INFORMATION SECURITY POLICY

RADIANT CASH MANAGEMENT SERVICES LTD.
RADIANT BUILDING, # 4/3, RAJU NAGAR, 1ST STREET,
OKKIYAM THORAIPAKKAM, CHENNAI – 600 096.

Information Security Policies & Procedures

Approved by	:	Col. David Devasahayam
Designation	:	Chairman & Managing Director
Approval Date	:	31/MARCH/2023
Prepared by	:	Karthik S
Designation	:	Chief Technology Officer

Effective 31 March 2023

Approval Sheet

Version: 11.9

Col. David Devasahayam
(Chairman & Managing Director)
Radiant Cash Management Services Ltd

Karthik S
(Chief Technology Office)
Radiant Cash Management Services Ltd

TABLE OF CONTENTS

INTRODUCTION

Radiant Cash Management Services Pvt. Ltd. is engaged in the business of cash logistics management, with Collection Executive Presence 2200+ locations in India, wherein 7000 plus cash executives collect/deliver cash. Key clients are mostly banks, NBFCs and insurance companies and to a small extent retail chains. Key segments of the business operations include:

I. Cash Pickup & Delivery: Cash executives collect cash from corporate customer Points of Radiant's client (typically a bank) and retail outlets and deposit the cash inthe bank account of the customer either on the same day or next day. Radiant also delivers cash on behalf of the bank to its customers on the same day or vault it, as required under a shared or dedicated 'transport' model.

II. Cash Van Operations: Radiant Operates Can Vans at multiple locations theseare classified into 4 major types based on the Service Offerings:

- Cash Van on Request (Inter/ Intra)
- Cash Van for Operations
- Dedicated Cash Van
- Cash in Transit

ATM Services: we also provide end-to-end ATM solutions to major banks and financial institutions in India. We provide Cash in transit (CIT) services in majorityof states across the country, Our superior network, technology and risk management solutions allow us to provide secure and efficient cash services to our clients including cash replenishment, deposit clearance and reconciliation and 24/7 maintenance services by our well trained employee network spread across the country enabling us to manage First Line Maintenance (FLM) of ATMs.

1.1 Abstract

In order to accomplish the above business goals we have built tailor made Enterprise Class software which accomplishes our business critical requirements and thesesolutions allow us to provide real-time information for data reliability and consistency.

We have mobile and handheld terminals for cash management services that help us track and trace all our assets on each route.

Our GPS-enabled, armored fleet of vehicles are tracked 24x7 almost anywhere in the country from the central Network Operations center (NOC).

We have enterprise private owned data center facility where the software is hosted and data managed centrally with 24x7 data backup and replication facility and business continuity plan (BCP) and disaster recovery (DR) Facility.

Linux Cluster is an integrated set of software components that has been deployed in a variety of configurations to suite our needs for performance, high-availability, load balancing, scalability, file sharing, and economy.

We do not host or use any software / Applications developed or provided by the bank, however All software applications provided by OEM / Vendor Supplier are scanned and analyzed for vulnerabilities prior to deployment into production server in the test bed.

We do not use Point of Sale (POS) machines or web based online payment gateways in our business.
We do not store client bank account no or any other confidential data of the bank's customer in our Server, however we store and process MIS Data as given by the bank.

We store the MIS data in the central ERP which require specific user ID and password in the ERP and the same is provided to individual staff based on the instructions of their departmental managers / head on a RBAC - Role Based Access Control system, which grants highly differentiated access permissions for users depending on their designation, department, access rights and Users are forced to change their password every 45days, User accounts are deactivated after 90 days of inactivity, User accounts are locked out after three unsuccessful attempts

All connection to the external network are carried via Firewall, IPS using secured protocols and the same is configured to restrict access of various resources, Domain Level Group policies are in effect in the entire network which restricts the usage of all Hardware Software resources.

We follow an approved method to isolate the services to bank both physically and logically to segregate from other Clients and The exchange over shared networks is protected against unauthorized interception by Virtual Private Networks (VPN) with encrypted tunnels or end-to-end encryption between authenticated end-points.

As information security becomes increasingly important to the continued success of business, we follow appropriate security framework across the organization In order to manage these critical systems in a secured manner.

At Radiant Cash Management Services Pvt. Ltd, we have our IS policy in place which is custom document reflecting company's environment and culture, and meets our specific security needs and explains how we implement Information Security principles and technologies in our business.

The same is drafted and prepared by the Chief Technology Officer of the company and approved by the Management, this document is revised and published 2 times in the year during (March & September).

The hard copy of the same is made available in all physical offices of RCMS Pan India, the same is communicated to all the Regional Heads, Branch Heads, Department Heads by email and the same is passed on to all the employees who work under each of the business units.

Radiant Integrity Techno Solutions Pvt. Ltd. (RITS), is an ISO 9001-2008, ISO 27001- 2005(ISMS) Certified company, with its core competency and successful deliveries in ERP Financial Enterprise Solutions, RITS has built the Cash Logistics Management End-to-End ERP Suite integrated with Android based solution and Handheld based Terminals with the Middleware and backend server system for management of Cash Logistics operations.

2 Identification & Authentication of Users

We have implemented access controls and also ensure that all the employees are authorized to access the information system resources and are identified to the information system with unique user ID. The owner of the user ID will be held responsible for all the actions performed under their user ID.

All authorized users will be given only those privileges and entitlements necessary to perform their functions. Entitlement review of all the users will be carried out on semi-annual basis. Immediate supervisor or relevant manager will ensure that an access right of any user is changed within 24 hours on account of registration/termination or change in job profile.

Applications and systems that process, store, or transmit data are monitored, logged, and retained for one year when used by general and privileged users.

2.1 Password Construction Rules

i. All users will be identified to the System by a unique user ID and will use an static password as the method of authentication.
ii. Users will be forced to change their password on first login.
iii. The purpose of a User ID and password is to create security from unauthorized access tothe application or systems or confidential data. User ID's and passwords must conformto the following criteria:
iv. Every employee must use a unique User ID that is associated. No generic/shared UserID's are allowed.
v. It is permissible to use the same User ID and password for each system or application that a user accesses. In all cases, each user is entirely and personally responsible to maintain the complexity and secrecy of his or her password.

Following guidelines will be useful for users in constructing passwords:

a. Consist of a minimum of eight (8) character having a combination of Alpha(Upper and Lower case), Numeric and a Special characters
b. Not to contain any blanks
c. Not to contain the user's name
d. Not to be reused for 6 consecutive times
e. To be changed on a periodic basis or will be forced to change every 30days. Radiant has incorporated password security control such that previous password history can't be repeated to use at any attempt of changing the password.
f. Will be disabled after more than three (3) consecutive failed login attempts.
g. Will be disabled after 30 days of inactivity.
h. Not to be stored or shared.

Description	Examples
Upper-case English Letters	A, B, C, Z
Lower-case English Letters	a, b, c, z
Westernized Arabic Numerals	0, 1, 2, ... 9
Non-alphanumeric (“special characters”)	For example, punctuation, symbols: ({}[],.<>;:’”?/|\`~!@#$%^&*()_-+=)

2.2 User ID Creation/Deletion

I. The supervisor/manager must send a notification to the security administrator for creation of new user accounts and deletion of the existing user’s ID when the person is no longer working for the process/organization using the ID Creation/Deletion standard form.
II. The security administrator will create/delete the ID within 48 hours ofreceiving the request.

Our Organization ensures that appropriate background and reference checks are performed on all staffs (permanent/temporary/onsite vendors) that are responsible for processing Client information.

3 Information Classification, Labelling & Protection

3.1 Information Classification

I. All data are to be classified in the following categories as per its criticality/risk rating:

   a. Customer Confidential: All customer data, which is provided to the organization by the Client for processing will be protected from unauthorized access and kept in lock and key when not being used/processed. This data would only be shared on a need to know basis.

   Radiant has its commitment to Data security policy set up and the strategies are joined in the Annexure V that gives the detailed mechanism of the policy and procedure.

a) Corporate Confidential: All data pertaining to the organization which if compromised could lead to an adverse impact on the organization would be protected from un- authorized access. This data would not be shared with anyone outside the organization.
b) Public: This data which is available to be shared with anybody outside the organization, and which has no data confidentially restrictions as per governing rules and regulations or customer contracts.

II. Copying, archiving and dumping of any system data is authorized by the organization heador Customer representative in writing and copies will be treated with the same level of security and access restrictions as the original.
III. Live sensitive data is not to be used for testing, training or demonstration purposesunless so transformed that it is not possible to identify the original content.
IV. Live and test data, wherever possible are to be logically separated.

3.2 Information Labelling

i. All confidential data is to be labelled as appropriate so that the employee is awareof its risk level and protection to be accorded to it.
ii. Information must be labelled as per the classification defined above
iii. Manual documents (soft/hard copy) must be labelled by inserting the classification inthe documents' footer.
iv. If labelling every document is not feasible, the files in which the documents are filed must be labelled accordingly
v. Labelling can be done by manually marking the classification on the files.
vi. Information must be handled as per its classification. Confidential information must bekept under lock and key when not in use and destroyed securely.

3.3 Information Protection

i. Transfer of Electronic Transportable media (such as floppies, CDS, DVDs, Tapes) – Allthe data stored on any electronic transportable media must be encrypted
ii. Encryption shall be done using approved cryptographic algorithms and key lengths (AES128bit) and security protocols such as:
   a. Entrust
   b. WinZip
   c. Secure PDF
   d. PGP

3.4 Secure Disposal

I. Documents should be shredded when no longer required and disks/ DVD's/ CDs should becut/ shredded/ broken into pieces when not required or damaged beyond repair.
   This should be done before discarding the documents as trash.
II. Hard disk drives, which are rendered permanently unusable or are no longer needed, technically obsolete, or have already been damaged, should be erased using the secure erase utility. The scrapped Hard Disk is to be kept in the custody of IT Security Officer.
   Recovery procedures in case of crash physical processing area are strictly prohibited.
III. Our organizations follow the following mechanism.
   a. Use of Shredder: Paper media containing sensitive material will be disposedof using paper shredders or secure bins.
   b. Disposal of electronic/magnetic media and devices: Electronic media should be destroyed using paper shredders or secure bins. Employees are be encouraged to shred discarded information on their own.
   c. Data stored on the PCs and file servers should be retained as per recordretention plan as instructed by the Client.

4 Physical Security

4.1 PC and Laptop

I. PCs and notebook computers must not be left unattended for long periods while signed-one.g.: during lunch, coffee breaks etc.
II. Users must either logoff or user has to ensure that the password controlled screensaveris activated if they are leaving their PC.
III. The screensaver is set by the System administrator through server policy andwill be activated by default after 10 minutes of inactivity.
IV. IT equipment should not be removed on any occasions. If the users find any IT relatedequipment's, they should inform their supervisor/Manager/System administrator.

The following standards must be applied to Radiant Data Center.

4.2 Data Center

- Access to the Data Center must be restricted to authorized personnel only.
- Third parties who have been granted access to the Date Center must be accompanied at all times by authorized personnel.
- Access to the Data Center must be controlled by a physical access control mechanism such as an electronic or combination lock.

4.3 Fire detection/prevention

- The Data Center must be fitted with smoke/fire detectors and fire extinguishing equipment, which should be set to automatic operation when the computer room is left unattended for long periods.
- Fire detection and prevention equipment must be tested at least twice a year.

4.4 UPS/Backup Generator

- Each production server must have a UPS installed to protect against power surges.
- The UPS and generator must be tested every 3 months.

5 User's Internet and Email Access

As an employee of RCMS using its information technology services, you are provided with access to the vast information resources of the Internet to help you do your job faster and smarter. The facilities to provide that access represent a considerable commitment of company resources for telecommunications, networking, software, storage, etc. This E-Mail and Internet Usage Policy is designed to help you understand our expectations for the use of those resources in the particular conditions of the Internet, and to help you use those resources wisely.

