the employees shall adhere to the acceptable usage of facilities such as systems, Email and Internet provided to them, that in-turn facilitates for a secure and productive working environment. Employees of RAMTeCH accessing company electronic-mail services are not supposed to use or access an electronic-mail account assigned to another individual to either send or receive messages. If there is need to read another's mail (while they are away on vacation for instance), message forwarding, and other facilities are used instead. However, in case of exigencies, approval from the competent authority is taken for user privileged transfer of viewing and accessing the emails.

1.4 Information Security – Internal Controls and Processes

Consists of the various tools and policies employed to secure information:

- All administrative functions on RAMTeCH machines are controlled by our own IT department
- Secure network domain & login and password policy. All passwords are changed every 45 days
- User access control and rights authorized by CISO - No shared User ID's including System Administrators

- The CISO reviews user access rights on fortnight basis and System Admin ensures that all access permissions granted to the employees are removed when circumstances change, and all the permissions changed are recorded in the review of existing accounts logs
- Encrypted file and data transfer - Based on client requirements we will encrypt the data viz. PGP encryption AES 256 Bits and WinZip AES 128 Bits
- All data at rest or in transport is encrypted using AES with 128bit /256 bit/PGP encryption
- Controlled access with segregated and dedicated project areas, servers, workstations, & LAN's (exclusive as required)
- Restricted access and use of servers, data storage, and internet. No wireless LAN or Bluetooth
- Limited menu and submenu options for individual uses
- Limited or 'No' access to internet or personal emails
- Employees are not authorized to download or install any kind of software or applications
- Clear desk and screen policy
- All removable media and associated ports are disabled on all production systems
- Personal devices like cell phones, cameras, laptops, recorders are NOT allowed into client and project areas
- Secure email and FTP/SFTP servers
- Security and anti-virus software
- Periodic critical updates and security updates for servers and desktops
- Logging and audit of data changes
- All our Employees access the network within the secure office premises only
- RAMTeCH implements multifactor authentication (MFA) for the system administrator and select IT staff in order to access the servers for any kind administration or maintenance. System administrator gets a push or OTP notification to access the server
- RAMTeCH implements multifactor authentication (MFA) in order to access their email accounts. Email users are enabled with MFA authentication to access their emails. Users get a push or OTP notification to access their email.
- At RAMTeCH removable media drives are disabled (CD, USB, and Floppy drive etc.)
- Clock synchronization to all the clocks of desktops and security systems is enabled and verified periodically.
- The clocks of all relevant information processing systems within the organization or security domain are appropriately synchronized with Indian Standard Time (<http://www.indiaforum.org>) on every fortnight
- Critical and sensitive systems are isolated from the production network segments using subnet masks, VLAN etc.,

1.5 IT Security – Network Connections (Internet, Firewalls, Intrusion Detection)

Consists of tools and policies employed to manage secure external access to system and information:

- Limited internet access
 - Proxy server used for logging and monitoring
 - Authorized users are only given access to specific required sites or are allowed through VPN
- External connections and VPN
 - Primary production work done onsite - No remote access
 - External access for customers must be approved by CISO

- VPN is controlled using one-time password authentication – token device or a public or private key system with a strong pass phrase
- When actively connected to network, VPN will force all traffic over VPN tunnel – all other traffic will be dropped
- VPN users are automatically disconnected from the network after 30 minutes of inactivity
- Secure sFTP for delivery and data transfer
- Firewall and intrusion detection and protection
 - Hardware firewall to prevent and detect unauthorized intrusions
 - Networks are separated by subnet by project

We do have capability of implementing 2-factor authentication for both production/administrative access. Employees access the network from within the secure office premises only. We are using Duo and performing a 2-factor authentication for the users to access the machines assigned.

