Radhakrishna Finance Private Limited
Information Technology Policy

Radhakrishna Finance Private Limited come under Section-B category of asset size below 500 crores. The Information Technology Policy is designed considering the basic standards mentioned in RBI Master Direction-Information Technology Framework for NBFC sector. It also includes the main policies and sub policies given below.

Using this policy

One of the challenges facing organizations today is enabling employees to work productively while also ensuring the security of the IT network and crucial part is the data on it. Given that technology is continually changing, employees play a significant role in IT security. This policy provides a framework for users to follow when accessing IT systems and the data on them. It is intended to act as a guideline for organization looking to implement or update their own Acceptable Use Policy.

Sl. No.	Policies	Policy No.
1	Physical/ Logical Access Control Policy	ITP-001
2	Password Policy	ITP-002
3	A Well-Defined User Role	ITP-003
4	Maker Checker Concept	ITP-004
5	Information Security Policy	ITP-005
6	Cyber security Policy	ITP-006
7	Electronic channel security Policy for Mobile Financial Services, Social Media & Digital Signature Certificates	ITP-007
8	System Generated MIS Reports	ITP-008
9	System Generated COSMOS Returns	ITP-009
10	Business Continuity Planning Policy	ITP-010
11	Data Backups and Retention Policy	ITP-011
12	E-mail Usage and Retention Policy	ITP-012

Sl .No.	Policy Name	Policy No	Effective Date
1	**Physical/ Logical Access Control Policy**	ITP-001	1st April 2021

Purpose

The objective of this Access Control Policy is to provide access to information processing facilities and information assets of organization only for authorized purposes and to establish individual accountability.

Scope

This policy applies to any entity (person) and the access credentials (such as user accounts) with access to the information processing facilities and information assets.

Policy

The access control policy has been segregated into two parts namely Physical Access Control and Logical Access Control.

Physical Access Control

1. Physical access to all information processing facilities shall be protected by access control systems such as biometric systems, access card etc.
2. Where locks with keys are used, procedures for secure management of the keys must be in place.
3. Records from access control systems must be kept secure and archived.
4. Access to the specific areas (such as data centre, backup storage locations etc.) requires approval from the IT Department. Additional physical access control measures shall be implemented to restrict the access to the selected personnel.
5. All users who have physical access to the information processing facilities shall wear visible identity cards.
6. Access cards, passes, keys or other tokens must be retrieved from staff or contract staff when their employment or contract ceases.
7. Access passes shall be provided to visitors & vendors while entering the premises and should be retrieved on leaving the premises.
8. All physical access must be logged and made available for review when required.

Logical Access Control

Access to the IT components and data is generally known as logical access. In other terms, any access to the Information processing systems should be considered as logical access. Logical access should be based on the principles of Authentication, Authorization and Accountability

Logical access

1. Access to the IT infrastructure which includes, but not limited to, network devices, network VPN services, operating systems, applications, databases, data files should be granted on the basis of business needs.
2. Access should be allowed on the basis of positive identification and positive authorization.
3. Any access to information systems should be denied by default and access permissions are built, step by step, on a need-to-know basis or on the concept of least privileges.

4. Adequate segregation of duties or separation of privileges within systems should be incorporated. This will ensure that authority is not focused on a single individual.

User Authorization

1. All access requests to data and systems must be formally authorized. Access must be given only on a need-to-know basis.
2. Any access requested by a contractor, temporary staff, or third parties must be authorized by IT Sr. Manager and must be for a limited period, with a defined end date and time. Such access must be promptly disabled

User Access Modifications

1. Access must be modified as required when employees move internally within organization or on vacation for more than 15 days
2. The IT Systems Manager shall have the authority to disable accounts without reference if necessary and notify IT Department.
3. Transfer of user accounts or using other employee user credentials to login is also not permitted.

User Access Review

1. All user access privileges must be recorded and reviewed annually. IT Systems Manager shall coordinate with other departments to perform this review
2. The access rights of all user accounts must be on a need-to-know basis.
3. All user activities should be logged and should be made available for review when required

Administrator Access Modifications

1. Whenever a System, Application and/or Network Administrator leave the team/department, steps must be taken to change all the administrative passwords of organization information systems which are under the custody of the staff. This should include, but not limited to, the passwords of routers, switches, firewalls, servers, databases and service accounts.

