GST No. 07AACCR8458C1ZB
MSME Reg. No.: DL01E0011477

RASCO Automotive Systems Private Limited
*Formerly, **Radiator Supply Company**, Established 1953*
135 LGF World Trade Centre Barakhamba Lane Delhi – 110 001
***T:**+91-(0)11-3001-0141*
***E:** info@rascoindia.com **W:** www.rascoindia.com*

RASCO'S INFORMATION SECURITY POLICY

Confidential / Internal Use Only

1. Introduction

1.1. Purpose & Objective.

This document defines RASCO Automotive Systems Private Limited's position on information security. RASCO Automotive Systems Private Limited ("**Company**") is a private limited company incorporated under the Companies Act 1956 and existing under Companies Act 2013 having its registered office at 135, LGF, World Trade Centre, New Delhi-110001, India. The Policy is applicable across the Company and is also subject to amendment at any time depending upon the changes in business requirements or environment with requisite approvals.

The objective of this Policy is to describe the security requirements for information assets belonging to the Company and used across the Company. These assets can be in written, spoken or computer-based form and the protection and security of these assets from unauthorised disclosure, misrepresentation, loss or wrongful use is of vital importance. Management and staff must ensure the Confidentiality, Integrity and Availability of all information assets, as required.

The terms confidentiality, integrity and availability are defined as follows:

a) **Confidentiality.** Ensuring that the RASCO's information is protected from unauthorised disclosure or use.

b) **Integrity**. Ensuring that information held on information systems is not subject to malicious or accidental alteration and that systems and processes function correctly and reliably.

c) **Availability.** Ensuring that information systems are always available to authorized users when needed.

1.2. Applicability and Scope.

This Policy applies to all employees. The employees include:

a) Permanent RASCO employees, both full-time and part-time.

b) Contingent workers or contractors whether hired directly by RASCO or via a third-party agency.

c) Agents, Officers, and Directors of RASCO.

1.3. **Importance of the Policy to all employees.**

Every person working on behalf of RASCO is responsible for security of the information assets. All employees play a vital role in implementing controls and processes needed to help manage access to, and use of, RASCO and RASCO customer's information assets.

1.4. **Owner.**

The Chief Information Security Officer (CISO) is the owner of this Policy and will be responsible for reviewing and updating the Policy as and when required based on the change in the business requirements or environment. The CISO will also ensure that the updated Policy is implemented across the Company.

2. Organisational of Information Security.

The objective of this clause is to manage the information security within the organisation.

2.1. Internal Organisation. The organisation of information security will be enforced by:

a) Establishing a management framework to initiate and control the implementation of information security within the organisation.

b) Ensuring that a governance framework is developed to maintain information security within the organisation; and

c) Assigning the security roles and coordinating the implementation of security across the organisation.

2.2. Management Commitment to Information Security. The roles and responsibilities of Senior Management will include:

a) Periodic review of information security at Company;

b) Review of security incident monitoring processes within the Company;

c) Approval and review of information security projects;

d) Approval of new or modified information security policies;

e) Performing other necessary high-level information security management activities;

f) Ensuring that there is clear direction and visible management support for security initiatives in place; and

g) Promoting security through appropriate commitment and adequate resourcing.

2.3. Roles and Responsibilities

Board of Directors/ Audit Committee	The Board has delegated day-to-day risk management to executive management, who has delegated authority and responsibility for managing the Information Security of the Company to the Chief Information Security Officer (CISO). Risk Management is overseen by the Risk Management Committee.
Chief Information Security Officer	The CISO establishes, implements, maintains, and enforces the Company's

	Policy to manage the protection of resources against accidental or unauthorised modification, destruction or disclosure through the development and implementation of information security policies, procedures and technical security solutions
System Administrator	A superuser/privileged user with a level of access above that of a normal user, or with supervisory responsibility for Information Systems, Network and Information Resources.
Employees and Staff	Security is a foundational element throughout the Company; it is everyone's responsibility to promote this Policy through their role in Company. All employee's working within the Company environment have responsibilities which are summarized in Clause 6, 7, 8 and 9. These include but are not limited to: • Maintaining confidentiality of your passwords; • Protecting Company issued equipment; • Escalating potential access or physical security concerns to Information Security. • Ensuring that access to sensitive data is done in accordance with record retention and disposal policies; and • Understanding the risk assessment process and when to engage Information Security.