1.6 Physical Security

Consists of physical security measures that are implemented to safeguard personnel and prevent unauthorized access to critical assets, systems and information that reside in the office building:

- Compound walls and gates are used to restrict access to the facility for safety and security reasons
- 24 x 7 Security Guards, CCTV Surveillance (Client Specific)
- Three level security systems (Permanent ID check at main building entrance, Security check at premise entry and Access control with Face recognition reader at entry)
- Physical Security Perimeter- entire office space and building premises divided into various security zones
- Access into the facility is controlled via multiple access controls (Thumb impression, face recognition, employee swipe ID card and physical lock system). Only individuals with valid credentials can enter the office through turnstile at the main entry and through swipe cards assigned to certain client and project security zones
- Demarcation of project areas (Client Specific)
- All personnel, vendors, sub-contractors, and visitors are to display visitor passes within the facility
- All visitors, contractors, and vendors must register at the security their laptops, mobile phones, etc. before entering the facility
- Visitor sign-in and photo ID verification. Visitors must be accompanied by manager as well as “Visitor & House” logs are maintained
- Secured storage devices, controlled access to physical media
- Proper destruction and disposal of paper and electronic media
- Random exit search as well as security checks are performed to ensure compliance
- All areas (doors and windows) are locked when it is not in use
- At RAMTeCH office we do engage third party for data; hence no access is given to any third parties.
- Regular security drills are carried out, which essentially include training on fire fighting and inspection of the office premises
- The critical location like Server Room is fitted with smoke detector to raise an alarm in case of any smoke
- The manual alarm switches provided at different locations to notify the fire
- Appropriate fire-fighting equipment and other countermeasures provided and suitably located on site

All personnel within the facility are required to display their employee ID cards or visitor passes. Security guards are placed at the entrance of the office and blocks 24/7 and are required to check the employee IDs. All blocks have electronic access controls. Employee ID cards are used to authorize entry into these blocks. At a minimum, person entering the block, time in and time out are recorded and maintained. In case, a person from other cross-functional department wants to enter the block, he or she needs to identify himself by writing down his name, business purpose, time in and time out in the logbook placed with the security guard.



Security guards are used to protect the office and facilities. These third-party security guards are at the entrance of the facility and at each block. Each security guard will have to sign an NDA and a confidentially agreement.

1.7 Information Back-up and Disaster Recovery

Consists of processes and procedures for backing up and storing information:

- All Client data received backed-up “as-is” when received
- All Client data deliverables backed-up “as delivered” upon delivery
- Servers, storage, data directories backed-up daily, weekly, and monthly
- Secure, offsite storage for weekly and monthly backups
- Data storage is password protected
- Production data backed up automatically according to predetermined schedule



System and project data is backed up in accordance with industry procedures and standards. Daily, weekly, and monthly backup are taken at a specific time. These project backups are completed per the policy guidelines. The following retention period is applicable for the project backups.

Backup	Retention Period
Daily	1 Week
Weekly	1 Month
Monthly	1 Year

Project backup media are stored in fireproof safes within the facility. One key is kept with an authorized person in the office and the other at an offsite location (RAMTeCH Noida Office). The name of the authorized person and the key number are labelled on the safe. A detail logbook is maintained within the safe with the directory structure of files and backup.

An additional copy of the backup is kept at our RAMTeCH Noida Office. Only authorized personnel have access to these backups.

1.8 Privilege Management

At RAMTeCH, all data system users have a unique identifier ("User-ID") for their individual use only. Procedures for Defining, Identify and authenticating User IDs are:

- The employee code is assigned a User ID
- Users are assigned unique User IDs and have specific access rights
- All systems including PCs in the production area have a BIOS system level password to prevent anyone from changing the setup
- Only authorized users will be able to access the server after successful user authentication
- Allocation and use of access privileges are restricted and controlled based on the procedures detailed below:
 - Development of privilege profiles for each system based on intersection of user profiles and system resources
 - Granting of privileges based on these standard profiles
 - A formal authorization process from Chief information security officer (CISO) for any additional privileges
 - As per the password policy users are required to change their random and complex initial passwords at their first login
 - Store and transmit passwords in encrypted form only

The network/server access is provided for groups not for individuals. All the operators and technicians are grouped into users. Every technician is given access to his or her home directory. The Supervisory group is given access to all project-related specifications and source data along with Incoming and outgoing communications on a need's basis by the Project Manager.

RAMTeCH follows passwords, which have 15 characters minimum, and the complexity of the password include lower case, number, and a special character. As per the password policy, all passwords are changed every 45 days. Complex passwords should be maintained on the systems transmitting, processing, or storing any project data

While creating and using password, these are the Don'ts that needs to be taken care of:

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- Do not use the "Remember Password" feature of applications (e.g., Outlook, Messengers).
- Do not use the same password for RAMTeCH accounts as for other non-RAMTeCH access (e.g., personal ISP account etc.).
- Do not share RAMTeCH passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential RAMTeCH information.