Local Administrator Access

1. Local Administrator access to workstations shall be granted only when there is a requirement. This elevated privilege shall be granted based on the approval from the IT Department and will only be valid for a limited period of time.

Temporary Accounts

1. Third parties, Temporary staff or staff filling a temporary role shall not use an existing user's identification.

2. The temporary account that is released for use must be for a limited period with a predefined end date and time.

Third party access

1. Access granted to third parties, which includes but not limited to vendors, contractors, external auditors, etc should have the supporting business documents which clearly justify the business needs.
2. Third party access must be for a limited period with a predefined end date and time.

Termination of Access

1. The Employees' Manager ensures that all such user accounts to access ended.
2. Any client user accounts used by the employee should be disabled or the account password should be changed.
3. Codes or passwords for systems, equipment access passwords (routers and switches), administrator passwords, and other common access control information should be changed when appropriate.
4. IT System Managers should be informed by the Human Resources department when employee resignation / termination processed.

Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action, up to termination of employment.

Sl. No.	Policy Name	Policy No	Effective Date
2	**Password Policy**	ITP-002	1st April 2021

Purpose

The purpose of this policy is to provide the guidelines necessary for all of the employees of the Radhakrishna Finance Private Limited users to create appropriate passwords and to use them and protect them in an appropriate manner.

Scope

The policy applies to all Radhakrishna Finance Private Limited computers and devices that store company information. It applies to all users of the organization's network, using any device that has access to the network.

Policy

All company-owned workstations and servers must be protected using a user ID and strong password combination. Passwords are used for user accounts, servers, data base, e-mail accounts, network devices, Web & Mobile applications, Firewall devices, Wi-Fi devices, etc. Users of any company-owned systems that require a password must follow the guidelines below for creating passwords:

1. Passwords for typical user accounts should be at least eight characters in length; administrative passwords should be at least 15 characters in length.
2. A password cannot be a word or phrase that can be found in any dictionary or a word spelled backwards.
3. It should contain at least one upper case letter, one non-alpha character and at least one special character (e.g. @#$%^&).
4. Must not be a common pattern found on a standard keyboard or any other common pattern of letters or numbers.
5. It should not be based on personal information such as birthdays, addresses, names, etc.

It is important to protect the secrecy of passwords. The following guidelines must be followed when handling passwords:

1. Passwords can never be written down anywhere that is not under lock and key (no sticky notes!).
2. All user account passwords must be changed every 180 days and cannot be reused. All administrative passwords must be changed every three months.
3. Password can never be included in e-mails or other form of electronic communications.
4. Users must have different passwords for each system that does not use some method of single sign on.

5. Never reveal your password to anyone over the phone, including help desk personnel.
6. Do not share your passwords with assistants, co-workers, family members, or friends. All passwords must be treated as company confidential.
7. Do not use the ''Remember Password'' feature of any application.
8. Do not store your passwords in any portable electronic device such as tablets or cell phones.

Any exceptions to this policy must be approved in advance by the company IT department.

Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action, up to termination of employment.

Sl. No.	Policy Name	Policy No	Effective Date
3	**A Well Defined User Role**	ITP-003	1st April 2021

Purpose

The objective of this User Role Policy is to define individual user role of organization.

Scope

This policy applies to all individuals under organization with access to the information processing facilities and information assets.

Policy

A Well-Defined User Role

Individuals who have been granted access to specific information assets in the performance of their assigned duties are considered Authorized Users. Users will get access to data only through the authorization and access control process. Access only that data which s/he has a need to know to carry out job responsibilities. Disseminate data to others only when authorized by the concerned departments under the organization.

User Registration and Deregistration

1. Every staff, customer and third party, requiring access to the IT infrastructure, standalone systems and applications must have a unique user ID and a personal secret password. This user ID and password will be required to establish positive identification and authentication.
2. Human Resources department is required to inform the IT Department with up-to-date and relevant personnel details to ensure that the appropriate security controls are implemented in light of this information
3. Unique user IDs assigned so that access and modifications can be traced.
4. The user who gains access to the system / application should read and understand the Information Security policy and related policies before the logical access are granted. Non- compliance with the policies will result in disciplinary action, which is dependent on the nature and severity of the transgression.
5. The user registration should be approved by the IT Sr. Manager after reviewing the business need for the access of the requesting user.