2.4. Confidentiality.

2.4.1. Employees will sign agreement highlighting confidentiality requirements as part of their initial terms and conditions of employment.

2.4.2. Without specific written exceptions, all programs and documentation generated by, or provided by any employee for the benefit of the Company are the property of the Company and all employees providing such programs or documentation will sign a statement to this effect prior to the provision of these materials.

2.4.3. Whenever communications with third parties necessitate the release of the Company's sensitive information, a standard Non-Disclosure Agreement (NDA) or confidentiality clause, authorised by the Company's legal department, will be signed by the third party.

3. Human Resource Security.

The objective of this Clause is to ensure that users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

3.1. Prior to employment.

3.1.1. Roles and responsibilities. Users will fulfil all security roles and responsibilities as laid down in this Policy.

3.1.2. Screening.

a) Background screening, as required for the role, on permanent staff will be carried out at the time of job applications.

b) Information systems technical details, such as network addresses, network diagrams, and security software employed, will not be revealed to job applicants until they have been hired and have signed a confidentiality agreement.

c) Persons who have a criminal conviction will not be hired into, retained for, promoted into, or maintained in computer-related positions of trust.

3.1.3. Terms and conditions of employment.

a) The terms and conditions of employment will include the employee's responsibilities for information security as laid down by the Policy.

b) Employees of the Company will grant the Company exclusive rights to patents, copyrights, inventions, or other intellectual property they originate or develop.

3.2. During employment.

3.2.1. Management responsibilities.

a) Management will require employees, contractors and third-party users to apply security in accordance with Company's established policies.

b) Senior Management will ensure that information security within their departments is treated as mandatory and employees are encouraged to adhere to Company's information security policies.

c) Information security awareness, education, and training**.**

d) All employees of the organisation and, where relevant, third-party users will receive appropriate training and regular updates in organisation policies and procedures.

3.3. Termination or change of employment.

3.3.1. Human Resources will notify IT department and all other stakeholders (from support and business functions) about the transfer or termination of any employee and any other third-party personnel or contractors of the organisation without delay.

3.3.2. Unless the IT department has received instructions to the contrary, within 30 days after an employee has permanently left the Company, all files held in that user's directories will be purged unless reporting manager needs that data.

3.3.3. The system user IDs will be disabled for a period of one month after an employee has permanently left the Company.

3.3.4. Removal of access rights.

System privileges and access to information and information assets to an employee will be removed within 72 working hours after receiving mail from personnel department.

4. Physical and Environmental Security.

The objective of this Clause is to prevent unauthorised physical access, damage, and interference to the organisation's premises and information.

4.1. Secure areas.

4.1.1. Physical security perimeter.

a) All single-user computer and communications equipment will be located in a room with adequate access control mechanism installed e.g. keypad or a proximity cards access.

b) Every Company single-user computer and communications facilities will have a physical security plan that is reviewed and updated annually by the executive management.

4.1.2. Physical entry controls.

a) Access to every office, computer room, and work area containing sensitive information will be physically restricted to limit access to authorised personnel only.

b) Employees will not permit unknown or unauthorised persons to pass through doors, gates, and other entrances to restricted areas at the same time when they go through these entrances.

c) Visitor or other third-party access to Company offices, computer facilities, and other work areas containing sensitive information will be controlled by guards, receptionists, or other staff. Further, physical security controls like CCTV, Biometric entry shall be in place.

d) Single-user computer and communications facilities (including telephone closets, network router and hub rooms, voice mail system rooms, and similar areas containing computer and / or communications equipment) will be kept locked at all times and not be accessible by visitors without an authorised IT staff escort to monitor all work being performed. There shall be no wireless connections.