This policy applies to all users of Radiant owned and operated computer systems and networks.

The word 'company' in the following text means Radiant or any organization using Radiant owned or managed systems.
Any exceptions to this policy require the express written consent of both the Radiant and /or the Director of Human Resources.
Any employees who discover a violation of this policy shall notify to the Head of IT department immediately.

Any employee who violates this policy or uses the Internet system for improperpurposes shall be subject to discipline, up to and including discharge.

- The use of Radiant's Internet and e-mail systems is intended for Radiant businessincluding staff research, communication, and professional development within the broad business objectives of the company.
- The company has software and systems in place that can monitor and record all Internet usage. We want you to be aware that our security systems are capable ofrecording (for each and every user) each World Wide Web site visit, each chat, newsgroup or email message, and each file transfer into and out of our internal networks, and we reserve the right to do so at any time. No employee should have any expectation of privacy as to his or her Internet usage. Our managers may review Internet activity and analyze usage patterns, and they may choose to publicize this datato assure that company Internet resources are devoted to maintaining the highest levels of productivity.
- The confidentiality of any electronic message using Radiant's e-mail or Internet systemshould not be assumed. Even when a message is erased, it is still possible to retrieve and read that message.
- Personal use of Internet and e-mail services cannot interfere with business operations and normally should be limited to non-working hours (breaks, lunch).
- E-mail and Internet services, or any other network or computer resources, shall not beused for viewing, archiving, storage, distribution, editing or recording of threatening, obscene, harassing or derogatory material; or transmittal of material that is confidential to the company (e.g. membership lists, accounting records, business plans, etc).
- E-mail and Internet services, or any other network or computer resources, shall not beused for the viewing, archiving, storage, distribution, editing or recording of any kind of sexually explicit image, material or document.
- Radiant has no control over the information or content accessed through the Internet and cannot be held responsible for its content.

- No employee may use the company's Internet facilities to deliberately propagateany virus, worm, Trojan horse, or trap-door program code
- No employee may use the company's network facilities knowingly to disable or overload any computer system or network, or to circumvent any system intended to protect theprivacy or security of another user.
- Users of Radiant's information systems are prohibited from using password protection to restrict access to files on Radiant systems, without authorization from Radiant's Network Administrator.
- Each employee using the Internet facilities of the company shall identify himself or herself honestly, accurately and completely (including one's company affiliation and function where requested) when participating in chats or newsgroups, or when setting upaccounts on outside computer systems.
- The chats, newsgroups and e-mail of the Internet give each individual Internet user an immense and Un precedent reach to propagate company messages and tell our business story. Because of that power we must take special care to maintain the clarity, consistency and integrity of the company's image and posture. Anything any employee writes on the Internet in the course of working for the company can be taken as representing the Radiant's corporate posture. For this reason, users of Radiant's e-mail system are prohibited from using their Radiant e-mail address (e.g. **someone@radiantcashservices.com or other radiant domains**) or otherwise identifying themselves as employees of Radiant when participating in non-work relatedonline discussion forums, bulletin boards, web sites, or chat sessions. Temporary orcontract workers are not permitted to use Radiant e-mail and Internet services unless authorized by Radiant Management. Only those employees or officials who are duly authorized to speak to the media, to analysts or in public gatherings on behalf of the company may speak/write in the name of the company to any newsgroup. Other employees may participate in newsgroups in the course of business when relevant to their duties, but they do so as individuals speaking only for themselves. Where an individual participant is identified as an employee or agent of this company, the employee must refrain from any unauthorized political advocacy and must refrain from the unauthorized endorsement or appearance of endorsement by the company of any commercial product or service not sold or serviced by this company, its subsidiaries or its affiliates. Only those managers and company officials who are authorized to speak tothe media, to analysts or in public gatherings on behalf of the company may grant such authority to newsgroup or chat room participants.
- Employees are reminded that chats and newsgroups are public forums where it is inappropriate to reveal confidential company information, customer data, trade secrets, and any other material covered by existing company secrecy policies and procedures.
- Employees releasing protected information via a newsgroup or chat – whether or not the release is inadvertent – will be subject to all penalties under existingdata security policies and procedures.
- The company retains the copyright to any material posted to any forum, newsgroup, chat or World Wide Web page by any employee in the course of his or her duties.
- Use of company Internet access facilities to commit infractions such as misuse of company assets or resources, sexual harassment, unauthorized public speaking and misappropriation or theft of intellectual property are also prohibited by general company policy, and will be addressed under the relevant provisions.
- All staffs have the responsibility to use the Internet in a professional, ethical and lawful manner.
- Users must not use the Internet facilities to download, display, generate and /or pass on to other materials like text, pictures, which would be considered offensive.

- All access to the Internet from Internal network will be via an approved channel that will be secured by a firewall.
- Users must not deliberately perform acts that waste computer resources or unfairly monopolies resources to the exclusion of others. These acts include sending mass mailings or chain letters, spending excessive amount of time on the Internet, failing to exit from websites, engaging in online chat groups, uploading or downloading large files, accessing streaming audio/video files etc.

6 Antivirus, Firewall, Network and SoftwareRelated Controls

6.1 Antivirus

I. Anti-virus Software must be installed on all PCs and servers and a process establishedfor regular updates (at least once weekly) and these should be checked periodically

II. Anti-virus products should be configured to run checks for known viruses at start-up andto operate in memory-resident mode to check for viruses during normal processing.

III. Updates to anti- virus products and updates to virus identification files for LANconnected workstations should be automatically installed over the LAN server.

IV. At login, the server should verify that the latest version of the anti-virus products andvirus identification file is installed on the desktop and updater it as appropriate.

V. Anti-virus product updates and updates to virus identification files for standalonePCs should occur within one week from when they are made available.

6.2 Firewall

Install firewall to help prevent unauthorized access to the PCs connected to the internet. Be sure to update the firewall products with security patches or newer versions on a regular basis. Firewalls must be configured with deny all rule as far as possible. Log reviews must be carried out periodically to determine any attempts of unauthorized access.

6.3 Software Related Controls

I. Must have software licenses for all software & hardware inventory, these should be checked regularly to ensure adequate no of licenses are used for the software installed.

II. Proper inventory of all the software and hardware used by the organizationwill be maintained

III. All security patches must be tested and applied to the operating system of all PCs and related critical software (mail server/internet gateway/firewall/etc.), a process should be established to ensure timely updates.

IV. Uncertified freeware and shareware are not allowed to be downloaded or installed. Users are strictly advised not to install any freeware/shareware on their own on the company owned desktops or laptops.

V. Administrator rights for desktop/ server should be controlled and password policies setup. All PCs must have BIOS password, which are known only to the employees. PCs should never be operated with administrator access; instead normaluser accounts should be created for all users. All administrator access passwords should be help in dual control with designated persons and copy of password should be stored in two separate sealed envelopes, which are to be kept under lock and key under dual control.

6.4 Network Security Policies and Procedures

6.4.1 Introduction:

This document contains multiple sections that are in many ways inter-related. Several concepts, with security being foremost, become threads that run through the entire document and are common to multiple areas of discipline. All of these records are stored in server data systems and must be treated in a manner consistent with current best practicesto ensure their confidentiality, integrity and availability.

This document strives to define methodologies to support the three essential principles for guarding data in servers and system:

- **Confidentiality:** Ensuring that only authorized users can access confidential or sensitive information. By precisely defining groups of users, and regularly auditing the accuracy and consistency of those groups, we can limit and control who has access to which data. Through a variety of policies, practices and systems, we work to ensure that only those who are authorized will access any given data resource.
- **Integrity:** Ensuring that data has not been tampered with, either on the network or in storage. Our goal is to ensure that data integrity is maintained at all levels.
- **Availability:** Data must be available to those who are authorized to use it. Denial-of- Service attacks is becoming common, and our goal is to ensure that users can access the data they need.

6.4.2 Formal Information Technology Permissions Approval:

Written permission e-mail or otherwise, from an authorized contact person in the IT Department , must be attained in order to add new network accounts and/or devices, grant network file rights, search archived e-mail, or install new application software on a PC.

6.4.3 Network Component Passwords – Contingency Access

Network Operations related Passwords (Servers, Apps, switches and equipment) areto be stored in a secure and password protected management application.

In the event that the appropriate Network Support or Server Administrators are not available in an emergency access to the password vault files, access can be provided by one of the following people:

- Information Technology Head (CTO)
- Network Operations Team leader
- Help Desk Supervisor

6.4.4 Network Component Passwords – Change Cycle:

Passwords on infrastructure components must be changed at the following times:

- At least once every 180 days.
- In the event that a password or system becomes compromised allinfrastructure passwords are to be changed as soon as possible.

6.5 Virtual Private Network (VPN)

Approved / Authorized employees may utilize the benefits of VPNs,for enterprise class software resources usage using local IP.

6.5.1 Additionally:

- It is the responsibility of employees to ensure that unauthorized users are not allowed access to radiant internal networks.
- Authentication must use a two-factor authentication method provided by the Radiant Applications.
- When actively connected to the network, VPNs will force all traffic to and from the PC over the VPN tunnel. All other traffic will be dropped.
- Software must provide an embedded firewall feature, which must be active.
- Gateways will be set up and managed by Information Technology Department
- All computers must use up-to-date anti-virus software.
- All computers must have the most current operating system security patches applied.
- Users will be automatically disconnected from the network after 30 minutes of inactivity.
- The VPN session is limited to an absolute connection time of 24 hours.
- It is the responsibility of employees to ensure that unauthorized users are not allowed access to radiant internal networks.
- Authentication must use a two-factor authentication method provided by the Radiant Applications
- When actively connected to the network, VPNs will force all traffic to and from the PC over the VPN tunnel. All other traffic will be dropped.
- Software must provide an embedded firewall feature, which must be active.
- All employees, with the exception of authorized Information Technology Support Staff, must use a RCMS owned laptop and have a bona fide business need to access the RCMS internal network via VPN.

- Users of computers that are Not RCMS owned equipment must configure the equipment to comply with RCMS VPN and Network Connection policies. RCMS-approved VPN clients may be used.
- Using VPN technology with personal equipment, users must understand that their machines are a de facto extension of RCMS network, and as such are subject to the same rules and regulations that apply to RCMS-owned equipment, i.e., their machines must be configured to comply with RCMS Security Policies and Procedures.

6.6 Wireless Communication

- Includes all wireless communication devices capable of transmitting packet data (e.g., personal computers, wireless phones, smart phones, etc.) connected to any of internal networks. Wireless devices and/or networks without any connectivity to the RCMS networks do not fall under the purview of this policy.
- All wireless access points and base stations must be registered and approved byInformation Technology Dept. All wireless LAN access must use and approved vendor products and security configurations. A data encryption method, which meets or exceeds the Information Technology standard, is required. Client authentication must be accomplished using a two-factor authentication method.
- All wireless network interface cards (NIC) (i.e., PC cards) used in laptop or desktop computers must be registered and approved by Information Technology. If a mobile device contains both a LAN NIC and wireless NIC, the wireless NIC must be disabled while the device is connected to the internal network via the LAN NIC.

6.7 System and network configuration standard

6.7.1 Purpose:

The purpose of the Radiant system and network configuration security standard is toestablish the rules for the maintenance, expansion and use of the network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of the Radiant and its client information.

6.7.2 Scope:

The Radiant's system and network configuration standard applies equally to all individuals with access to any Radiant information resource.

6.7.3 Description:

The Radiant's network infrastructure is provided as a central utility for all users of Radiant information resources. It is important that the infrastructure, which includes cabling and the associated equipment such as routers and switches, continues to develop with sufficient flexibility to meet user demands while at the same time remaining capable of exploiting anticipated developments in high speed networking technology to allow the future provision of enhanced user services.