6. The user should be deregistered or disabled when the access is no more needed.

User identification and Authentication

1. Users are accountable for all activities performed with their personal user IDs. User IDs shall not be utilized by anyone other than the individuals to whom they have been issued except for super administrator accounts.
2. All systems that connect to the IT infrastructure must make use of proper access controls that prohibit access to resources without proper authentication procedures
3. Every authentication process for computers connected to the IT infrastructure must (wherever possible) include a notice warning against unauthorized use and consequences thereof.

Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action, up to termination of employment.

Sl. No.	Policy Name	Policy No	Effective Date
4	**Maker Checker Concept**	ITP-004	1st April 2021

Maker-checker is one of the central principles of authorization in the information systems of Radhakrishna Finance Private Limited. The principle of Maker and Checker means that for each transaction, there must be at least two individuals necessary for its completion. While one individual may create a transaction, the other individual should be involved in confirmation/authorization of the same.

There is every possibility of a mistake creeping in a transaction, if a single person handles the entire process of the transaction in the system. The Maker& Checker is a procedure followed in all major financial institutions to do away with such accidental / procedural mistakes created. This ensures that the transaction is done with four eyes principle and the person in charge who is answerable to the functions of the branch/HO as the approving authority, is part of the sanction process of the loans and other transactions in the system.

The important points of the Maker-Checker are mentioned below for deeper understanding and effective functioning.

1. The Maker is the person who enters the transaction in the computer system. He / She enters all the relevant details in the Software Module. Once entered, it is submitted for approval of the Checker.

2. The Checker is the person in charge who has to verify the details of the transaction entered by the maker logging in his / her login ID. He/ She should go through the details of the transactions entered by the maker and verify the same. Once satisfied, Checker can approve the transaction. If the Checker feel that the transaction cannot be approved for any reasons then, the Checker can reject the transaction.

3. Once approved by the Checker, the maker can go for the printing of the documents and complete the transaction.

4. Approval matrix is created based on the amount of the transaction in the application software. Branch level and HO level approvals are required to complete the transaction categorized in different hierarchy levels.

5. In case the Maker/Checker is on leave for the day or absent for short periods then he/she have to approach their reporting authority who will allot the powers of the Checker to another person, who is the in charge in the absence of the Maker/Checker. The reporting authority should take care to re allot the role of the Maker/Checker to the person of the branch/HO once the staff resumes for duty.

6. If the branch level authority cannot do this process due to leave or absent for short periods meeting etc., this can be done by the authorized HO official. This needs a prior intimation to HO official to do the change/ allotment of the Maker/Checker.

Sl. No.	Policy Name	Policy No	Effective Date
5	**Information Security Policy**	ITP-005	1st April 2021

Purpose

This policy establishes the integral foundation for security standards, processes and procedures of Information Security that will be followed by the organization

Scope

The policy applies to all users of information technology within the company. Policy also applies to all data assets of the organization which includes,

1. Intellectual property owned by company or provided by a third party.
2. Personally Identifiable Information for employees, clients or other third parties.
3. Financial and business information of the company, its employees, clients or other third parties.
4. All Public or Private data or information assets of the company.

Policy

The IT Department must establish and provide governance for information technology policies, procedures, and best practices for the company's technology infrastructure in order to secure all IT assets and promote the most efficient use of technology resources.
The IT Department will submit a report to the Board of Directors at its monthly meeting of each calendar year, and submit interim reports at the request of the Board, on the current status of the company's technology policies and procedures.
Data Protection Mechanism:
All privileged data information will be protected by data protection mechanisms to ensure the highest levels of confidentiality, integrity and availability. Non-privileged information will be protected to ensure the highest levels of integrity and availability. Information systems will check entered information for accuracy, completeness, validity and authenticity. Information systems will be configured such that they prevent unauthorized and unintended information transfer.