4.1.3. Equipment maintenance.

a) Preventative maintenance will be regularly performed on all computer and communications systems.

b) All information systems equipment used for production processing will be maintained in accordance with the supplier's recommended service intervals and specifications, with any repairs and servicing performed only by qualified and authorised maintenance personnel.

c) All hardware and software products will be registered with the appropriate vendors for maintenance, after Company staff takes delivery of new or upgraded information systems products.

d) The Annual Maintenance Contracts for all hardware and software products, if applicable, will be monitored and reviewed after every six months.

4.1.4. Security of equipment off-premises.

a) Any use of equipment for information processing outside company premises will require authorisation by management. Authorisation for issue of mobile computing devices (laptops) will be considered as an authorisation for use of equipment for information processing outside Company premises.

b) Employees will store mobile phones and other hardware sensibly and securely when storing outside Company's premises e.g. hotels, airports. Equipment will not be left unlocked, logged in or powered up without the employee being with the equipment.

4.1.5. Secure disposal or re-use of equipment**.**

a) Information will be erased from equipment prior to disposal or re-use.

b) Equipment will be disposed in an environmentally sensitive manner, taking account of any recycling facilities provided by manufacturers, local authorities or commercial organisations.

5. Asset Management.

The objective of this Clause is to achieve and manage appropriate protection of Company assets.

5.1. Inventory of Assets.

5.1.1. Information assets at the Company will be classified based on the impact on the organisation, due to loss of their confidentiality, availability and integrity.

5.1.2. An inventory of all critical information assets will be drawn up and maintained to ensure appropriate protection of Company's information assets. The asset inventory will include all information necessary in order to recover from a disaster, including type of asset, backup information, license information, security classification and business value.

5.1.3. An owner will be identified for each of the information assets at the Company. The owner will be responsible for:

a) Ensuring that information and assets associated with information processing facilities are appropriately classified; and

b) Defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies.

5.2. Information classification.

5.2.1. Information assets of the organisation will be classified based on their relative business value, legal requirements and impact due to loss of confidentiality, availability and integrity of the information asset.

5.2.2. The level of security will be identified based on the information classification performed.

5.2.3. Assets shall be grouped under the following asset types:

a) Physical assets;
b) Software assets;
c) Information assets;
d) Services assets; and
e) People assets.

5.2.4. The information assets will be classified in the following four categories:

a) Restricted: Information that is highly sensitive and is available only to specific, named individuals (or specific positions).

b) Confidential: Information that is sensitive within the Company/Business and available only to a specific function, group or role.

c) Internal: Information that is sensitive outside the Company/Business and needs to be protected. Authorised Access to employees, contractors, sub-contractors and agents on a "Need to Know Basis" for business related purposes.

d) Public: Public Information (including information deemed public by legislation or through a policy of routine disclosure), available to the Public, all employees, contractors, sub-contractors and agents.

e) If information is not marked with one of these categories, it will default into the “Internal” category.

5.3. Information labelling and handling. The owner or creator of information will assign an appropriate label to the information, and the user or recipient of this information will consistently maintain an assigned label.

5.4. All employees will have a personal responsibility for safeguarding all proprietary information, which includes but is not restricted to sensitive documents and information, from disclosure to unauthorised parties.

5.5. No usage of physical drives. The usage of physical drives like CD/DVD ROMs, USB drives or external hard drives, SD Cards, etc. in all ports are disabled by the Company.

5.6. Procedure in case of theft of Company Assets.

5.6.1. If Company asset is stolen, users will immediately notify the police or security as well as IT department/ administration department and give them specific information to identify the device/asset.