Secure Log-in: To keep the data secure and confidential, the data or application is not displayed until successful log-on.

If the user login or password is input wrong, then login is rejected through validation procedure. Passwords are not transmitted in clear text. No display of passwords as entered (passwords are masked). In total only up to 5 unsuccessful logons are permitted.

If there is a suspicion of someone compromised the user account password, then change the password immediately. After resetting your password, report the incident to head/incident response team of Information Security.

1.9 Media Disposal

Disposal of assets shall be done based on the clearance taken from the asset owner. Clearance shall include that there is no confidential information in the system/asset/equipment or if such information exists, special tools shall be used for erasing the sensitive information. Shredders shall be used to destroy the documents that contain information that is confidential or internal in nature. After receiving confirmation from the concerned Project Manager, the disposal of Media will take place per the following methods:

- Obsolete optical media, such as CD-R, CD-RW, DVD-R, DVD-RW etc., are destroyed or defaced so that the data is unrecoverable.
- Printed material containing sensitive, data are destroyed in a safe and systematic manner, such as shredding or burning.
- Furthermore, disposal procedures recognize that records stored on electronic media, including tapes, and disk drives present unique disposal problems in that residual data can remain on the media after erasure. Since that data can be recovered, additional disposal techniques, such as multiple security wipes are to be applied to remove sensitive information.

1.10 Backup Media Disposal

The destruction of backup data will be carried out after the completion of contractual obligations including any warranty periods or 6 months whichever is earlier, as per the above-mentioned process. Necessary communication for confirmation will be sent to the client, after completion of time period.

1.11 Employee Separation (Exit Process for Leavers)/Role Change

When staff are off boarded at RAMTeCH we have a process to ensure that access privileges are immediately revoked for employees leaving the company for whatever reason or moving to a new job role internally. For all the employees who leave the organization, apart from the access rights removal including physical access, we communicate to the clients for removal of user access on the last day of their working. Proximity cards and system access are retrieved and decommissioned immediately.

Each employee that is off boarding must go through a thorough clearance process to obtain a clearance certificate. This is required in order to obtain clearance. This process includes returning of proximity cards.

When the employee notifies RAMTeCH of their last working day, the project manager notifies the customer that an employee will no longer require access their system and the date that this

will take effect, whether it is immediate or at a future date. This includes conditions when the work is completed, and the employee no longer has a need to retain access to the system

CISO in consultation with Information Security Forum shall oversee inclusion of appropriate security clauses and procedures in Job Change/Job termination procedures for suspect employees of RAMTeCH and ensure that appropriate and timely actions are taken so that internal controls and security are not impaired by such occurrences. The procedures will include but not limited to:

- Recovery of all documents, issued keys, borrowed IT equipment (e.g., laptops, data media) and company ID Card.
- Revoking/deleting of all entry and access rights held by the RAMTeCH staff. This includes external access authorizations over data communications equipment. If, in exceptional cases, several persons shared one access right to an IT system (e.g., by using a common password), the access rights are altered upon termination of employment by one of those individuals.
- It is explained explicitly to the departing person that all confidentiality agreements remain in force and that no information obtained in the course of his /her work may be disclosed and if need be, a separate undertaking is taken.
- Updating of contingency plans if the departing staff member was assigned functions under the plan.

Optionally, all entry and access rights relating to IT systems may be revoked even for the period from giving notice of termination to actual termination of employment, and in addition, the individual concerned may be prohibited from entering rooms requiring protection such as data center etc.

1.12 Incident Management

This policy is intended to develop, communicate, and implement formal methods and procedures for detecting and reporting incidents relating to exceptional situations in day-to-day administration of IT and information security related areas of RAMTeCH. RAMTeCH's network administrators will be monitoring for intrusion and security events. In case of any intrusion, it will be immediately brought to the notice of the Incident Response Team (henceforth referred to as IRT) or immediate Manager (who will alternatively inform the IRT). The IRT in turn will report to Chief Information Security Officer (CISO) for immediate action on the incident. Any incident will be categorized into various levels - high, medium & low. If the incident is categorized as high and impacting the business, it will be immediately communicated to the client. Since Inception, RAMTeCH did not have any security breaches.