Responsibilities of IT Department:

1. Determine appropriate security policy requirements based on its business objectives,
2. Assessment of risk, and interpretation of legal, regulatory and contractual obligations
3. Validate that the security controls meet the company requirements driven by security policy and risk acceptance
4. Notify security requirements of changes through a change request process
5. Facilitating training for improving better IT Security controls
6. Request exceptions to the documented information security controls, as necessary

All operating units within the company that use information technology (IT) are responsible for:

1. Adhering to the IT policies issued by the IT Department.

2. Developing and implementing, when appropriate, additional IT policies and procedures specific to their operating units.
3. Promoting IT policy adherence.
4. Complying with the requirements of the IT governance model adopted by the organization.
5. Ensuring the security of the IT systems and the network to which they are connected.
6. Informing the IT Department if there are any problems with a policy or if inputs from other sources do not comply with the defined policies.
7. Providing an annual "refresher" for current employees highlighting the changes made or problem areas during the previous year.
8. Maintaining the functionality of the IT systems within their area.
9. Facilitating training and the dissemination of information.
10. Preventing unauthorized access to company information, personal files and e-mail.
11. Developing and maintaining a plan for recovery of mission critical data and systems if a loss is sustained.

Sl. No.	Policy Name	Policy No	Effective Date
6	**Cybersecurity Policy**	ITP-006	1st April 2021

Purpose

Objective of the Cyber Security Policy is to preserve confidentiality, integrity and availability of organizations information or system in the Cyberspace (internet) or connected to cyberspace. Cyberspace is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it". The purpose of this policy are to ensure the appropriate and inappropriate use of company internet resources, including the use of browsers, electronic mail, instant messaging, file upload and downloads and voice communications etc.

Scope

Is to protect organization, its information assets and its stake holders from cyber-attacks or internet bone attacks. All devices, systems connected to internet and all stakeholders in the scope.

Policy

1. IT Department must ensure:
    a. Cyber security roles and responsibilities are defined, coordinated and aligned with internal roles and external partners
    b. Must establish a cyber-security Framework which enable to identify, protect and detect, respond and recovery from Cyber-attacks.
    c. The organization's place in its own industry ie NBFC sector is identified and communicated to all stakeholders
    d. Dependencies and critical functions for delivery of critical services are established
    e. Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)
    f. Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders
    g. Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed
    h. Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cyber security program
    i. Response and recovery planning and testing are conducted with suppliers and third-party providers
    j. Establish Computer Emergency Response Teams (CERT) and establish practices for sharing risk-related information (e.g., threat and vulnerability information) with external

entities, including those with which the organizations have a risk relationship as well as those which could supply or receive risk-related information (Other CERTs)

k. The organization's personnel and partners are provided cyber security awareness education and are trained to perform their cyber security-related duties and responsibilities consistent with related policies, procedures, and agreements.

2. Technical Controls
    a. File Integrity checking mechanisms are used to verify software, firmware, and information integrity
    b. A baseline configuration of IT system is created and maintained incorporating security principles
    c. A vulnerability management system is implemented
    d. Mechanisms (eg. failsafe, load balancing, hot swap, DOS/DDOS protection) are implemented to achieve resilience requirements in normal and adverse situations
    e. Establish SOC and baseline of network operations and expected data flows for users and systems is established and managed. The network is monitored to detect potential cyber security events
    f. Event data are collected and correlated from multiple sources and sensors
    g. Physical environment and Personnel activity are monitored to detect potential cyber security events
    h. Setup Security Continuous Monitoring for unauthorized mobile code and malicious code detection
3. Incident Response
    a. Response processes and procedures are executed and maintained, to ensure response to detected cyber security incidents and Response plan is executed during or after an incident
    b. Voluntary information sharing occurs with external stakeholders to achieve broader cyber security situational awareness
    c. Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
    d. Analysis is conducted to ensure effective response and support recovery activities
    e. Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. Newly identified vulnerabilities are mitigated or documented as accepted risks
    f. Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities
4. Recovery

a. Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cyber security incidents
b. Recovery planning and processes are improved by incorporating lessons learned into future activities
c. Restoration activities are coordinated with internal and external parties (e.g. coordinating centres, Internet Service Providers, owners of attacking systems, victims, and vendors)

Sl. No.	Policy Name	Policy No	Effective Date
7	**Electronic channel security Policy for Mobile Financial Services, Social Media & Digital Signature Certificates**	ITP-007	1st April 2021

Purpose

The organization is committed to ensuring compliance to all requirements including legal, regulatory, organizational policies and ensures any changes in the security measures to enhance e-channel security must be carried out in a controlled manner with appropriate records maintained.

Scope

All electronic channel-based assets which are owned or leased or outsourced.