5.7. Procedure in case of disposal of business sensitive information.

5.7.1. The Company shall not retain/store/preserve the business sensitive information of the client after the delivery of the end product to the client. Any business information/deliverables/ end product delivered to the client will be destroyed/deleted from the information system of the Company immediately after the confirmation of receipt of the same by the client. In case, the Client wishes the Company to retain/store preserve the data/information for the client in the information system of the Company, the client shall provide an express request for the same to the Company. Upon such approval of request by the Company, the Company shall charge such basic fee/amount for storing/preserving such information of the client as per the terms and policies of the Company.

5.7.2. Records of disposal, including time of destruction, name of person who destroyed it and means of disposal will be maintained.

5.7.3. Procedures will be defined to identify items that might require secure disposal.

5.7.4. In cases where contractors are used for collection and disposal services for paper, equipment, etc. care will be taken while selecting a suitable contractor with sufficient experience and which complies with this Policy.

6. Network Security.

6.1. Do obtain approval from System Administrator prior to monitoring and scanning devices.

6.2. **Don't:**

6.2.1. Connect personally owned devices (such as laptops, routers, or switches) to the Company network.

6.2.2. Use port or security scanning.

6.2.3. Execute any form of network monitoring, unless this activity is a part of your job duties.

6.2.4. Circumvent user authentication of any host, network or account.

6.2.5. Use any program, or send messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means.

6.2.6. Allow business sensitive data to reside in a non-production environment. Data used for testing must be removed from production environments prior to the system being used in a production capacity, other than customer testing.

6.2.7. Intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate or to damage or otherwise hinder the performance or access to any information resource, or negligently allow the same to occur.

6.2.8. Copy data that is protected by copyright using Company equipment.

7. Access Control.

Every user/employee will be provided with his/her own computer system of the Company. The user shall be obliged to sign a legally binding ownership agreement, whereby the user is/will be responsible for the data in the information/computer system along with the security of the data. Further, each user/employee will have a unique user account with a User ID and password to access the said computer system. Users will be responsible for setting their passwords and ensuring that their password is protected. Further, no administrative privileges will be granted to the users. Each employee of the Company will login as a standard user with limited/restricted rights based on their work profile as allocated by the Management. The administrative privilege rights of the computer/information systems of the Company shall be under the control of the System Administrator.

7.1. **Do:**

7.1.1. Be responsible for all activity performed under your user account.

7.1.2. Ensure, with your superior, only the appropriate minimum privileges are granted and are in-line with your role and responsibilities.

7.1.3. Ensure your Company credentials are protected at all times.

7.2. **Don't:**

7.2.1. Access data, a server or an account for any purpose other than conducting Company business, even if you have authorised access.

7.2.2. Reveal or share your account password or other credentials to others or allow use of your account by others under any circumstances. This includes family and other household members.

7.2.3. Provide access to another individual, including family members, either deliberately or through failure to secure your access.

7.2.4. Write your password and/or PIN on paper, store in a document, reuse on other systems or websites, or send in an email.

7.2.5. Share Passwords or personal identification number (PIN) with others under any circumstances.

7.2.6. Store Passwords in an unsecured manner (e.g., written on paper, stored in a spreadsheet or other document, etc.)

7.2.7. Utilize a USB devices for reading or writing purposes without manager approval and written approval from line manager.

8. Internet Usage.

8.1. **Do:**

8.1.1. Be accountable for all Internet activity carried out under your user account.

8.1.2. Access the Internet only for business purposes during business hours.

8.1.3. Implement a duty of discretion, confidentiality and ethics when communicating on social networks.

8.2. **Don't:**

8.2.1. Cause any action on the Internet which is illegal and cause harm to Company or other parties.

8.2.2. Visit any website or download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity including gambling, gaming, or hacking.

8.2.3. Discuss Company business on the Internet and social media networks or give the impression that you are acting in any official capacity on behalf Company unless it is specifically allowed in your employment contract or job description.

8.2.4. Use Company username or password to register and visit any non-Company Internet site.

8.2.5. Install or store files downloaded from the Internet until they have been scanned for viruses or other malicious functionality.