- Radiant information technology Dept. (IT) owns and is responsible for the Radiantnetwork Infrastructure and will continue to manage further developments and enhancements to this infrastructure.
- To provide a consistent Radiant network infrastructure capable of exploiting new networking developments, all PCs, laptops, cabling must be installed by Radiant IT Team.
- All network connected equipment must be configured to a specification approved by
- Radiant IT - IS Policy.
- All hardware connected to the Radiant network is subject to Radiant IT management and monitoring standards.
- Changes to the configuration of active network management devices must not be made without the approval of RCMS IT Head.
- The Radiant network infrastructure supports a well-defined set of approved networking Protocols. Any use of non-sanctioned protocols must get approval from Radiant IT.
- The networking addresses for the supported protocols are allocated, registered and managed centrally by Radiant IT.
- All connections of the network infrastructure to external third party networksis the responsibility of Radiant IT. This includes connections to external synchronous optical (sonet), ISP and telephone networks.
- Firewalls must be installed and configured following the Radiant firewall implementation standard documentation as mentioned in the IS Policy. The use of departmental firewalls, switches, routers, hubs are not permitted without the written authorization.
- Users are not permitted to alter network hardware in any way and must not install network hardware or software that provides network services without Radiant IT approval.IT Team reserves the right to remove any network device that does not complywith standards or is not considered to be adequately secure.

6.7.4 Enforcement:

Any violation of this standard may result in disciplinary action in accordance with Radiant IS policy and procedures

6.7.5 Review:

As per InfoSec policy review has been conducted bi-annually. Respective Administrators/Personals/Heads should conduct review and should submit review report without failure as instructed.

7 Data Backup, Storage and Retrieval

I. Back up of the system data will be undertaken post approval of the client and based on therequirements defined by the client. Backups May be taken on DVDs /Backup Hard disks and the same will be encrypted in storage. Backup Data will load separately into separate storage workstation to test the backup media. Backups will not be taken if not required by the client.

II. If data is not required after it has been sent to the client. It should be purged at the end ofthe day from the PCs and file servers.

III. Access to the back media should be restricted to the supervisors.

IV. **Backup frequency:** Frequency at which backup to be taken will be determined on the basisof criticality of data and the directives from the client.

V. **Backup data testing:** Backup media should be tested regularly to ensure that themedia can be relied upon during a contingency.

VI. **Backup inventory:** Proper inventory of the Backup should be maintained in the prescribedformat.

VII. **Back up data retention:** backup data shall retain for a period as specified by the client.

VIII. **Offsite storage:**
Backup data can be stored at a secure offsite location in an encrypted format after getting an approval from the client.

7.1 Record Retention Policy

The retention of data and determination of useful retention of system logs is determined by system administrators under the direction of the IT Head. System administrators and database administrators are responsible for the execution of retention and adherence to the schedule.

7.2 Record Types

This policy addresses electronic data generated by systems in various formats (.txt, .tar, .zip,etc), and all systems provided for the user for the storage of data. For user generated data, *retention* refers to the length of time a document is available for recovery once deleted by the user from the system.

7.3 Litigation Hold

When Radiant receives a litigation hold for electronic data, the data and email as well as any associated backups as of the day of the hold are copied and quarantined. Any backup retention policies that would delete files older than 90 days are removed so that files are retained.

7.4 Records Retention

Radiant has document outlining the retention of system logs, responsible party and location. User data, for the purpose of this document, data that has already been deleted bythe user is retained via backup copies.

Data that resides on user desktops/laptops is retained for 30 days beyond deletion. Once 30 days has passed, this data is permanently removed and no longer able to be recovered. ‘

Data that resides on Radiant provisioned data center storage (shared network drives andfile locations) is retained for 365 days beyond deletion.

Email Trash: Radiant does not perform mandatory purge of data in the users Trash folder. Deleted mail remains in these folders until the user empties the trash from the system. The 30 day retention applies to email that has been purged from users' Trash.

7.5 Procedure

Responsible	Action
Data Owner/Departments	Data owners/departments will designate records coordinator for their areas and report that designation to the IT Team.
IT Department	The IT Dept. role is to authorize any changes to the Retention,
	Storage, and Destruction policies and procedures; review and
	approve retention schedules and revisions to current retention
	schedules; address compliance audit findings; and review and
	Approve control forms relating to business records.
Legal Services	Legal Services serves as subject matter expert and provides
	counsel regarding records designations and legal and statutory
	Requirements for records retention and pending legal matters.
	It ensures that access to or ownership of records is appropriately
	Protected in all lines of business or facility closures.

7.5.1 Guidelines for Retention of Records/Information and Schedules:

Record Retention	Unless otherwise stipulated, retention schedules apply to all records. Records will only be discarded when the maximum specified retention period has expired, the record is approved for destruction by the Operations Head, and a Certificate of Destruction is executed.
Non-record Retention	Non-records are maintained for as long as administratively needed, and retention schedules do not apply. Non-records may and should be discarded when the business use has terminated.
E-mail communication retention	Depending on content, e-mail messages and documents transmitted by e-mail may be considered records and are subject to this policy. If an e-mail message would be considered a record based on its content, the retention period for that e-mail message would be the same for similar content in any other format. The originator/sender of the e-mail message (or the recipient of a message if the sender is outside Organization) is the person responsible for retaining the message if that message is considered a record. Users must save e-mail messages in a manner consistent with departmental procedures for retaining other information of similar content.

7.5.2 Storage and Destruction Guidelines

Active/Inactive Records	Records are to be reviewed periodically by the Data Owner to determine if they are in the active, inactive, or destruction stage. Records that are no longer active will be stored in the designated off-site storage facility. Active stage is that period when reference is frequent and immediate access is important. Records should be retained in the office or close to the users. Data Owners, through their Records Coordinator, are responsible for maintaining the records in an orderly, secure, and auditable manner throughout this phase of the record life-cycle.
Active/Inactive Records, continued	Inactive stage is that period when records are retained for occasional reference and for legal reasons. Inactive records for which scheduled retention periods have not expired or records scheduled for permanent retention will be catalogued and moved to the designated off-site storage facility. Destruction stage is that period after records have served their full purpose, their mandated retention period, and finally are no longer needed.

Storage of Inactive Records	All inactive records identified for storage will be delivered with the appropriate Records Management Forms to the designated off-site storage facility where the records will be protected, stored, and will remain accessible and catalogued for easy retrieval. Except for emergencies, the designated off-site storage facility will provide access to records during normal business hours.
Records Destruction	General Rule: Records that have satisfied their legal, fiscal, administrative, and archival requirements may be destroyed in accordance with the Records Retention Schedules. Permanent Records: Records that cannot be destroyed include records of matters in litigation or records with a permanent retention. In the event of a lawsuit or government investigation, the applicable records that are not permanent cannot be destroyed until the lawsuit or investigation has been finalized. Once the litigation/investigation has been finalized, the record may be destroyed in accordance with the Records Retention Schedules but in no case shall records used in evidence to litigation be destroyed earlier than a specified number of years from the date of the settlement of litigation. Destruction of Records Containing Confidential Information: Records must be destroyed in a manner that ensures the confidentiality of the records and renders the information unrecognizable. The approved methods to destroy records include. A Certificate of Destruction form must be approved and signed by the appropriate management staff prior to the destruction of records. The Certificate of Destruction shall be retained by the off- site storage facility manager. Destruction of Non-Records Containing Confidential Information: Destruction Non-Records containing personal or other forms of confidential corporate, employee, member, of any kind shall be rendered unrecognizable for both source and content by means of shredding, pulping, etc., regardless of media. This material shall be deposited in on-site, locked shred collection bins or boxed, sealed, and marked for destruction. Disposal of Electronic Storage Media: Electronic storage media must be assumed to contain confidential or other sensitive information and must not leave the possession of the organization until confirmation that the media is unreadable or until the media is physically destroyed.

Records Destruction, continued	Disposal of Electronic Media: Electronic storage media, such as CD-ROMS, DVDs, tapes, USB thumb drives, disk drives containing confidential or sensitive information may only be disposed of by approved destruction methods. These methods include: CD-ROMs, DVDs, and other storage media that do not use traditional magnetic recording approaches must be physically destroyed. Disposal of IT Assets: Department managers must coordinate with the IT Department on disposing surplus property that is no longer needed for business activities according to the Disposal of IT Assets Policy. Disposal of information system equipment, including the irreversible removal of information and software, must occur in accordance with approved procedures and will be coordinated by IT personnel.

8 Remote Storage Media

8.1 Objective:

Enable the correct data to be made available where it is required. Maintain the integrity of the data. Prevent unintended or deliberate consequences to the stability of RCMS computernetwork. Avoid contravention of any legislation, policies or good practice requirements. Build confidence and trust in the data that is being shared between systems. Maintain high standards of care in ensuring the security of personal, protected and restricted information. Enable the disclosure of information as may be necessary by law.

8.2 List of Removable Media devices

Removable media devices include:

- CDs. DVDs.
- Optical Disks.
- External Hard Drives.
- USB Memory Sticks (also known as pen drives or flash drives). Media Card Readers.
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards).
- Digital Cameras.

8.3 Policy aims to mitigate the following risks:

- Disclosure of RESTRICTED or personal information as a consequence of loss, theft orcareless use of removable media devices.
- Contamination of networks or equipment through the introduction of viruses through the transfer of data from one form of IT equipment to another.

- Potential sanctions against the individuals imposed by the Information Technology Head as a result of information loss or misuse.
- Potential legal action against the individuals as a result of information loss or misuse.
- Damage to RCMS reputation and loss trust and confidence as a result of information loss or misuse.
- Non-compliance with this policy could have a significance effect on theefficient operations and may result in financial loss.

8.1 Compliance

If any user is found to have breached this policy, they may be subject to disciplinary action. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If the user / employee does not understand the implications of this policy or how it may apply to him/ her, they are requested to seek advice from the IT Team**.**

8.2 Key Messages

- The use of removable media devices is only be approved if there is a valid business case for its use.
- Any removable media device that has not been supplied by Information Services must not be used.
- All data stored on removable media devices must be encrypted where possible.
- Damaged or faulty removable media devices must not be used.
- Special care must be taken to physically protect the removable media device and stored data from loss, theft or damage.
- Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss.
- Removable media devices that are no longer required, or have becomedamaged, must be disposed of securely to avoid data leakage.

9 Disaster Recovery Procedures and Business Continuity plan

I. The firm provides for a disaster recovery procedures in case of any uneventful mishap orbreakdown of systems at the site. The objective of the plan is to enable the organization to survive a disaster and to re-establish normal business operations canresume normal processing with in a reasonably time frame.

II. The IT Head is designated as the project manager in charge of the BCP team and is responsible for developing and maintaining the organization's business continuity plan(BCP).The team also consists of team leaders drawn from the different departments.

III. The BCP team is responsible for assessing existing vulnerabilities: implementing disaster avoidance and prevention procedures: and developing a comprehensive plan that willenable the organization to react appropriately and in a timely manner, in the eventually ofany disaster.

IV. A through security assessment of the computing and communications environment including personnel practices; physical security; operating procedures; backup and contingency planning; systems development and maintenance ; database security; systems and access control software security; insurance; security planning and administration ;application controls; and personal computers is essential.

V. The security Assessment will enable the project team to improve any existing emergencyplans and disaster prevention measures and to improve any existing emergency plans and disaster prevention measures where none exist.

VI. The BCP team is responsible to present findings and recommendation resulting from theactivities of the management so that corrective actions can be done initiated in a timely manner.

VII. The project team required to identify critical systems. Processes and functions; asses the economic impact of incidents and disasters that results in a denial of access to systems services and others services and facilities; and asses the "pain threshold". That is the length of time business units can survive without access to systems, services and facilities.

VIII. The BCP procedures are put to test at predefined intervals of time in order to assess theeffectiveness of the same and to make necessary amendments to reflect changes in the physical, processing and external environment.