- An incident may be detected by anybody in the organization. The concerned personnel shall immediately bring it to the notice of the Incident Response Team (henceforth referred to as IRT) or immediate Manager (who will alternatively inform the IRT).
- The IRT in turn will report to CISO of the incident.
- The incidents may also be reported to the CISO directly through email or verbal communication and in case of non-availability of CISO, the incident is escalated to Operations Head.
- The incident reporting forms are available at all security posts, and all the employees are made aware of the availability and its usage.
- 'Information Security Issue' once logged and assigned to a department may be modified and reassigned to another department.
- These 'Information Security Issue' logged can be read by the 'Incident Response Team (IRT)' member from the department to which it has been assigned AND the same forwarded to the CISO as required.

- The IRT member will do closure of 'Information Security Issue' from the department to which it has been assigned. If needed, the CISO can also close it.
- Basic statistics (number of Issues logged and closed, overall and by department) will be available for review by the CISO and all ISF members.
- Problems arising due to faults in EPABX systems, access control system not working, problems with access control cards, air conditioning not working & other kinds of physical & admin related Issues are reported to the admin department.
- Formal event reporting processes and procedures are in place, Actions to be taken and points of contact are defined. Issues/Problems are resolved as defined.

1.13 Antivirus policy

End-point security software is deployed across all Desktops, Servers, and Laptops with regular definition updates and scanning across servers, Desktops, and Laptop Computers to prevent from any kind of spyware/malware /virus/worms damaging RAMTeCH data and its client's data to check any other vulnerability.

SYSADMIN is responsible for deployment of anti-virus software and maintaining the Anti-virus system. All the desktops used by staff, Laptop computers and server computers connected to the network are up-to-date anti-virus product installed and running.

Antivirus activities are centrally managed. New viruses represent a continual threat, requiring continual research to plan proactive measures against them. It is the responsibility of SYSADMIN to install and update the anti-virus software on desktop computers in facility, laptops of RAMTeCH employees and on servers.

- Anti-virus software scanning engine and the virus pattern files are kept up to date. The time of updating the virus patterns is minimized. The latest virus definition files are automatically updated on all workstations & servers
- All computers of RAMTeCH including servers, desktops & laptops have standard and supported anti-virus software installed
- The virus scanners are scheduled to run to scan for viruses at every day at predefined schedule.
- Virus-infected computers are removed from the network as soon as they are identified, until they are verified as virus-free
- Any activities with the intention to create and/or distribute malicious programs into and from RAMTeCH networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited & protected
- Scans are performed on incoming and outgoing emails to avoid phishing etc.,
- The Host Intrusion Prevention component of End point security prevents applications from performing actions that may be dangerous for the operating system, and ensures control over access to operating system resources
- The Web Threat Protection component of End point security protects incoming and outgoing data that is sent to and from the computer over the HTTP and FTP protocols and checks URLs against the list of malicious or phishing web addresses
- The Web Threat Protection component of End point security intercepts every web page or file that is accessed by the user or an application via the HTTP or FTP protocol and analyses them for viruses and other threats

Firewall usage and controls in place to detect intrusions or unauthorized access to the IT environment

Network perimeter is protected by the deployment of a hardware firewall to prevent/detect malicious intrusions of unauthorized persons. In addition, a proxy server having built-in firewall is also installed for Internet access.

Access is restricted to limited sites on a need basis. Logs are maintained and periodically checked for any type of internal/external intrusions.

The servers are placed in locked racks, which in turn are kept in server room that is protected by proximity cards. Only authorized personal are allowed to enter the server room. Any unauthorized access can be checked from the logs for proximity cards.

Vulnerability Scanning: Vulnerability and Patch Management notifies IT administrators about the status of patch installation and enables them to run reports on scans, look for potential weak spots, track changes and gain extra insights into the organization's IT security as well as on every device and system across the corporate network. Information about existing exploits and known threats as well as CVEs (common vulnerabilities and exposures) are also available. Automated vulnerability scanning enables rapid vulnerability detection, prioritization, and remediation

Updates and patches for all the desktops and servers are downloaded and managed through End point security servers. All updates are cross verified during the monthly maintenance checks. Before distribution, these can be tested to ensure they won't impact on system performance.