Policy

1. Implement adequate security measures on the internal networks and network connections to public network or remote parties. Segregate internal networks into different segments having regard to the access control needed for the data stored in, or systems connected to, each segment
2. Maintain access security logs and audit trails. These should be analysed for suspicious traffic and/or intrusion attempts
3. Passwords shall be encrypted when stored on the databases and should not be readable when decrypted and should also be one way hashed
4. All connections to the Applications must go through firewalls
5. Conduct regular audit to assess the adequacy and effectiveness of the risk management process and the attendant controls and security measures.
6. Perform vulnerability test or assessment to evaluate the information security policies, internal controls and procedures, as well as system and network security
7. Conduct penetration testing at least annually
8. Any High value transection and transfer of critical information must protect by strong digital signatures.
9. Implement “end-to-end” Secure Sockets Layer (SSL) encryption that is appropriate to the sensitivity and importance of data to protect confidentiality of information while it is stored or in

passage over external and internal networks. TLS – recent versions secured encryption algorithm should be used.

10. Any communication occurring in a Social Media must be respectful to the company, fellow employees, our affiliates, and our business partners.
11. The company may request at any time that you cease any communication concerning the company in Social Media or require you to block access to such communication if the company believes that such action is necessary to ensure compliance with government regulations or other laws.

Sl. No.	Policy Name	Policy No	Effective Date
8	**System Generated MIS Reports**	ITP-008	1st April 2021

Purpose

The purpose of MIS is reporting and is to provide the necessary information to the managers and supervisors at various levels to help them to discharge their functions of organising, planning, control and decision making are no more relevant and useful in the process of decision making.

Scope

Provide support and maintenance to existing management information systems (MIS). Generate and distribute management reports in accurate and timely manner. Develops MIS documentation to allow for smooth operations and easy system maintenance.

Policy

1. Collect the exact requirement from the concerned department.
2. Ensure that all departments are fulfil the decision-making capacity.
3. Easy to understand.

Sl. No.	Policy Name	Policy No	Effective Date
9	**System Generated COSMOS Returns**	ITP-009	31-Aug-18

Purpose

To know the extent of participation of NBFCs in Interest rate Future market. ... Concerned NBFCs are required to file the specified returns online through COSMOS application.

Scope

Cosmos is Microsoft's internal data storage/query system for analysing enormous amounts (as in petabytes) of data. ... The Scope article in particular provides an architectural overview of the system and breaks Cosmos into three parts: Storage, Execution Management and Query Language

Policy

1. Collect the exact requirement from the concerned department.
2. Ensure that all departments are fulfil the decision-making capacity.
3. Easy to understand.

Sl. No.	Policy Name	Policy No	Effective Date
10	**Business Continuity Planning Policy**	ITP-010	1st April 2021

Purpose

The purpose of this policy is to create and maintain a Business Continuity Plan (BCP) for the IT support of critical company processes. An effective plan allows the company to minimize the adverse effect of emergencies that arise. The Company has an ethical obligation to the organization's workforce, shareholders, and customer stakeholders to protect the continuing operations of the business.

Scope

This policy encompasses all IT processes and technology that supports critical business functions.

Policy

The IT Department is responsible for creating, maintaining, and testing the IT Business Continuity Plan. The following activities must be performed:

Identify Critical Processes.

To identify the business processes critical to the company's financial and legal well-being, a bi-annual Business Impact Analysis (BIA) is conducted. The result is a Recovery Time Objective—that point at which company losses become intolerable (Recovery Time Objective—RTO). The IT Business Recovery Plan must ensure that critical IT processes (equipment and software) can be recovered at a remote site within the RTO.
The IT Department initiates and submit the BIA. The BIA will:

1. Encompass all departments and areas of the company.
2. Identify the point in time that the financial and legal issues seriously threaten the company's survival.
3. Identify the processes required to meet all regulatory requirements.
4. Include a risk assessment of natural and man-made risks to the critical processes.

Business Continuity Planning.

The IT Department will assemble plans for every identified critical business function.