10 Incident Management

This document provides a framework for security event/incident handling and response within our organization. It outlines the steps to be taken when security events are discovered and establishes the organizational requirements, including roles and responsibilities for incident processing and protection. Using this document, incident handling and response can be performed in a consistent manner.

It is essential that all security events within the organization should be reported to the IT teamor Supervisor/Manager of the team for recording, tracking and reporting to management.

10.1 Information Security Event:

An information security event is an identified occurrence of a physical, system, service or networkstate indicating a possible breach ofinformation security policy or failure of safeguards such as:

- A door propped open to a Computer Room of facility
- Change to an employee's current password without a system prompt
- Loss to a service or error messages appearing in applications.
- Unauthorized persons observed in physical processing areas
- Persons observed accessing information/physical assets that is unrelated to their functional responsibilities.

10.2 Information Security Incident:

An Information Security incident is defined as any irregular or adverse event that occurs within theorganization. It may be a single or series of unwanted or unexpected information security events thathave a significant probability of compromising business operations and threatening information security.

Some examples of possible incident categories include, but are not limited to:

- Compromise of system integrity
- Denial of system resources
- Worm or virus attacks
- Illegal access to the system (either a penetration or intrusion)

Malicious use of system resources:

- Any kind of damage to the system initiated inside or outside of organization
- Loss or theft of equipment
- Notification of a software vulnerability that effects a production application
- Any activities that violate Radiant IS policy are considered an incident. Security incidents canbe either accidental or deliberate.

10.3 Security Incident Handling

All staff will follow the procedure outlined below whenever they detect or suspect a security incident:
Any incident resulting out of an accidental or intentional breach of security policy and resulting in any misuse/ loss of information / media OR affecting the physical access to such media / information is classified as a security incident.
Such incidents may be broadly classified as below:

- Unauthorized access to Client specificdata /information.
- Misuse / distraction of Client specific data / information.
- Intrusion / tampering of physical assets of the organization by unauthorized / externalpersonnel.

a) Any event / incident of a suspicious nature, like unauthorized persons observedin physical processing areas, persons observed accessing information/physical assets that is unrelated to their functional responsibilities, etc.

b) Virus attack which impacts Client's information's. Theft/damage to Client's information assets including fire/floods, etc.

10.4 Report incidents to:

- In the event of a possible incident or suspicious event is detected, the employee should report the incident to his/her immediate reporting functional superior.
- The functional superior is required to further contact their local designated IT support professional and escalate the matter to the IT head.
- If a local or designated IT support staff is unavailable, individuals should determine and complete the initial essential actions as instructed on information security awareness training.

Notification regarding events of incidents should be further shared to all the relevant Regional/Branch Heads, Department heads/functional superiors, Stakeholders, Clients etc… within an hour and the notification contains the following:

- Incident Date/Time.
- Incident Reported by.
- Incident Description.
- Timeline (Depending upon the severity of the events it will be resolved within 24 to 48 hours)

10.5 IT Team Response:

Radiant IT professionals have additional responsibilities for IT security incident handling and reporting for both the systems they manage personally for their units and the systems of userswithin their units.

In the case of an IT security incident, IT staff should:

- Respond quickly to reports from individuals.
- Take immediate action to stop the incident from continuing or recurring.
- Determine whether the incident should be handled locally or reported to the IT Head.
-

If the incident does not involve the loss of confidential information or have other serious impacts to individuals or the organization, the IT staff should:

- Renovate the system
- Restore service
- Preserve evidence of the incident.

If the incident involves the loss of confidential information or critical data or has other potentially serious impacts, the IT support staff should:

- Report the incident to IT head.
- IT head will investigate the incident in consultation with the relevant professionals anddevelop a response plan
- File an IT Security Incident Report form including a description of the incident anddocumenting any actions taken thus far.

Security Investigation:

Security investigations must address the following:
What happened and its impact Why it happened and how?
What needs to be done immediately to prevent further damage and facilitate initialrecovery?
What needs to be done in the longer term to prevent a further occurrence?
Identify if any person is culpable and whether disciplinary action is necessary?

10.6 Report incidents within:

Any security incident should be reported to the functional superior immediately to enable the suitable escalation/action to contain the incident. The person identifying an incident will report to the manager whom he reports to, who in turn, will immediately contact the IT head.

10.7 Report to include:

The reporting manager should immediately document the events to ensure that a clear and accurate record is provided to persons involved in the incident's management. The incident report will be further forwarded to the respective teams and the same will be updated in incident register. The report should include the following information:

- Initial assessment of the extent of impact.
- Date, Time and location of the event.
- Name of the individual that detected the incident.
- Description of the sequence of suspicious events observed (including name and function of anyone suspected of being involved in the event)
- List of anyone else that witnessed or observed the events.

11 General Guidelines

- Password should not be shared or written down.
- Users are solely responsible for activities associated with their ID's and password.
- Users are advised not to use predictable passwords.
- Every desktop and laptop (if any) must have an automatic screen saver password, setto time out not later than fifteen minutes of inactivity. If you're PC does not have this functionality, report this to your IT person/system administrator. When you leave your PC unattended, set the screen saver (typically set by hitting Ctrl + Alt + Del and selecting "Lock computer").This ensures that no unauthorized person is using the system in the user's absence.
- Users must not connect to any external network from desktops that are being used to process any Client's information. This means that there should not be any connectivity to the Internet or any other network unless required for a business purpose.
- Intentionally using systems to distribute any virus is strictly prohibited. Any suchincidence if observed must be reported to the IT person/System administrator.
- Do not install software on your computer that is not licensed. All installations must be done by the IT person only.
- Do not store non-business related images in your PC. In case you observe any suchinstances report to your supervisor immediately.
- The anti-virus updates should be regular and for all PCs on the network includingthe server.
- Sensitive Information sent through external networks must be encrypted by using encryption software to protect the information. WinZip can be used for this purpose.
- Employees must receive periodic training in good security practices and shouldbe aware that:
- The collection, storage, use, disclosure and transfer of personal information(including customer and employee data) may be subject to privacy laws and regulations.
- Criminals, hackers and other unauthorized individuals use Social Engineering Techniques to obtain access to Client information. Make sure your employees are aware of the common social engineering techniques such as Psychological subversion, Masquerading, Shoulder surfing < Tailgating and Dumpster diving and are able to appropriately respond to them.

- Users must log off and switch off their PCs at the end of their work period.
- Documents of confidential or sensitive nature (especially Client Information) should not be left unattended on desktops or in open cabinets, desk drawers or cupboards after office hours.
- Fax machines should be cleared at the end of the day and switched off (if not used).
- Nothing of a confidential or sensitive nature should be appended to work area partitioning oron desktops e.g. telephone numbers/names of customers/customer account numbers.
- Users must not give Sensitive Information to other employees, vendors, orcustomers unless they are sure that they are entitled to see it.
- None of the PCs in the LAN should be connected to the printer unless required forthe business purpose.
- The floppy drives, USB ports, and CD drive should not be enabled on any PC,Server unless required for business purpose.

Adhering to the above mentioned guidelines are an integral part of every employee's responsibilities within his/her job. Failure to do so will result in corrective action including terminations of services.

12 ACCESS CONTROL: Business requirements

12.1 Business requirements for access control

The objective of this category is to control access to information, information processing facilities, and business processes.

12.1.1 Access control policy

An access control policy should be established, documented and periodically reviewed, based on business needs and external requirements. Access control policy and associated controls should take account of:

- Security issues for particular data systems, given business needs, anticipatedthreats and vulnerabilities;
- Security issues for particular types of data, given business needs, anticipatedthreats and vulnerabilities;
- All relevant legislative, regulatory and certificatory requirements;
- Relevant contractual obligations or service level agreements;
- Other organizational policies for information access, use and disclosure; and
- Consistency among such policies across the organization's systems and networks;

Access control policies include:

- clearly stated rules and rights based on user profiles;
- consistent management of access rights across a distributed/networked environment;
- an appropriate mix of logical (technical) and physical access controls;
- segregation of access control roles -- e.g., access request, access authorization, access administration;
- Requirements for formal authorization of access requests ("provisioning"); and requirements for authorization and timely removal of access rights ("de-provisioning").

12.2 Enterprise Role-Based Access Control (ERBAC):

12.2.1 Role-based access control (RBAC)

It is an approach to restricting system access to authorized users. It is referred to as role- based security.
Within an organization, roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Members or staff (or other system users) are assigned particular roles, and through those role assignments acquire the computer permissions to perform particular computer-system functions. Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user's account; this simplifies common operations, such as adding a user, or changing a user's department.

12.2.2 Advanced Features for Enterprise-Wide Role-Based Access Control:

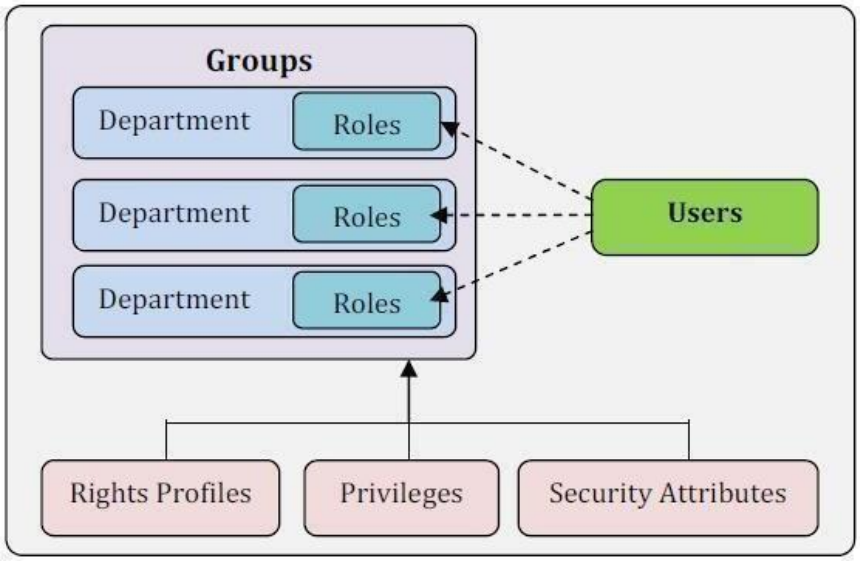
a) User Login Logs
b) User Role Assignment - Mandatory Access Control (MAC) or Discretionary Access Control(DAC).
c) User Role Assigned History
d) User Transaction Logs – Daily Text File Updates
e) Online Access Users (Live / Active / Inactive Users)
f) Login Authentication Methods [Catha, OTP-(Email/SMS), Image Auth_t]
g) Custom Settings for Integration of SMS / Email.
h) Device Based access controls (Mobile, Handheld, and Tablets)
i) Periodic Access Permission Auditing
j) User Account Restriction (Login Failure – No of Attempts)
k) Forgot Password through Email / SMS / Admin through phone (Resetpassword to Default and Change on first Login)
l) Role Authorization [Database – Update, Insert, Append, Delete] [Locks – Open,Close] [Reports –Create, View, Print] [Applications – Read, Write, Execute]
m) Last Accessed User Info - On login display first + last name and profile picture with lastaccessed date & time.
n) Account Terminations View
o) Password Encryption / Decryption (Encrypted Data Source Passwords Match)
p) Page URL Hide through HD access.
q) User ID Availability Checker
r) Password Security Level Checker (Low-Medium-High)
s) Digital Signature – Token PKI Authentication – RSA Algorithm Validation for MAC ID.
t) RSA Secure Software Tokens: strong authentication by Deploying RSA softwaretokens on PCs and Laptop and transform them into intelligent security tokens.

12.2.3 Three primary rules are defined for RBAC:

a) Role assignment: A subject can exercise permission only if the subject has selected or been assigned a role. Role authorization: A subject's active role must be authorized for the subject. With rule 1above, this rule ensures that users can take on only roles for which they are authorized.
b) Permission authorization: A subject can exercise permission only if the permission is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can exercise only permissions for which they are authorized.