Should a vulnerability event occur that may affect client data, RAMTeCH will notify the customer within 24 hours. The customer will be notified both by email and verbal communications. The process for the response is dependent on the security event.

At RAMTeCH we do have a formal process for identifying threats and vulnerabilities. Prevention is the first priority. Threats analysis and risk evaluations are carried out on a continuous basis. We have a hardware firewall at the perimeter level and any identified threats and vulnerabilities remediation to fix this is immediate. Since Inception, RAMTeCH has not had any security breaches. However, in the case of any incident we will notify the client within 24 hrs of time.

Should a vulnerability event occur that may affect client data, RAMTeCH will notify the customer within 24 hours. The customer will be notified both by email and verbal communications. The process for the response is dependent on the security event.

1.14 Business Continuity

Consists of formal processes and protocols for business continuity in case of event that disrupts normal business functions.

- Formal COB plan defined in ISMS policy
- Risk identification, impact analysis, and mitigation plans
- Emergency management team and call tree established

- COB site definition and activation including regular testing and live drills
- COB checklist, maps, contacts
- Business resumption plan
- Process measurements and ongoing COB process improvement to mitigate risks

Protecting Against External & Environmental Threats: Emergency procedures describe how to respond to an environmental disaster situation and other problems, which may result in the declaration of a disaster and activation of the recovery plan. The procedures described in this document are applicable to all personnel and the entire infrastructure of RAMTeCH. The Facility layouts are as follows on floor wise and the respective HOD's are responsible to implement the procedures in their corresponding areas:

- Production Department
- Administration and Infrastructure Support Department
- Accounts Department
- Human Resources Department

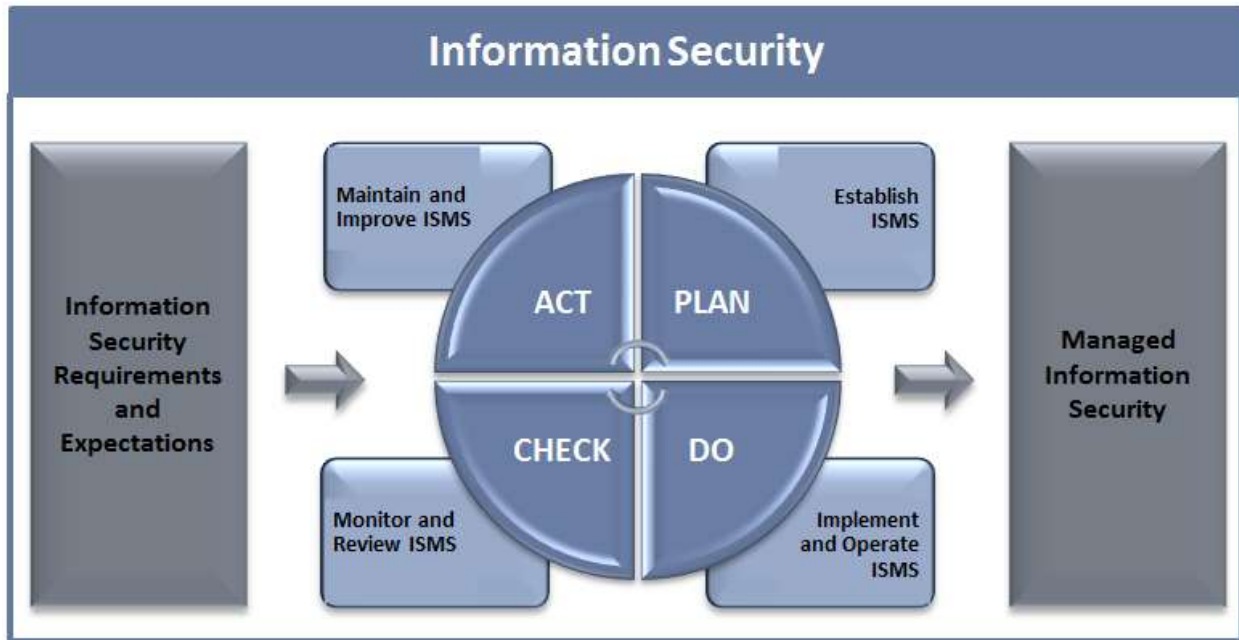
1.15 System Audit and Logging Policy

Auditing is done for all critical servers & networking equipment of RAMTeCH. Their events are logged for failure of events. Logging is the process of storing information about events that occurred on the system, firewall or network. All the logs shall be retained for a minimum period of one month or till the date they are reviewed and assessed. The retaining period vary from system to system depending on the criticality of the system. To minimize the risk of security threats we configure critical operating parameters such as password policy, access control etc. Monthly all the systems are checked for any non-permitted software installation.