8.2.6. Disable or remove security software that has been installed by Company including but not limited to antivirus, patch management, and encryption software.

8.2.7. Install any type of peer-to-peer file sharing software.

8.3. **Use of E-mails and Electronic Storage.**

8.3.1. The Company official email cannot be accessed via web browser. Only email client installed in computer systems can be used to access emails. All web-based email portals like, Gmail, outlook, Yahoo, etc. shall remain inaccessible. Detailed email log is maintained to view email interactions of all employees.

8.3.2. **Do:**

8.3.3. Be aware that individual monitoring of e-mails and electronic storage may occur based on a valid legal ground, including for business continuity, security purposes, compliance and human resources investigations, or other legal purposes such as litigation, regulatory inquiry and other legal proceedings, in accordance with applicable laws and regulations.

8.3.4. Be vigilant of common security risks to avoid phishing, visiting potentially malicious websites, installing malware or fall victim to social engineering.

Reputable organisations will not ask you to run software or click on a link to verify your password.

8.3.5. Rely on your personal e-mail account for sending personal e-mails than on your professional e-mail account.

8.3.6. Ensure business sensitive data sent via email is always encrypted. To encrypt an outbound message containing business sensitive data, click the "Send Securely" button with the "New Memo" window in Outlook.

8.3.7. Report suspicious email to System Administrator by using the report phishing button.

8.4. **Don't:**

8.4.1. Use your system/workstation or other Company-issued devices, regardless of your location, to:

a) Send any business sensitive data to a personal email account;

b) Send business sensitive data to another Company staff member's personal email address, even if he or she indicates they don't have access to their work email account.

c) Automatically forward any Company email to a personal email account.

8.4.2. Open a link or attachment from an unknown sender.

8.4.3. Click on links, open up documents, run programs, or go to web pages supplied by an unexpected suspicious source email, or phone request by an unknown source.

8.4.4. Send data classified as Highly Confidential—Special Handling unencrypted via e-mail over public networks.

8.4.5. Use the auto-forward feature to send an email from an email system approved by Company to an email account not created by Company.

8.4.6. Forward, reply, or reply to all from an unexpected suspicious email, or phone request by an unknown source.

9. Workspace Security.

9.1. **Do:**

9.1.1. Securely store all work-related items and lock all cabinets containing work-related items outside business hours, unless such cabinets are located in a locked office.

9.1.2. Remove any work-related items or any item that could be considered work related, from workspaces outside of normal working hours.

9.1.3. Remove documents from unattended fax machines, photocopiers, and printers.

9.1.4. Lock computer access by using the Windows password-protected screensaver feature at any time that the computer is turned on but not actively in use.

9.1.5. Obtain approval from your management and notify Physical Security before you remove any Company-owned equipment or software from Company facility.

9.1.6. If you are working from outside a Company facility (e.g., telework or touchdown workspaces) you must additionally:

a) Ensure that remote access from outside a Company facility will not result in additional security risks to Company information resources.

b) Confirm with management whether any of the work-related items intended to be used off-site can be removed from Company premises.

c) Completely remove all information resources before the telework or touchdown workspace is used by a different individual or group.

9.2. **Don't:**

9.2.1. Leave work-related items unattended at any point in time (during or outside normal working hours) unless securely stored.

9.2.2. Leave laptop computers, etc. unattended outside normal working hours, unless located in a locked office.

9.2.3. Install Software that has not been approved by Asset Management on your workstation.

9.2.4. Disable or remove security software that has been installed by Company.

10. Security Operations.

10.1. File Transfer Protocol (FTP) & Cloud Data Share Platform.

10.1.1. Configuration. The FTP and Cloud Data Share Platform currently implemented by the Company is ZOHO Workdrive, the security details of which may be updated from time to time and can be located at: https://www.zoho.com/workdrive/security.html.

10.1.2. Industry Standard Data Security. The ZOHO Workdrive as per their representations meet industry-specific compliance standards such as SOC 2 Type II and ISO 27001. It uses a defence-in-depth approach to provide security at the physical, logical, and data levels.