12.2.4 Three levels of RBAC:

- Core RBAC
- Hierarchical RBAC, which adds support for inheritance between roles
- Constrained RBAC, which adds separation of duties



Radiant has integrated the parts and duties of its employees under Logical access rights approach to review the same and to perform every action all the while in the process. TheLogical access rights concerning RBAC are accessible in Annexure IV.

13 Change Management

13.1 Introduction

Change Requests head on with a Change Management process, which describes such a process, in brief. Change in software development can be a change in specifications, user requirements, design change, code change or so on.

13.2 Origination of changes

Changes can originate from various sources including customers, end users, the project team or the test team. Changes from customers and end users would normally be changes in their requirements; from the project team design changes could come; and the testing team could request code changes. Changes are communicated to the Software Project Manager (SPM) using a Change Request (CR) form. The CR would contain details of the project, module and component which are likely to be affected by the CR and may include reasons for the CR.

13.3 Procedure for CR resolution

Normally when a CR is received, the first activity is to record it in an Excel Sheet that facilitates CR Register functionality, this forms the main tool for tracking all CRs to resolution- which may be rejection of the CR or implementation. All CRs received would be entered in the excel sheet and would be tracked through to closure. Then the CR is analyzed by the SPM (Software Project Manager) who would analyze the CR and approve or reject it. The analysis would determine:

a) Whether implementation of CR would be feasible
b) The amount of effort and calendar time it would take to implement the CR
c) The impact of the CR on the overall project – especially in terms of effort, schedule and cost once the analysis is completed, the Impact Analysis would be submitted to IT Head or the SPM who would approve or reject the CR. In case of rejection, the decision along with the reasons wouldbe communicated to the originator of the CR and the CR is closed in the CR Register. Once a CR is approved for implementation, it would be implemented in accordance with the CR implementationstrategy decided and recorded in the Software Configuration Management Plan (SCMP). Various strategies are:
d) Implement CRs as and when received, immediately on receipt
e) Collate all CRs and retrofit them at the end of development
f) Situational implementation – that is
    - If the component which is affected by the CR yet to be coded or is being coded, then implement it when it is coded
    - If the coding of the component which is affected by the CR is completed, keep the CRpending and retrofit it at the end

Once this is decided, the CR would be implemented in line with the analysis and implementation strategy decided by IT head or the SPM. Implementation for the CR would be carried out as follows:

a) The CR would be allocated for resolution to one or more team members as necessary by theSPM
b) The team members would carry out necessary coding and modification of existing code asnecessary. This activity would be governed by the coding guidelines for the project.
c) The CR would them be allocated for Peer Review. Peers would review the code to ensure that the:

- Implementation fulfils the requirements of the CR
- The implementation conforms to the defined coding guidelines and other software engineering standards of the organization
- There is no trash code or malicious code left in the software
- The changed code ensures efficiency of execution and response times

a) Once the CR is approved in the Peer Review, it would be submitted for Regression Testing tothe testing team
b) The testing team would carry out regression testing to ensure that all functionalities requested in the CR are correctly working and that no other original functionality is affected by the implementation
c) Once regression testing is completed, and all defects pointed out in peer review or regression testing are resolved and closed, then the CR is closed in the CR register and further action is only taken as needed.

13.4 Acronyms Used

- Software Project Manager (SPM)
- Change Request (CR) form
- IT Head / (Change Control Board)
- Software Configuration Management Plan (SCMP)

13.5 Change Request

1. The CR would normally contain the following entries:
2. The CR Id, which could be a serial number
3. The CR description
4. Date on which the CR is received
5. Allocation details for Analysis including date of allocation, completion date, to whomit is allocated
6. Allocation details for Approval of CR including date of allocation, completion date, to whom itis allocated
7. Allocation details for Resolution of CR including date of allocation, completion date, towhom it is allocated
8. Allocation details for peer review including date of allocation, completion date, to whom it is allocated
9. Allocation details for regression testing including date of allocation, completion date, to whom it is allocated
10. Status – open, closed or under analysis / approval / resolution / peer review/ Regression testing.
11. Date on which CR is closed.

13.6 Role:

One individual may be responsible for several roles as well as several individuals maybe fulfilling a single role. The IT Department is responsible for managing the execution of the Change Control.

13.7 Procedure:

1. A request must be submitted to the IT Head.

2. If the initial request is approved by the IT Head and is not an emergency Change, an appropriate Change Control Team is formed.

3. An impact analysis is performed by a member of the Change Control Team to determine what applications are affected by the change, if an outage is required and to determine the approximate costs and risks associated with the request. A back-out plan is also developed and included in the impact analysis to ensure that unsuccessful changes or undesirable results do not adversely impact business processes.

4. The Change Control Team will meet as needed to review proposed changes. The ITHead is the coordinator of the Change Control Team.

5. If a request is denied, the requestor is notified in writing.

6. Requests that are approved are categorized by priority (critical or normal), a change

7. Implementer is assigned, an implementation date is determined, and responsibility for end user communications is assigned.

8. Emergency changes and IT changes: In the event of an emergency requirement for a change, the IT Head must approve a change prior to implementation and document reason for change, implementation notes and appropriate testing.

9. The Change Control Team will develop test scripts as necessary and assign test responsibilities so that users can validate the changes in the production environment. User acceptance information (name, date, summarized results, etc., as applicable) is documented in a database.

10. Once completed and tested, the documentation and history of the project is retained. All user approvals that were captured by email will be also be saved. The IT Head will maintain copies of approval emails in his/her email files to facilitate validation of the contents of emails.

13.8 Rollback Plan:

For safety measures before implement into LIVE we will take backup of the configuration, data and code file. Based on the result of UAT and as per our SIT process we will proceed further into LIVE implementation in LIVE after the end of production hours. On production hours we will check with data before and after implementation of new requirement into LIVE will ensure the negative of any data loss, if any discrepancy happens will try to resolve in one or two hours based on priority if it is not resolved within the stipulated time we will revert the changes in production environment on approval of IT head and issues, error or bug faced while in LIVE will be resolved in development environment. On successful testing again procedure to proceed LIVE will be initiated.

14 Program me Development - SDLC (Software DevelopmentLifecycle) Model.

We follow the Agile SDLC Model in Application Development.

14.1 Agile SDLC:

Agile software development is a group of software development methods in which solutions evolve through collaboration between self-organizing, cross-functional teams. It promotes adaptive planning, evolutionary development, early delivery, continuous improvement, and encourages rapid and flexible response to change.

- Speed up or bypass one or more life cycle phases
- Usually less formal and reduced scope
- Used for time-critical applications
- Used in organizations that employ disciplined methods

14.2 Our Agile Manifesto is based on 12 principles:

- Customer satisfaction by early and continuous delivery of useful software
- Welcome changing requirements, even late in development
- Working software is delivered frequently (weeks rather than months)
- Close, daily cooperation between business people and developers
- Projects are built around motivated individuals, who should be trusted
- Face-to-face conversation is the best form of communication (co-location)
- Working software is the principal measure of progress
- Sustainable development, able to maintain a constant pace
- Continuous attention to technical excellence and good design
- Simplicity—the art of maximizing the amount of work not done—is essential
- Self-organizing teams
- Regular adaptation to changing circumstance

We use Extreme Programming (XP) Agile Method &Adaptive Agile Method:

14.3 Extreme Programming (XP) - Practices:

1. Planning game – determine scope of the next release by combiningbusiness priorities and technical estimate
2. Small releases – put a simple system into production, then release newversions in very short cycle
3. Metaphor – all development is guided by a simple shared story of howthe whole system works
4. Simple design – system is designed as simply as possible (extracomplexity removed as soon as found)
5. Testing – programmers continuously write unit tests; customers writetests for features
6. Refactoring – programmers continuously restructure the system without changingits behavior to remove duplication and simplify
7. Pair-programming -- all production code is written with two programmersat one machine
8. Collective ownership – anyone can change any code anywhere in thesystem at any time.
9. Continuous integration – integrates and builds the system many times a day – everytime a task is completed.
10. 40-hour week – work no more than 40 hours a week as a rule
11. On-site customer – a user is on the team and available full-time to answer questions
12. Coding standards – programmers write all code in accordance withrules emphasizing communication through the code

14.4 Adaptive SDLC:

Combines RAD with software engineering best practices
Project initiation

- Adaptive cycle planning
- Concurrent component engineering
- Quality review
- Final QA and release
- Project initialization – determine intent of project
- Determine the project time-box (estimation duration of the project)
- Determine the optimal number of cycles and the time-box for each
- Write an objective statement for each cycle
- Assign primary components to each cycle
- Develop a project task list
- Review the success of a cycle
- Plan the next cycle

15 Deployment for RCMS Enterprise Network

15.1 Hardware Management + OS Provisioning + OS Updates + Virtualization Management

- By Default All users will login to DC1 and Node 1 will Active, and node2 will be passive. DRBD Component will be available on HA and all the data will be backed up dynamically. In case of failure of Active Node 1 in DC1 the Coro sync will map the user traffic to node2 as a BCP. The user will not be required to wait for the changeover and no operation delay time will be observed.
- **R sync** (**Remote Sync) is** used for **copying** and **synchronizing** files and directories **remotely** from DC1-Node 2 to DC2-Node1. DRBD in DC2 will transfer data from Node1 to Node2 on HA and all the data will be backed up dynamically.
- In case of Failure of DC1 the firewall will route the traffic to Public IP of DC2. The user willknow about the DR Change over and will be required to wait for 30mins Changeover time.

15.2 MySQL with DRBD/Pacemaker/Coro sync/Oracle Linux

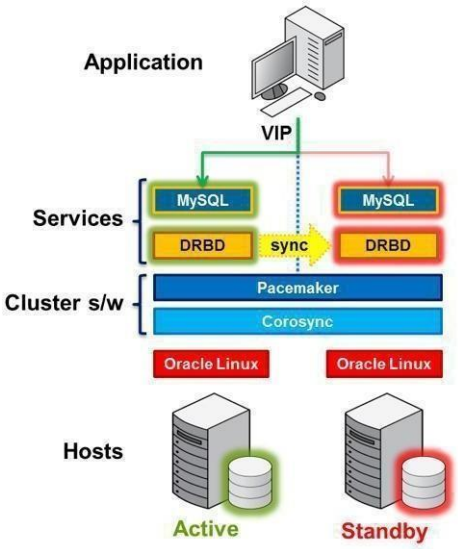
DRBD (Distributed Replication Block Device) is one of the leading solutions for MySQL HA (HighAvailability). When combined with Pacemaker and Coro sync, we have:

- An end-to-end, integrated stack of mature and proven open source
- Technologies, fullysupported by Oracle (as part of MySQL Enterprise Edition).
- Automatic failover and recovery for service continuity.
- Mirroring, via synchronous replication, to ensure failover between nodes without the risk of losing committed transactions.
- Building of HA clusters from commodity hardware, without the requirement for shared-storage.
-

The following figure illustrates the stack that can be used to deliver a level of High Availability for theMySQL service.

At the lowest level, 2 hosts are required in order to provide physical redundancy; if using a virtual environment, those 2 hosts should be on different physical machines. It is an important feature that no shared storage is required. At any point in time, the services will be active on one host and in standby mode on the other.
Pacemaker and Coro sync combine to provide the clustering layer that sits between the services and the underlying hosts and operating systems. Pacemaker is responsible for starting and stopping services, ensuring that they are running on exactly one host, thus delivering high availability and avoiding data corruption. Coro sync provides the underlying messaging infrastructure between the nodes that enables Pacemaker to do its job; it also handles the nodes membership within the cluster and informs Pacemaker of any changes.