Establishing an audit trail is an important facet of security. Monitoring the creation or modification of objects gives a way to track potential security problems, helps assure user accountability, and provides evidence in the event of a security breach.

1.16 Client Information Security

The following review model has been adopted by RAMTeCH to ensure a continued process of on-going improvement to the Information Security policies and protocols.



Measures Relating to Client Information Security

Management is continually aware of and has taken responsibility for the security aspects of its clients' information. Security organization and resources deployed reflect this commitment.

- Prevention is the first priority. Threats analysis and risk evaluations are carried out on a continuous basis
- Preparedness is essential to mitigate incidents rapidly and effectively. Response plans are developed and tested to deal with assessed risks
- Security measures and procedures are submitted for regular inspections, validations, and verifications by security specialists (internal and external) help in maintaining high levels of security standards at RAMTeCH
- The level of professionalism, knowledge and integrity of staff involved in security matters on behalf of RAMTeCH are tightly controlled and are commendable according to the BSI ISO certification agency. Appropriate training plans, recruitment and contracting procedures are established and implemented
- Any incidents, including security breaches and irregularities would be reported and recorded. Corrective actions taken are followed up through regular verifications to improve the overall security standard
- Strategic focus and effort are put into making our Security Management System (ISMS) at a continual improvement process

1.17 Operational Change Management

Changes to information processing facilities and systems are controlled using appropriate change management procedures.

- Risk assessments, including an analysis of potential impacts and necessary countermeasures or mitigation procedures
- Processes for planning and testing of changes, including fallback (abort/recovery) measures

- Managerial approval and authorization before proceeding with changes that may have a significant impact on operations
- Advance communication/warning of changes, including schedules and a description of reasonably anticipated effects, provided to all relevant persons
- Documentation of changes made and the prior steps in the change management process
- Change Control process includes a scheduled maintenance window and planned well ahead and communicated to users before the implantation

Changes to routine system operations are tested and approved before implementation.

1.18 Risk Assessment Approach and Management

Risk management is a process that ensures company to balance the operational and economic costs of protective measures to achieve gains in mission capability by protecting the Information system and data that support their organization's missions. It is the total process of managing risks to Company operations, Company assets, or individuals resulting from the operation of an information system. It includes risk assessment and Cost-Benefit Analysis (CBA) as well as the selection, implementation, testing, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including the impact on the mission and constraints due to policy, regulations, and laws.

As a preliminary risk assessment, Team Leaders/System Owners ensure that all systems and data under their purview have been categorized in accordance with Risk Assessment, Standards for the Security Categorization of Information Assets

Risk assessment is carried out as per the standard policies defined and established within the company. All assets are identified and evaluated based on the principles of the ISMS requirements. Risk assessment is carried out in accordance with the guidelines of ISO 27001:2013. However, these guidelines are further simplified in a manner suitable in all manners to RAMTeCH.

The risk identification is done based on the business requirements and infrastructure support it requires to run the business 24X7. The local legal framework and internal laws and data security requirements, geo physical locations are the major characterizes in listing the risk including natural calamity and disaster.

The assets are identified and evaluated for risk based on the requirements of confidentiality, integrity, or availability of the information of these assets and or services.

RAMTeCH systems face threats from many sources, including the actions of RAMTeCH employees, external users, and contractor personnel. The intentional and unintentional actions of these individuals can potentially harm or disrupt RAMTeCH systems and their facilities. These actions can result in the destruction or modification of the data being processed, Denial of Service (don'ts) to the end users, and unauthorized disclosure of data, potentially jeopardizing RAMTeCH mission. Therefore, it is highly important that stringent safeguards be taken to reduce the risk associated with these types of threats.

General physical access controls restrict the entry and exit of personnel from a protected area, such as an office building, Server Room, or room containing Information assets/IT equipment. They include the protection of sensitive data and systems while in rest, as well as while away from the protection of company facilities. These controls protect against threats associated with the physical environment. It is important to review the effectiveness of general physical access controls in each area during business

hours and at other times. Effectiveness depends not only on the characteristics of the controls used but also on their implementation and operation.