10.1.3. Encryption in transit and at rest. As per the representations of the ZOHO Workdrive, the data/information is encrypted at rest with 256-bit Advance Encryption Standard (AES). During transit, Perfect Forward Secrecy (PFS) generates a unique key for each session to encrypt files.

10.1.4. Disaster recovery. As per the representations of the ZOHO Workdrive, their servers are well protected from all kinds of physical damage. The servers run on distributed grid architecture. In case of server damage, a copy of the files will be safely backed up in an alternate server and available without any noticeable delay.

10.1.5. Intrusion protection. As per the representations of the ZOHO Workdrive, All files are first checked for viruses before being uploaded and stored in Zoho servers. The screening uses powerful Intrusion Detection and Intrusion Prevention systems (IDS/IPS) and systems are secured from DDoS attacks.

10.1.6. Two-factor authentication. As per the representations of the ZOHO Workdrive, the WorkDrive account is protected with a Two-Factor Authentication (TFA). To ensure strong protection, user gets a unique code generated every time he/she logs into an account.

10.1.7. Shared links that expire and can limit downloads. Data shared is available only for as long as it is wanted to be. Expiration dates can be set on documents while sharing them externally. After the expiration date, external parties will not be able to view the data. Download limits can be set, so the data would be available for download only the number of times as set by the user.

10.1.8. Data Transmission.

a) External. All data shared clients, vendor or external parties is via secure FTP Cloud Solution, Zoho Workkdrive.

b) Internal. All data transmitted internally is shared via FTP Cloudshare solution deployed at Company, Zoho Workdrive. Teams/employees work on this cloud platform to collaboratively create and edit data. Company emails carry attachments up to 5MB Data only.

10.2. Anti-Virus and Malware Protection.

10.2.1. Antivirus software has been installed on all computers and servers. Virus update patterns are updated daily on the servers and workstations. Virus update engines and data files are monitored by the System Administrator.

10.2.2. Configuration. The antivirus software currently implemented by the Company is AVAST Small Office Protection the details of which can be accessed at: https://www.avast.com/en-in/business/products/small-office-protection. Following are the features of the said software:

a) Multi-OS support: Advanced endpoint security for employees in the office or on the go. Covers multiple devices, including PCs, Mac computers, iPads, iPhone, and Android mobile devices.

b) Ransomware Shield: Prevents ransomware from harming files in protected folders.
c) Remote Access Shield: Blocks unwanted remote connections to prevent Remote Desktop Protocol (RDP) exploits and brute-force attacks.
d) Next-gen AV: Blocks virus, spyware, and malware in real time.
e) Web Shield: Checks URLs and certificates to ensure they are safe before a network connection is made.
f) Email Shield: Continuously checks incoming and outgoing emails to ensure they are malware-free.
g) File Shield: Scans files, URLs, and email attachments to prevent malware, ransomware, and more.
h) Wi-Fi Inspector: Finds and fixes weaknesses in the network that might be putting PC at risk.
i) Real-Site: Keeps employees away from fake sites designed to steal the data.
j) Sandbox: A safe environment to test dubious programs and files, safely separated from the rest of the PC.
k) Advanced Firewall: A customizable firewall that filters network traffic and stops untrusted connections.
l) Sensitive Data Shield: Stops spyware from accessing sensitive documents on the computer.
m) Webcam Shield: Stops webcam spying. Apps will ask for permission before webcam is turned on.
n) Data Shredder: Permanently delete confidential files that contain financial or customer data Company doesn't want recovered.
o) Software Updater: Updates the most popular apps on the PC to help plug security holes.
p) Do not disturb mode: Silences notifications from Windows and other applications.
q) Real-time Updates: Notifies of any security updates for the best protection.
r) Phishing Net: Uses cloud database to protect business from even the newest phishing sites.