15.3 Server HA Components Architecture



The core Pacemaker process does not have built-in knowledge of the specific services to be managed; instead, it uses agents that provide a wrapper for the service-specific actions. For example, in this solution we use agents for Virtual IP Addresses, MySQL and DRBD: these are all existing agents and come packaged with Pacemaker. The essential services managed by Pacemaker in this configuration are DRBD, MySQL and the Virtual IP Address that applications use to connect to the active MySQL service.

16 Mobile Device Management (MDM)

16.1 Introduction

Mobile devices, such as smart phones and tablet computers, are important tools for the organization and Radiant Cash Management Services Pvt. Ltd. supports their use to achieve business goals.
However, mobile devices also represent a significant risk to data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the organization's data and IT infrastructure. This can subsequently lead to data leakage and system infection. Radiant Cash Management Services Pvt. Ltd. has a requirement to protect its information assets in order to safeguard its customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices and applications.

16.2 Scope

1. All mobile devices, whether owned by or leased by Radiant Cash Management Services Pvt. Ltd.
2. Employees, inclusive of smart phones and tablet computers that have access to corporate networks, data and systems are governed by this mobile device security policy.
3. Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk authorized by security management must be conducted.
4. Applications used by employees on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy.

16.3 Policy

16.3.1Technical Requirements

1. Devices must use the following Operating Systems: Android 2.2 or later, I OS 4.x or later.
2. Devices must store all user-saved passwords in an encrypted password store.
3. Devices must be configured with a secure password that complies with Radiant Cash Management Services Pvt. Ltd.'s password policy. This password must not be the same as any other credentials used within the organization.
4. Only devices managed by IT dept. will be allowed to connect directly to the internalcorporate network.
5. These devices will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by the IT department using Mobile Device Management software.

16.3.2 User Requirements

- Users may only load corporate data that is essential to their role ontotheir mobile device(s).
- Users must report all lost or stolen devices to Radiant Cash Management Services Pvt. Ltd.IT Department immediately.
- If a user suspects that unauthorized access to company data has taken place via a mobiledevice, they must report the incident in alignment with Radiant Cash Management Services Pvt. Ltd.'s incident handling process.
- Devices must not be "jail broken" or "rooted"* or have any software/firmware installedwhich is designed to gain access to functionality not intended to be exposed to the user.
- Users must not load pirated software or illegal content onto their devices.
- Applications must only be installed from official platform-owner approved sources. Installation of code from untrusted sources is forbidden. If you are unsure if an application is from an approved source contact Radiant Cash Management Services Pvt. Ltd. IT Department.
- Devices must be kept up to date with manufacturer or network provided patches. Asa minimum patches should be checked for weekly and applied at least once a month.
- Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with corporate policy.
- Devices must be encrypted in line with Radiant Cash Management Services Pvt. Ltd.'s compliance standards.

- Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify Radiant Cash Management Services Pvt. Ltd. IT immediately.
- The above requirements will be checked regularly and should a device be noncompliant that may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.
- The user is responsible for the backup of their personal data and the company will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.
- Users must not use corporate workstations to backup or synchronize device content suchas media files, unless such content is required for legitimate business purposes.
- *To jailbreak/root a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.

16.3.3 Actions which may result in a full or partial wipe of the device, orother interaction by IT

1. A device is jail broken/rooted
2. A device contains an app known to contain security vulnerability (if not removed within agiven time-frame after informing the user)
3. A device is lost or stolen
4. A user has exceeded the maximum number of failed password attempts

16.3.4 Use of particular applications which have access to corporate data

1. Network storage solutions: Radiant Cash Management Services Pvt. Ltd supports the use ofthe following storage solutions in SSD, SAN and also Backup Drives.
2. The use of solutions other than the above will lead to a compliance breach and the lossof access to the corporate network for the user.

16.4 Mobile Control

BYOD is today's reality; we embrace these devices in order to see the productivity gains, efficiencies, and innovations they bring to a mobile workforce. But we have the right solutions in place, we use OEM supplied MDM-Sophos Mobile Control (MDM), it is easy and cost-effective to secure end points, their mobile and web access, and our business data to subscribe for BYOD please get in touch with IT Department.

17 HR Recruitment policy

17.1 Objective:

- To streamline the Recruitment process in all the verticals of the company.
- To ensure that we always hire the Right people forth Right job at the Right time.
- To enable HR to initiate the hiring process at any point of time during theyear.

17.2 Scope:

This policy is applicable to all vacant positions across the functions,levels and hierarchy.

17.3 Recruitment Quality Norm

While recruiting a candidate for any role, position, level, function, it should always be ensured that there is no compromise on the quality of people, we hire. Besides checking the presence of role specific key competencies and the behavioral attributes required to perform a job, few basic eligibility criteria should be considered, even before a candidate is called for the initial rounds of interview:

- Academic Qualification: prescribed qualification should be followed.The competency requirement for various posts is in Annexure I.
- Computer proficiency: All the short listed candidates should be run through aprofessional test (typing, Excel, communication and any other skills that maybe required to test). Candidates qualifying this test would be eligible for the next rounds of interview.
- Reference Check: Reference check is must for all recruitments across the country and HR should always ensure that reference check is done before extending the job offer to a selected candidate

17.4 Recruitment Sources

Radiant will be using various recruitment sources in order to ensure that the vacancies are filled with the most suitable person available in a cost effective and timely manner.
The following sources will be used to recruit the candidates:

a) **Advertising in News papers**
   Prior permission required from CMD/Dir HR & Admin to publish advertisement in the newspapers. Generally profiles which are not available in the regular job portals can be recommended for Newspaper advertisement.
b) **Job Portals**
   Candidates can be pooled for selection by posting jobs in the paid jobportal as well as the free job portals like Quikr, Sulekha, and Olx etc.
c) **Referrals**
   Candidates referred by employees will be scrutinized and tested according tothe company policy. No compromise will be made for referral candidates in terms of competency and skills required for particular vacancy.

d) Walk – Ins

Candidates can walk in directly for any of the vacancies andthereafter regular testing and interviews will be followed.

17.5 Recruitment Approval Matrix:

Any recruitment across the organization, at any level/function has to be approvedby the concerned authorities as specified in the matrix below:

Levels	Designation	Interviewing authority	
		Preliminary	Final
Senior Management	Head, Director, COO, CEO,GM, AGM	CMD	CMD
Middle Management	Manager, Deputy Manager, Asst Manager	HR	CMD/Dir. HR
Lower Management	Associate, Assistants, Executives, Admin	HR	Dir HR

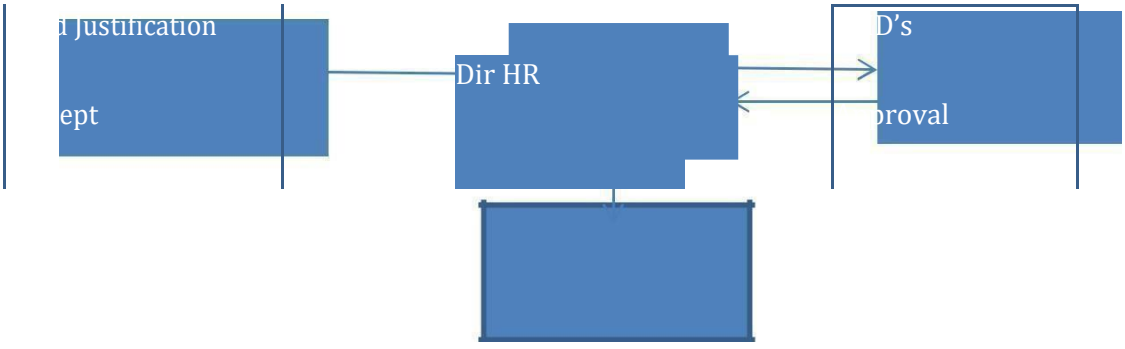
17.6 Compensation Proposals, Negotiation & issuing the offer letters:

Based on the salary slab in Annexure- III approved by the managementHR prepares the compensation proposals. HR sends the offer letter duly approved & signed by theconcerned authority, in the format pre-approved.

17.7 Requisition for Staff:

The HR co-ordinate's the recruiting process at Chennai. The following procedure is followed while recruiting a candidate. A requisition should be forwarded in the format given in Annexure II by email for recruitment of staff, to the HR section in order to initiate the recruitment process.

Phase – I : Pre - Selection



- Need justification should contain the detailed job description / job profileof the proposed vacancy.
- The core competencies and the minimum academic qualification required for thepost are to be specified clearly.
- If the post requires previous experience, this should be specifically statedfor how many years and from what type of organization
- The requisition should also mention the name of the section where s/he willbe absorbed and for what period. The amount of salary proposed may be given.
- Any other relevant information justifying the recruitment.
- The requisition should be made by the designated person responsible inthis regard.

17.8 Phase – II: Selection Process

Wherever necessary, Panel Interview may also be conducted, in which the Dept Head,HR and the technical representative should be present.

17.9 Joining & Orientation of New Staff:

The selected candidate should join the service on the agreed day and should officially inform her/his joining date. Services of an employee shall be deemed to commence from the working day on which he/she reports for duty/job. On joining the new employee is required to furnish the following documents:

- Reference Letter
- Resume
- Address Proof
- ID Proof
- Salary Certificate / Pay Slip (TDS Statement) from previous employer
- Relieving letter – from previous employer, if working

Proof of qualifications (Certificates / Mark sheets)The HR section will complete the following:

- Individual file will be created with all the relevant documents ofthe new appointee.
- Employment letter will be issued.
- Application for ESI, PF and Salary Account will be given.
- Identity card will be issued after one month from date of joining.
- Access card (wherever applicable) will be given after one week fromdate of joining.
- Uniform will be issued after completion of probation period.
- IS policy of the company explained and terms and conditions accepted?
- Induction training on IS policy.

17.10 Induction Training

The Purpose of the induction training is to make a new employee familiarize with the work processes and make him/her feel comfortable in the new set up. Induction will be for one day, either on the first day of the employment or as soon as possible. Where a group of employees join within the space of a few days, efforts will be made to hold induction in groups. In some cases, induction may involve a visit to other locations where Radiant has offices as well.

a) The induction training will generally involve:
b) Organizational history and background overview
c) Organization overview and structure
d) Briefing Timings, attendance system, Absenteeism and lateness
e) Departmental structure and interfaces
f) Who's who (names, roles, responsibilities)
g) Other sites and locations
h) Dress codes & Discipline procedures
i) Training and development
j) Information Security policy of the company (ISMS)

17.11 Probation

The purpose of the probation period is to allow both Radiant and the employeesufficient time to assess each other.

- All employees shall be under probation for the initial period of six months from the date of such engagements. The period of probation may be extended by a period of another 6 months at the discretion of management. Management will review the probation after 1 month of services and if find satisfactory, may reducethe probation period. The probation period is not linked to salary.
- At any time during the period of probation (including extension, if any), or at the end of such periods, the contract may be terminated without notice and without assigning any reason.
- The employee will be liable to ESI/PF deductions only after he is confirmedas a permanent staff.

17.12 Transfer

An employee is liable to be transferred to any other division, activity or geographicallocation of this company or any of its associates in present or come in existence in future. Insuch an eventuality, the employee shall be governed by terms and conditions and theremuneration as applicable to such new place to which his/her service may be temporarily or permanently transferred. Therefore, he/she will not be entitled to any additional compensation. In case the employee fails to report for duties at the transferred place, the management will be within its right and may draw a presumption that you have abandonedthe services on your accord and this contract will be terminated without any notice or salary in lieu of notice.

17.13 Resignation or Leaving the Company

An employee is required to give one month notice before he/she leaves the company. The notice period may be reduced at the discretion of the management which will be governed by the ability of the section in which he/she is working to find a suitable replacement. One month salary will be retained if adequate notice is not given.

Based on The role of the employee the software user access rights, Domain access for files,Firewall, email ID, MDM will be denied one day prior to the reliving date.
The IT Assets (Laptops, Mobiles, and Internet Dongles) needs to be surrendered on the Last working day to the IT department and requisite no dues email to be obtained.