1. Develop the plan.

a. Develop plans for the recovery IT processes, equipment, and software for all critical business processes identified by the BIA. These plans must address steps necessary to re-establish the IT functions at an emergency recovery location.

b. Based on the BIA, publish a restoration priority list of all critical technologies.

c. Create an emergency notification program to ensure the prompt notification of executive management in a crisis

2. Maintain the plan.
   a. Test all IT Business Continuity Plans at least bi-annually to demonstrate the ability to achieve the BIA determined Recovery Time Objective. Conduct a lessons-learned session with all participants to capture and incorporate improvements into the plans.
   b. Report all test results to the management by IT Department within 30 days of the test's completion.
3. Training.
   a. Train all members of the IT department in their roles in supporting the BCP.
   b. Train all new employees on their roles within 30 days of joining the department

Coordinate with other company disaster plans. The IT manager will coordinate the IT BCP with:

1. The Facilities Disaster Recovery plan and the Security/Safety department's crisis plan.
2. The various business recovery plans of other departments.

Sl. No.	Policy Name	Policy No	Effective Date
11	**Data Backups and Retention Policy**	ITP-011	1st April 2021

Purpose

This policy guides the frequency and type of data backups. It also addresses the length of time that backups must be retained.

Scope

The policy applies to all devices that hold or accumulate data in the support of critical company operations, to include servers, business applications, data base, surveillance systems, access controls, voice logger, Firewall devices, Telecommunications switches, PCs etc.

Policy

The IT Department is responsible for making and retaining an adequate number of data backup "safety" copies. To accomplish this, the IT Department may create further policies and procedures and delegate authority to implement them.

Devices

Data backups will be made of all devices that contain or collect data, to include at a minimum:

1. Servers and their internal disks
2. Storage Area Networks
3. Telecommunications switches (PBX)
4. surveillance systems
5. Desktop /Laptop PCs
6. Firewall

Types of Data

1. Personal data is not to be stored on company equipment.

2. Legal compliance data—must be identified. The label on the backup media must include what data it contains and the appropriate retention period. Care must be taken to ensure the data is securely stored.
3. Business critical data—must be identified. The label on the backup media must include what data it contains and the appropriate retention period. Quick access to this data is required in the event of a disaster.

4. Non-critical data—must be identified. Non-critical data is not legally required to be retained for a period of time. Typically this data is deleted after 13 months. The label on the backup media must include what data it contains and the appropriate retention period.

Data Backup Frequency

The frequency of data backups is determined by how frequently and how much a data storage element change.

1. Full backups weekly—all data is backed up weekly and retained for 12 months.
2. Incremental backups daily for changing data. These are retained for 30 days.
3. Off-site journaling is used for immediate backup of critical data that cannot be reconstructed from daily backups.

Data Retention

The organization retention period is determined by the data element with the longest required retention period on that backup media. If the contents of the media are not known, then the media must be retained for a minimum of seven years.

Off-site Storage

1. Data backups will be transported off site every week after the backups are created.
2. Once every calendar quarter, the IT Department will audit the off-site storage process to ensure that:
    a. Media is kept in a climate-controlled environment during transit.
    b. The storage facility is secure and fire proof.
    c. The storage facility is climate controlled.
    d. The data centre security is appropriate for media going out and for media coming in.
    e. There is a documented chain of custody for backup media from the point it leaves the data centre until it is returned.

Data Destruction

Data that has outlived its usefulness to the business, and whose age exceeds the legal limits for retention, must be properly destroyed.

1. The media must be rendered permanently unreadable. This is primarily accomplished through physical destruction. Paper documents are shredded, burned, and the ashes pulped. CDs and magnetic media are shredded.
2. When data is destroyed, it must be documented as to whom, by what means, when, and what the data consisted of data.

Sl. No.	Policy Name	Policy No	Effective Date
12	**E-mail Usage and Retention Policy**	ITP-012	1st April 2021

Purpose

This policy defines the acceptable use of the company's corporate e-mail system. The objectives of this policy are to outline appropriate and inappropriate use of Radhakrishna Finance Private Limited's e-mail systems and services in order to minimize disruptions to services and activities, as well as comply with applicable policies and laws.

Scope

The policy applies to all uses of company owned e-mail accounts and all company e-mail records.

Policy

Acceptable Uses of Company E-mail Accounts

The company provides e-mail accounts for business usage only. Every staff member has the responsibility to maintain and enhance the company's public image and to use the company's e-mail system in a responsible and productive manner that reflects well on the company.