10.2.3. Monitoring/Reporting. A record of virus patterns for all workstations and servers on the network are maintained. System Administrator is responsible for providing reports for auditing and emergency situations as requested by the CISO.

10.2.4. User Responsibility. Upon encountering a virus attack, users will immediately stop using the involved desktop/laptop and/ or any other computer system and report it to System Administrator within 24 hours from the knowledge of the virus attack. The users will not attempt to destroy or remove a virus, or any evidence of that virus, without directions from the IT department.

10.2.5. IT Department Responsibility.

a) Ensure all servers, desktops and laptops are installed with company standard Anti-Virus and Malware Protection Program. Proper password protection settings are available so that the Anti-Virus check cannot be disabled by the users;

b) Provide newer versions/ engines of Anti-Virus programs in regular and timely manner and ensure a quick roll-out across the organisation;

c) Ensure all Servers and PCs are updated with latest versions of the Anti-Virus and Malware Protection Program; and

d) Ensure Anti-Virus software run at least once in a week and are properly scheduled.

11. Business Continuity Management.

11.1. The objective of this clause is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

11.2. Information security aspects of business continuity management.

11.2.1. Including information security in the business continuity management process.

a) Business process owners will be responsible for ensuring that the key events that can cause disruption to their processes are identified and their potential adverse impact, financial & non-financial, is documented.

b) The scope of the business continuity plan will take into account applicable factors including customer requirements and legal regulations. The following will be considered while implementing any business continuity plan program:

(i) Identify critical business functions, applications and supporting technologies;

(ii) Develop an appropriate cost-effective recovery strategy;

(iii) Identify alternate, backup locations with the necessary infrastructure to support the recovery needs;

(iv) Identify the management and membership of the disaster response and recovery teams;

(v) Identify and document the required recovery actions, identify and ensure the availability of required resources, and compile this information as the recovery plan;

(vi) Train the recovery teams in the performance of their specific tasks;

(vii) Identify vendor recovery support capability;

(viii) Identify data protection and data recoverability status;

(ix) Identify functional team, recovery support and response capabilities; and

(x) Develop an ongoing testing and maintenance program to ensure that all processes are in a constant state of recovery readiness.

11.2.2. Business continuity and risk assessment. A strategy plan, based on appropriate risk assessment, will be developed for the overall approach to business continuity. Key considerations in such a plan will be:

a) Identify events that cause interruptions to business processes; and

b) Consider all critical business processes, not just information processing facilities.

11.2.3. Developing and implementing continuity plans including information security.

a) All departments will establish and use a logical framework for classifying all information resources by recovery priority that will permit the most critical information resources to be recovered first.

b) All departments will prepare, periodically update and regularly test the business recovery plan that specifies how alternative facilities will be provided so employees can continue operations in the event of a business interruption.

11.2.4. Business continuity planning framework. A single framework of business continuity plans will be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance.

11.2.5. Testing, maintaining and re-assessing business continuity plans.

a) If critical business activities could reasonably be performed with manual procedures rather than computers, a manual computer contingency plan will be developed, tested, periodically updated, and integrated into computer and communication system contingency plans.

b) Company Management will annually revise and document the support levels that will be provided in the event of a disaster or emergency.

c) Computer and communication system contingency plans will be routinely tested and followed up with a brief report to top management detailing the results.

d) Each calendar quarter, emergency contact information will be validated and revised indicating for every employee involved in business continuity and disaster recovery planning and implementation.

e) The roles and responsibilities for both information systems contingency planning and information systems recovery will be reviewed and updated annually.

12. Risk Assessment and Management Process.

All critical information assets should be risk assessed annually (as a minimum) using Company's Risk Assessment and Management framework. Each risk assessment should be clearly scoped and seek to identify, quantify and prioritize the information risks to the Company's business functions. Consideration should also be given to information risks that may affect Company's business partners.