18 IT Asset Management

18.1 Objective:

IT Asset Management is an important business practice that involves maintaining an accurate inventory, licensing information, maintenance, and protection of hardware and software assets utilized by RCMS.
Understanding what IT assets are deployed in RCMS environment will help optimize the use of IT assets throughout the company.

This document provides guidance on the steps that can be taken to protect IT systems. Information Security Program addresses the following areas:

- IT ASSET PLANNING and Acquisition
- IT Hardware Asset Control
- IT Software Asset Control
- Configuration Management and Change Control

18.2 IT Asset Planning and Acquisition

Planning:
Certain activities/events may trigger acquisition and/or disposition of IT Assets, such as:
Scheduled asset acquisitions, conducted in accordance with the Information Technology Plan.
Receiving an IT User access/Revoke Form due to an unplanned event.

IT team will review each IT User access/Revoke Form which shall be submitted to the functional superiors for budget approval.

Acquisition:
RCMS personnel shall use the IT User access/Revoke Form to request new or replacement IT Assets. This form shall be approved by the appropriate department manager before being submitted to IT team.

The same form shall be used for assets being relocated within RCMS or disposed of due to obsolescence.
IT team may receive all the physical (Computer, Laptop, Network devices etc...) and non-physical (Software, Applications etc...) Assets directly from vendor.

IT team will inspect and test assets for performance and capability prior to acceptance before implementing it into production.

18.3 IT Asset Management Policies and Procedures

IT users, to include, employees, business partners, and contract personnel shall not removeIT assets supplied by Radiant or its business partners from company premises, except under the following conditions.

IT assets assigned to employees, which may include laptop computers and Mobile / Handheld devices, may be removed from agency or company premises as deemed acceptable by the agency for the following reasons only:

- Tele-working
- Field work that is part of an assigned position
- Exceptions to this policy must be documented in writing and approved by the employee'ssupervisor and by the IT Head. Documentation of exceptions shall include:
- The business or technical justification;
- The scope of the exception, including quantification and duration (not toexceed one year);
- A description of all risks associated with the exception;
- Identification of controls to mitigate the risks; and
- Identification of any unmitigated risks associated with the exception.

IT users are responsible for safeguarding any IT assets they remove from the company's premises, including keeping these assets under their direct physical control wheneverpossible, and physically securing the assets (i.e., by means of lock and key) when they are not under the IT users direct physical control.

IT users must immediately report loss or theft of any assigned IT assets to their supervisor within 24 hours of a known occurrence.

Unless stated otherwise within agency or facility policy, IT users are not allowed to bring personal IT assets into work locations that personal IT assets may not be connected to the RCMS network.

In general, connection of personal IT assets to networks provided by RCMS or businesspartner for guest or public access is allowed if deemed acceptable by the company.

- Exceptions to this policy must be documented in writing and will be approved by the employee's supervisor and by the Head. Documentations of exceptions shall include:
- The business or technical justification;
- The scope of the exception, including quantification and duration (not toexceed one year);
- A description of all risks associated with the exception
- Identification of controls to mitigate the risks; and
- Identification of all unmitigated risks associated with the exception.

18.4 IT Software Asset Control:

1. IT users only use approved and appropriately licensed software by the Management.
2. Installation of software that is not approved or appropriately licensed IT assets areprohibited.
3. No less than annually, the CTO or designee will conduct an audit of software license distribution and reconciliation to verify and validate that all software used by Radiant has been appropriately licensed and approved.

18.5 Configuration Management and Change Control

All changes to IT assets used by Radiant will be made in accordance with thefollowing steps:

- Initiate change request
- Review and approve change
- Build and test change
- Create and document back up/back out plan
- Implement change
- Document change

19 IT Risk Assessment and Methodology

19.1 Objective:

Risk management is the process of identifying vulnerabilities and threats to theinformation resources used by an organization in achieving business objectives, and deciding what counter measures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization.

19.2 Definitions of IT risk

ISO
IT risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of occurrence of an event and its consequence.

19.3 Categories of IT Risk

19.3.1 Natural risks

- Floods
- Earthquakes
- Storms
- Other natural calamities.

19.3.2 Man-made risks

Terrorist attacks can be appropriately rated by determining past instancesof such attacks in the given location, or studying the prevalent socio-political.
Cyber-attacks or employee behavior is based on occurrence of previous incidents, as well as the organization's current ethical, regulatory, and access and authorization policies under implementation

19.3.3 Technology risks

- IT component or device failure
- Server failure
- Failure desktop terminal
- spam
- viruses
- malicious attacks
- threats
- vulnerabilities
- exposures
- hacking

19.4 Importance of protecting IT data and IT assets

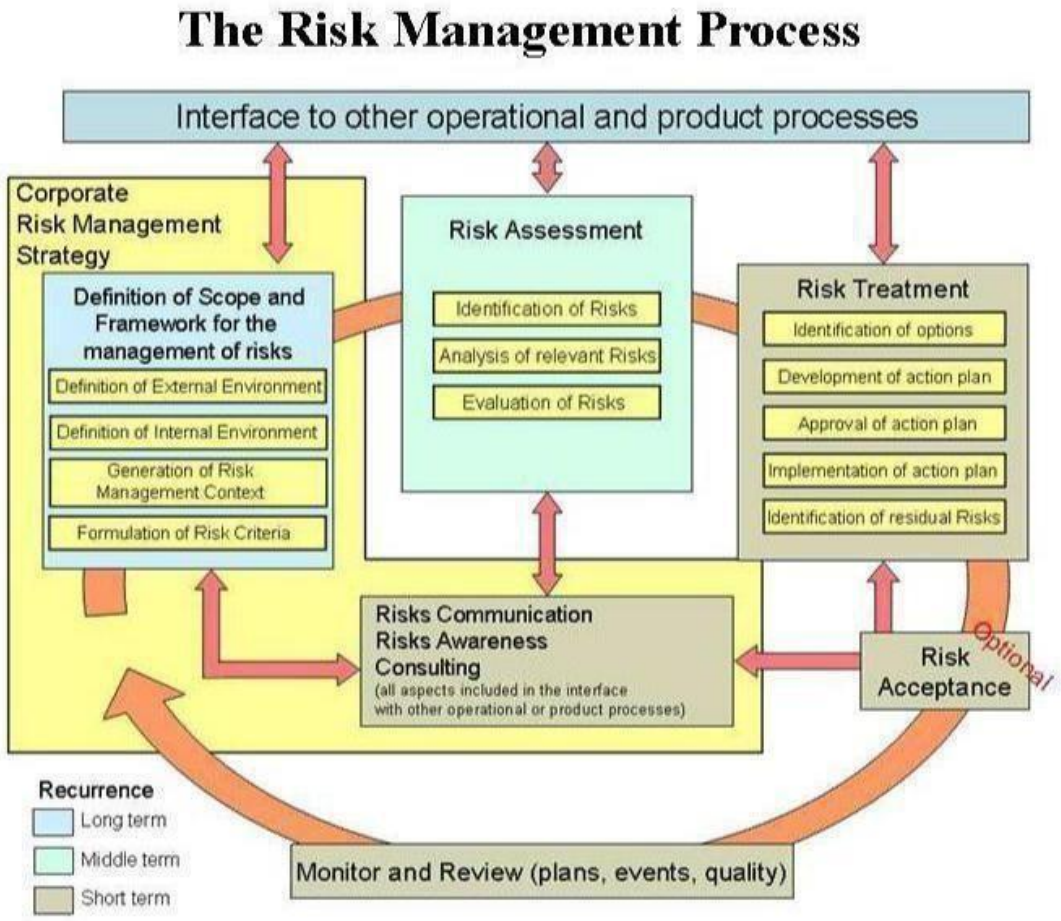
Online security is vital to protect our virtual assets (electronic data) and IT system. Data protection and a secure online presence will build our customers' trust and help us meet legal obligations, such as privacy laws.

19.5 Security threats for IT data and IT assets (RA)

Malicious software or malware spreads worms, viruses, Trojans and spyware through:email attachments; files on removable storage devices and visits to infected websites.

1. Hackers use malware to control computer remotely, steal or destroy information(including passwords), corrupt hardware and software, or spread malware.
2. Spam or junk emails promote fake or non-existent products and services such as get-rich-quick schemes, false prize or lottery wins, or fraudulent and poor-quality goods
3. Cookies track website visits and can build a profile of online interestsand buying habits, and report these details to third parties.
4. Online scams and fraudulent websites or emails are designed to trick into revealing sensitive information including bank account details, passwords or credit card numbers.
5. Phishing uses fraudulent emails claiming to be from a trusted sender, such as a bank, to 'fish' for information.

6. Pharming occurs when a hacker infects a computer with a malicious code anddirects to a fake website. Both are used for online identity theft or cyber fraud.



19.6 IT risk management

The establishment, maintenance and continuous update of an information security policies and procedures will provide a strong indication for a company in using a systematic approach for the identification, assessment and management of information security risks. The main goal of implementing IS policies and procedures is to minimize IT related risks and ensure business continuity by pro-actively limiting the impact of a security breach.

Different methodologies have been proposed to manage IT risks, each of them divided inprocesses and steps.

19.6.1 Identification & Authentication of Employees

1. We have implemented access control to enable the information resources in ourorganization.
2. We have ensured that all our employees are authorized to access our information system resources with unique user ID and password that our information system could identify.
3. Employees will be advised to change their password on first login.
4. The password must contain eight characters without any space in between
5. Those eight characters must include alphabets (upper and lower case);numeric and a special character.
6. Employees will be advised to change their password every forty five days. Radiant has incorporated password security control such that previous passwordhistory can't be repeated to use at any attempt of changing the password
7. Password will be disabled after thirty days of inactivity.
8. In case of an employee's termination his/her existing user's ID and access codewill become invalid.

19.6.2 Information Classification

a) Every data related to our business process are logically and physicallyclassified and labelled in order rate the risk critically.
b) Basically the data related to our business process are broadly segregated and labelled into three categories: Customer Confidential; Corporate Confidential and Public.
c) These data are highly secured which can be accessed only bythe authorized personnel.
d) Copying archiving and dumping of any data is authorized by the respectivepersonnel and treated with same level of security as the original data.
e) The business data, either hardcopy or softcopy will be treated with same level ofsecurity.
f) Electronic Transportable media such as floppies, CDs, DVDs, Tapes, etc are encrypted by using approved cryptographic algorithms and key length (AES128bit) and security protocols like Entrust, WinZip, Secure PDF and PGP.

19.6.3 Secure Disposal

- Once the requirement of a document is over we will securely dispose itwhich cannot be used or identified in future.
- Documents in paper and electronic media files will be trashed by using shredder.
- Data stored on the PCs and file servers should be retained as perrecord retention plan as instructed by the client.

19.6.4 Physical Security

a) We instruct our employees that PCs and notebook computers must not beleft unattended for a long-time.
b) Access to the data center is restricted to the authorized personnel only.
c) In case, third parties want to access our data center our authorized personnelwill accompany them.
d) IT equipment is under surveillance.
e) Physical access control mechanism like electronic or combination lockhas been implemented in order to control the access of data center.
f) Our data center is fitted with smoke/fire detectors and fire extinguishing equipment which is set to automatic operation.
g) Fire detection and prevention equipment are tested twice a year.
h) SNMP UPS is installed in every protection server which will protect theserver against power surges that will be tested every three months.

19.6.5 Software Security

- Anti-virus software has been installed on all PCs and serversand updated periodically.
- Firewall equipment has been implemented in all our systems to prevent unauthorized access to the PCs connected to the internet.
- Uncertified freeware and shareware are not allowed to download or install by users.
- Removable mass storage media and USB port are not permitted. If any
- Employee violates the policy disciplinary actions will be taken against them.
- If removable devices are required it must be used it must beapproved and documented.