The risk impact level is evaluated, and appropriate treatment plan are applied. The approval of management is taken for treatment as well as residual risk.

Treatment of Risk and Control Objective: Treatment and Controls are exercised based on the documented policy of risk treatment plan requirements depending on system sensitivity in accordance with procedure. Wherever required the assets may be insured as a treatment option or passed on the supplier. Such assets are clearly identified and documented.

Security Policies

Following is the list of relevant cyber security policies:

1. RAMTeCH ISMS Manual
2. Asset Management Policy
3. Acceptable Use Policy
4. HR Security & Training Policy
5. Physical Security Policy
6. Communication & Operations Security Policy
7. Backup Policy
8. Network Security Policy
9. Access Control Policy
10. Incident Management Policy
11. Antivirus Policy
12. Information Systems Acquisitions, Development & Maintenance Policy
13. Systems Audit Policy
14. Business Continuity Policy
15. Supplier Relationships
16. Patch Management
17. Pandemic Policy
18. Teleworking Policy

External Review: or Audit

RAMTeCH has undergone client review audits in past by our client for specific security requirements for the project. RAMTeCH has no history of any security breaches.

RAMTeCH staff sign an appropriate confidentiality undertaking as part of their initial conditions of employment. This may be included in a Code of Ethics and acceptable use policy Agreement that establishes the principles of conduct that all employees are expected to observe. RAMTeCH admits its willingness for company to evaluate security capabilities. RAMTeCH conducts regular audits to monitor compliance with the security policy.

1. It is the approach of "RAMTeCH" that all aspects of the "RAMTeCH" Information Security Management System (ISMS) are subject to an internal audit at least twice in every year. This helps ensure that not only policies and procedures are being applied but that new best practice can be gathered and applied

2. To establish, document and implement a program for the periodic internal audits at planned intervals to determine effectiveness of the Information Security management system. This feedback is used for control and improvement in organizational working
3. Audits are undertaken as a means of determining how effectively the Information Security systems are implemented and maintained
4. It verifies the compliance of the requirements of this international standard and to the documented Information Security management system
5. The Team Leader responsible for the area being audited ensures that actions are taken without undue delay to eliminate detected non-conformities and their causes. Follow-up activities include the verification of the actions taken and the reporting of verification results
6. Documented procedure for planning and implementing internal audits are maintained
7. The frequency of the audit is twice in a year, which may be increased, based on the status and importance of the activity. The audit covers all processes of the organization
8. Trained personnel, who are independent of those having direct responsibility for the activity being audited, carry out audits. Internal audits can also be conducted by an external agency
9. The documented procedures for internal audits are maintained

SECTION 2 – ISO CERTIFICATES



Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that:

Ramtech Software Solutions Pvt. Ltd.
3rd Floor, Usha Kiran Complex
1-8-167 to 179/C 141
S.D. Road
Secunderabad 500 003
Telangana
India

Holds Certificate No:

IS 542033

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

The Information Management system covering GIS, Engineering Services, KPO/ BPO, Software Development and support functions as per SOA Version 7.0 dated 3rd Aug 2023.

For and on behalf of BSI:

Theuns Kotze, Managing Director Assurance - IMETA

Original Registration Date: 2008-10-17

Effective Date: 2023-09-17

Latest Revision Date: 2023-09-12

Expiry Date: 2025-10-31



Page: 1 of 2

...making excellence a habit.™

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.

An electronic certificate can be authenticated [online](https://www.bsi-global.com/ClientDirectory).

Printed copies can be validated at www.bsi-global.com/ClientDirectory or telephone +91 11 2692 9000.

Further clarifications regarding the scope of this certificate and the applicability of ISO/IEC 27001:2013 requirements may be obtained by consulting the organization.

This certificate is valid only if provided original copies are in complete set.

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.