Unacceptable Uses of Company E-mail Accounts

Company e-mail accounts may not be used for transmitting, retrieving, viewing, or storage of any communications of a discriminatory or harassing nature or materials that are obscene. Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual's race, age,

disability, religion, national origin, physical attributes, or sexual preference shall be transmitted. No excessively abusive, profane, or offensive language is to be transmitted through the company's e-mail system. E-mail messages or attachments may also not be used for any purpose that is illegal or against company policy or contrary to the company's best interests. Solicitation of non-company business, or any use of the company e-mail system for personal gain, is prohibited.

Communications

Each employee is responsible for the content of all text, audio, or images that he or she places or sends over the company's e-mail system. All e-mails must contain the identity of the sender and may not represent the sender as someone else or someone from another company.

Any messages or information sent by an employee to another individual outside the company via an electronic network (e.g., blog, IM, bulletin board, online service, or Internet) are statements that reflect on the company. While some users include personal "disclaimers" in electronic messages, there is still a connection to the company, and the statements may legally be tied to the company. Therefore, we require that all communications sent by employees via the company's e-mail system comply with all company policies and not disclose any confidential or proprietary company information.

Privacy

E-mails are not private. The company reserves the right to monitor e-mail content ensuring that the e-mail system is used for appropriate purposes. Also, no security is hundred percent hacker-proof; someone outside the company may intercept and read e-mail. Routing of e-mail is not without errors; someone other than the intended recipient may receive the e-mail. Do not send anything by e-mail that should not be placed on the company bulletin board.

Personal E-mail Accounts

Accessing personal e-mail accounts is prohibited from company-owned computers, as they are a potential source of computer viruses. No company-related communication is permitted using personal e-mail accounts, as the communication may be subject to the company's communication retention policy.

Spam

Sending unwanted e-mail of any kind (spam) using a company e-mail account is prohibited.

Copyright Issues

Employees on the company's Internet system may not transmit copyrighted materials belonging to entities other than this company. Please note that non-adherence to this policy puts the company in serious legal jeopardy and opens the company up to significant lawsuits and public embarrassment. All employees obtaining access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify, or forward copyrighted materials, except with permission. Failure to observe copyright or

license agreements may result in disciplinary action up to and including termination. If you have questions about any of these legal issues, please speak with your manager or IT department before proceeding.

Monitoring

The company routinely monitors usage patterns in its Internet communications. The reasons for this monitoring include cost analysis, security, bandwidth allocation, and the general management of the company's gateway to the Internet. All messages created, sent, or retrieved over the company's Internet are the property of the company and should be considered public information. Notwithstanding comments above regarding our present intention not to monitor content, the company must reserve the right to access and monitor the content of all messages and files on the company's Internet system at any time in the future with or without notice. Employees should not assume electronic communications are totally private and should transmit highly confidential data in other ways. Electronic messages regarding sensitive matters should warn that such communications are not intended to be secure or confidential. This is just good business sense.

Retention

Company communications of any kind typically needs to be retained as you would any other corporate document. Please remember that e-mails deleted from your e-mail inbox are still saved on the company e-mail server. E-mails that are not managed as part of the corporate document retention policy are kept archived for seven years before being permanently deleted.

Attachments

Attachments with the following file extensions are prohibited, as they are potential security and virus threats:

.bat	Batch processing file used to execute system commands or programs.
.com	Windows command files.
.cpl	Control panel extension.
.exe	Windows binary executable files.
.js	Java script files.
.ocx	Object linking and embedding control.
.pif	Program information file used to tell Windows how to run non-Windows applications.
.scr	Screen saver programs; may include binary code.

.sys	System configuration files.
.vb	Visual Basic script files.

There is also a limit of 10MB of attachments for any e-mail message. Contact the IT Helpdesk if you have a need to transfer more than 10MB of files at any one time.

Confidentiality

Any e-mail message that is meant to be confidential must be labeled as such in the subject line. Forwarding of confidential messages requires the permission of the original sender. The corporate e-mail system will automatically attach a confidential message notification to all e-mails that are sent to addresses outside the organization. Do not attach your own individual confidentially notice as this will be redundant and may be inconsistent with the official company message.

Violations

Any employee who abuses the privilege of company-facilitated access to the Internet will be subject to corrective action up to and including termination. If necessary, the company also reserves the right to advise appropriate legal officials of any illegal violations.