12.1. Risk Analysis.

12.1.1. Risk analysis should be in accordance with Company's Risk Management Procedure and should be completed on the Risk Management template. Risk assessment steps should include as a minimum:

a) Location and source of risk;
b) Description of the risk;
c) Details of controls in place to manage risk;
d) Initial and residual risk scores;
e) Details of the actions required to manage the risk;
f) Individual responsible for overall management of the risk;
g) Details of any resources required to manage the risk; and
h) Timescales for risk review.

12.1.2. Risk assessors should include the following information asset threats in their review:

a) Physical damage;
b) Natural events;
c) Loss of essential services;
d) Compromise of information;
e) Technical failures;
f) Unauthorised actions; and
g) Compromised functions.

12.1.3. Approval of Risk Assessments.

All completed risk assessments and action plans should be sent to the executive management for review.

13. Security Audits.

13.1. Internal Security Audits.

13.1.1. Internal Audit department will conduct audit for license compliance every 12 months.

13.1.2. Internal Audit management must perform an annual review and random tests of production computer system backup processes.

13.1.3. Internal Audit will review the adequacy of information system controls and compliance with such controls annually.

13.1.4. Internal Audit will conduct annual compliance checks related to this information security policy.

13.1.5. Audits of operational systems will be planned with due care and agreed upon by the business owner to minimize the risk of disruptions to business processes.

13.1.6. Programming source code and its related technical analyses used to compromise security will be disclosed only to authorised personnel with a justifiable business requirement.

13.1.7. All information assets directly connected to the Internet must be subjected to periodic risk assessment performed.

13.1.8. Management will conduct review of whole Information Security System on annual basis. This kind of review will be based on various reports including Incident reports, internal audit reports and quarterly review reports.

14. Key Policy Information.

14.1. Monitoring, Reporting & Escalation.

Information Security follows formal procedures in compliance with applicable local laws and regulations for the investigation of security and policy violations. Information Security documents all investigative findings. If a violation is determined to have occurred, employees will be treated in accordance with defined HR procedures. Consequences may include disciplinary action, which may lead to termination. The Human Resources (HR) should be consulted in all cases where formal disciplinary action is necessary. Compliance with local law and Company policy and procedures must be reflected in disciplinary proceedings.

14.2. When computer security breaches or other wrongful acts are suspected, such acts must be reported immediately in the following manner:

14.2.1. **Step 1:** For urgent requests, immediately call the CISO at **+91-11-2341-1356**. For non-urgent requests, email **IT.SECURITY@RASCOGB.COM**.

14.2.2. **Step 2:** Provide as much detail about the incident as possible.

14.2.3. **Step 3**: If in doubt about whether to report an incident, please inform the CISO as a precaution.

14.3. Over the course of the investigation, Information Security may consult the HR Department, the Law Department, and outside law enforcement entities. Any contact with law enforcement agencies is managed by Information Security in conjunction with the Human Resources and Law Departments.

14.4. For further guidance regarding this Policy, please contact CISO at +91-11-2341-1356.

15. Security Training and Awareness

15.1. The Company assigns Information Security responsibility for the creation and management of security education, training, and threat awareness programs. The program's content must be evaluated for relevance, quality effectiveness, ensuring

and measuring retention of knowledge, cost, and value. The results of evaluation will serve as input for future curriculum and training sessions.

15.2. Security training and awareness delivers a mix of mandatory and voluntary trainings, programs, and events. Content will address security concerns most relevant at the time and may therefore change each year. Mandatory or formal awareness trainings include but are not limited to the following:

15.2.1. Annual Information Security Awareness Training provided to employees and staff. The training will equip staff with knowledge of Information Security requirements, consisting of its policy, directives, and controls.

15.2.2. A dedicated New Hire Security Training module that provides a glimpse into "day in the life" scenarios and how they interact with Information Security protocols.

16. Compliance

All employees are responsible for ensuring compliance with this Policy. In accordance with this violation of the policies in this document, whether done intentionally, negligently, or accidentally may result in disciplinary action up to and including termination. Lack of knowledge will not be deemed an excuse.