MANAGEMENT SYSTEM CERTIFICATE

Certificate no.:
149115-2014-AQ-IND-RvA

Initial certification date:
17 February 1999

Valid:
17 February 2023 – 16 February 2026

This is to certify that the management system of
Ramtech Corporation
A-6, Sector-67, Noida - 201309, Uttar Pradesh, India

has been found to conform to the Quality Management System standard:
ISO 9001:2015

This certificate is valid for the following scope:
Software development, geospatial data conversion & back office services

Place and date:
Chennai, 03 February 2023

For the issuing office:
DNV - Business Assurance
ROMA, No. 10, GST Road, Alandur, Chennai -
600 016, India



Sivadasan Madiyath
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.
ACCREDITED UNIT: DNV Business Assurance B.V., Zwolsseweg 1, 2994 LB, Barendrecht, Netherlands - TEL: +31(0)102922659. www.dnv.com/assurance

SECTION 3 – CYBER INSURANCE CERTIFICATE

Client#: 95724 RAMTSOF

ACORD **CERTIFICATE OF LIABILITY INSURANCE** DATE (MM/DD/YYYY) 3/07/2025

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer any rights to the certificate holder in lieu of such endorsement(s).

PRODUCER CBIZ Insurance Services, Inc. 222 S 9th St. STE 1000 Minneapolis, MN 55402 763 549-2200	CONTACT Name: Stephanie Schmitz Phone: 763 549-2204 Email: SSchmitz@CBIZ.com
INSURED RAMTeCH Software Solutions, Inc. 6203 Osgood Ave. N. Ste 200 Stillwater, MN 55082	INSURER'S AFFIRMED COVERAGE INSURER A: Travelers Property Casualty Co of Amerl 25674 INSURER B: Associated Industries Insurance Co, Inc 23140 INSURER C: Travelers Indemnity Company of Connect 25682 INSURER D: INSURER E: INSURER F:

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

ALTA	TYPE OF INSURANCE	MODEL NO.	FORM NO.	POLICY NUMBER	POLICY EFF. DATE (MM/DD/YYYY)	POLICY EXP. DATE (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> OTHER: _____ CIVIL AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PER <input type="checkbox"/> LOC <input type="checkbox"/> OTHER: _____			ZPP61M7274325IS	01/15/2025	01/15/2026	EACH OCCURRENCE: \$1,000,000 DAMAGE TO IMPROVEMENTS (Per occurrence): \$1,000,000 MED EXP (Any one person): \$10,000 PERSONAL & ADV INJURY: \$1,000,000 FEDERAL AGGREGATE: \$2,000,000 PRODUCTS - COMPROP AGG: \$2,000,000 OTHER: \$
C	AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTO ONLY <input checked="" type="checkbox"/> NON-OWNED AUTO ONLY <input type="checkbox"/> OTHER: _____			BA1L84271025ISG	01/15/2025	01/15/2026	LIABILITY - BODILY INJURY: \$1,000,000 BODILY INJURY (Per person): \$ BODILY INJURY (Per accident): \$ PROPERTY DAMAGE (Per accident): \$ OTHER: \$
A	<input checked="" type="checkbox"/> UMBRELLA LIAB <input type="checkbox"/> EXCESS LIAB <input checked="" type="checkbox"/> RETENTION: \$10,000			CUP8MM4402925IS	01/15/2025	01/15/2026	EACH OCCURRENCE: \$5,000,000 AGGREGATE: \$5,000,000 OTHER: \$
	WORKERS COMPENSATION AND EMPLOYER LIABILITY ANY EMPLOYER/EMPLOYEE GROUP/IF OFFICER/MEMBER EXCLUDED (Mandatory in MN) If yes, describe under EXCLUSIONS OR CONDITIONS below						<input type="checkbox"/> EXCLUDE <input type="checkbox"/> INCLUDE EL EACH ACCIDENT: \$ EL DISEASE - PER EMPLOYEE: \$ EL DISEASE - POLICY LIMIT: \$
A	Cyber/Professionals			ZPL41M7174A25IS	01/15/2025	01/15/2026	\$5,000,000/\$5,000,000
B	XS Cyber			ACL124237401	01/15/2025	01/15/2026	\$5,000,000

DESCRIPTION OF OPERATIONS/ LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

CERTIFICATE HOLDER **CANCELLATION**

Proof of Insurance

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE: Mark A. Smith

© 1998-2015 ACORD CORPORATION. All rights reserved.

ACORD 25 (03/16/03) 1 of 1 The ACORD name and logo are registered marks of ACORD
#544761971M4356395

ORLM