20 Vulnerability Management Process

20.1 Introduction

Vulnerability is defined as ***"A weakness of an asset or group of assets that can beexploited by one or more threats"***

Vulnerability management is the process in which vulnerabilities in IT are identified and therisks of these vulnerabilities are evaluated. This evaluation leads to correcting the vulnerabilities and removing the risk or a formal risk acceptance by the management of an organization (e.g. in case the impact of an attack would be low or the cost of correction does not outweigh possible damages to the organization).

The term vulnerability management is often confused with vulnerability scanning. Despite the fact both are related, there is an important difference between the two. Vulnerability scanning consists of using a computer program to identify vulnerabilities in networks, computer infrastructure or applications. Vulnerability management is the process surrounding vulnerability scanning, also taking into account other aspects such as risk acceptance, remediation etc.

20.2 Why Vulnerability Management is required?

The increasing growth of cyber-crime and the associated risks are forcing most organizations to focus more attention on information security. A vulnerability managementprocess should be part of an organization's effort to control information security risks. Thisprocess will allow an organization to obtain a continuous overview of vulnerabilities in their IT environment and the risks associated with them. Only by identifying and mitigating vulnerabilities in the IT environment can an organization prevent attackers from penetrating their networks and stealing information.

20.3 Vulnerability Scanners

As vulnerability management is the process surrounding vulnerability scanning, it is important to understand how vulnerability scans are performed and what tools that are available. Today, the level of technical expertise required to operate a vulnerability scanning tool is low.

Several vendors provide a variety of technical solutions, with different deployment options.

These deployment options include standalone, managed services or even software as a service (SaaS). We make use of McAfee, Rapid 7, Tenable Network Security as well as a few open source projects.

It's recommended an organization thoroughly tests vulnerability scanning products before deciding which solution best meets the requirements of the organization. Attention should be paid to the fact that scanning a single box with multiple products using their default settings could produce very different results. No matter which vulnerability scanning solution is selected, it's important to properly configure and tune scans to limit the amount of false positives in the scan results.

Weekly Network Scan:

With effect of 1st May of 2018, it is decided that the network teams are required to conduct a vulnerability assessment scan of all of their networked computing devices on a weekly basis. The network vulnerability assessment scan is carried out for reviewing and analyzing the computer network for possible security vulnerabilities and loopholes.

Our network admin evaluate the security architecture and defense of a network against possible vulnerabilities and threats during the scan which will be performed on every weekend. At the completion of the above vulnerability assessments, all discovered vulnerabilities must be documented and remediated.
The admin team will take the high/critical risks analyzed during the scan and the loopholesand threats will be fixed with high significance. Units must keep a record of all assessments and be able to produce reports if requested by management, the Information Security Officer or an external auditor. Scans shall be performed during hours appropriate to the business needs of the entity and to minimize disruption to normal business functions.

Monthly Vulnerability Scan:

With effect 1st May of 2018, we have implemented and incorporated vulnerability management policies and controls required to maintain high levels of network security in a diverse IT environment and it is required to perform the vulnerability scan for both network and internal web applications on monthly basis.

We use OWASP and Burp Suite tools aimed at making web application security "visible", so that our organization can make informed decisions about application security risks.

We believe that this will list the most critical web application security flaws that we utilizeand identify Critical Web Application Security Vulnerabilities.

The Vulnerability scan on web based applications will be performed on basis of thefollowing criteria:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entity (XXE)
- Broken Access Control
- Security Misconfiguration
- cross Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring

The security team will perform the scans in monthly and quarterly frequency with the above mentioned tool and generates the report on the vulnerabilities identified across all assets. The reports will be reviewed and forwarded to the Admin Team.

Upon receipt of the reports, if the admin team found any suspicious threats, they will be responsible to clear within the service level of one day.
Any findings that need to be mitigated later than the service level must be approved by the management and documented as exceptions. These are to be reviewed and approved by the IT manager and director of security.

Admin Team will maintain the vulnerability management solution for generation of reports, and will monitor the vulnerability posture of the company.

20.4 Associated risks

There is some risk involved with vulnerability management or more specifically, vulnerability scanning. Since vulnerability scanning typically involves sending a large number of packets to systems, they might sometimes trigger unusual effects such as – for example - disrupting network equipment. However, since vulnerability scanning is mainly limited to scanning and not exploiting, risks are minimal. In order to cover these risks, it's always important to inform various stakeholders within your organization when vulnerability scanning is taking place.

20.5 Objective

The main objective of a vulnerability management process is to detect and remediatevulnerabilities in a timely fashion. Many organizations do not frequently perform vulnerability scans in their environment. They perform scans on a quarterly or annual basis which only provides a snapshot at that point in time.
Any vulnerability not detected after a schedule scan takes place, will only be detected at thenext scheduled scan. This could leave systems vulnerable for a long period of time. When implementing a vulnerability management process, regular scans should be scheduled to reduce the exposure time.

Continuous vulnerability management regular scanning ensures new vulnerabilities are detected in a timely manner; allow them to be remediated faster. Having this process in place greatly reduces the risks an organization is facing.

20.6 Vulnerability Management Process: Step-by-Step

A vulnerability management process consists of five phases:

- Preparation
- Vulnerability scan
- Define remediating actions
- Implement remediating actions
- Rescan

20.7 Preparation

The preparation phase is the first phase in a vulnerability management process. To preventbeing overwhelmed by thousands of vulnerabilities identified in the first scans, it is recommended to start with a small scope. This can be achieved by starting out with a small number of systems or by limiting the number of vulnerabilities identified by the vulnerability scanner (e.g. only scan for vulnerabilities for which a known exploit granting remote access exists).

The first step is to define the scope of the vulnerability management process. It is important to obtain an agreement which systems will be included or excluded from the vulnerability management process. Besides the in scope systems, an organization should also determine the type of scans. Possibilities can include either an external scan performed from the perspective of an external attacker on the internet or an internal scan from the perspective of an attacker on the internal network. Both types of scans can be either unauthenticated or authenticated scanning.

An external scan provides an overview of security vulnerabilities which are visible from outside a network, taking into account all security layers on the network between the scanner machine and the target system. This controls can include includes network firewalls, intrusion detection systems, (web) application firewalls as well as any host based security controls which are present on the target system. The results of an external scan give an indication on the correct configuration of the network security controls between the scanner and the target system.

A scan performed from the internal network, provides an overview of vulnerabilities whichare visible from the local network, taking into account host based security controls that are present on the target system. By performing an internal scan of each component in architecture, the results can provide information on how well each layer is secured. ("Defense in-depth")

Both external and internal scans can be executed using authentication. In those cases, the scanning technology will authenticate itself to the target system using valid credentials in order to extract additional information from the system that would otherwise not be accessible. This information includes specific security configurations and software patch levels. Using authenticated scanning will result in more accurate and complete vulnerability scanning reports.

While each scan type has their own advantages, vulnerability management processes usually use a combination of both. Security officers should in the long term work towards performing internal scans on every component of the infrastructure.

When determining the scope of systems to include in the vulnerability management process, it is usually not feasible to include everything in the first iteration of vulnerability scanning. The rule of thumb should be to start small. This will ensure the number ofvulnerabilities discovered will be manageable. A risk based approach should be used to determine the scope for an initial vulnerability scan. There are several ways to approach this. Some organizations see external threats as the biggest risk and would start with a scope consisting of internet facing systems. Other organizations think their company information is at risk and will start with a limited scope of systems containing such information.

When implementing a vulnerability management process, it is recommended to start out with a small scope. The small scope will allow the stakeholders involved to focus on implementing the process and prevent them from being overwhelmed with vulnerability information from hundreds or thousands of systems.

Once the scope has been determined, the security officer should inform relevant asset owners in the organization. These people are accountable or responsible for the systems. The asset owner is responsible for identifying remediating actions to mitigate the identifiedvulnerabilities. In most situations, asset owners should make these decisions after examining the recommendations and risk assessment prepared by the security officer. It is important to obtain buy-in from asset owners within an organization. It is recommended toinform them about upcoming vulnerability scans. The objectives of the vulnerability management process should be explained to them in detail; including how this process affects the systems they are responsible for. Additionally what their responsibilities are in the whole process should be explained. Depending on system criticality, asset owners may have specific requirements such as not scanning production systems outside of maintenance windows or only performing scans during business hours. Depending on the organization and the mandate of the security officer, it may be necessary to obtain formal approval from each asset owners before performing vulnerability scans.

Informing IT, specifically teams managing firewalls, IDS or other security monitoring systems, should be part of any vulnerability management process. The alerting on such systems is often triggered by vulnerability scanning tools, so it's important to ensure these teams are aware of the vulnerability scans.

The last step of the preparation phase consists of planning the vulnerability scans. Depending on the scan configuration which includes the number of vulnerability checks, authentication scan type, and applications installed on the target, a vulnerability scan against a single IP address can take between a few minutes to a few hours. In case it is unclear how long a certain scan could last, it is recommended to perform a test scan on a similar test environment. This will provide an estimate on long these scans will take and their impact on the network.

The risk appetite of the organization plays an important role in the vulnerability management process. If an organization is willing to ignore some risks (e.g. due to limited resources being available), the scope of the vulnerability management process can stay limited, e.g. only high risks for which known exploits exist. Organizations that want to obtain a clear understanding of vulnerability in their environment and their associated risks should, with iteration of the process, increase the scope and grow towards their desired scope.

20.8 Initial vulnerability scan

Once the preparation phase is complete, the next phase of the process begins and the initialvulnerability scans are performed. Any issues which occur during the scans, for example systems becoming unavailable or poor application response, should be recorded since this may happen again in the future. In this case, actions may be defined to reduce the impact of future scans on the stability or performance of the target systems.

Most vulnerability scanning tools offer a wide range of reporting options to visualize scan results. It is necessary to use them to create a various number of reports. Management and the security officer will be interested in the risk the organization is currently facing, this risk includes number of vulnerabilities detected and the severity/risk rating of the identified vulnerabilities. Asset owners will want to obtain an overview of vulnerabilities inthe systems they are responsible for. The IT department will want an overview (per technology) of technical information about detected vulnerabilities as well as recommendations for mitigation and improvement.

20.9 Remediation phase

In the next phase, the asset owners, with the cooperation of the security officer and the IT department, will define remediating actions. The security officer will analyze the vulnerabilities, determine the associated risks and will provide input on risk remediation. The IT department will analyze the vulnerabilities from a technical perspective and answer questions such as if patches are available or whether the configuration can be hardened? The IT department recommendation also includes the feasibility of the possible remediating action such as whether installing a certain patch will result in the application no longer is supported by the vendor. In order to ensure remediation is given sufficient priority the security officer should set clear deadlines when the remediating actions will be implemented.

Asset owners should include a timeline in their action plan indicating when these remediating actions will be implemented. The remediation timeframe should be in line with the level of risk detected. This timeframe will be different for each organization since the reaction speed will depend greatly on the risk appetite of the organization.

If short term remediation is not possible, compensating controls should be identified in order to mitigate/remove the risk without correcting the vulnerability. Such compensating controls could include restricting network access to the vulnerable service, virtual patching, etc.

In case asset owners decide to accept the risk, it should be documented through a risk acceptance process. A risk acceptance or waiver process is a formal process in which an exception to the security policies can be requested. This request is analyzed with regards torisks the organization would be exposed to if the exception is granted. If possible, compensating controls to remediate these risks are proposed. In the final step of a risk waiver process, the asset owner analyses the risks, whether or not compensating controls can be foreseen .This allows the asset owner to make thoughtful decisions with regards to accepting the risk. The ability to signoff is determined based on the level of risk. Usually high risks can only be accepted by management of an organization, whereas small risks canbe accepted by asset owners. Risk waivers should always be limited in time to ensure these risks are revaluated on a regular basis (e.g. annually).

20.10 Implement remediating actions

The planned remediating actions should be executed in line with the agreed timeframes. Ifa problem occurs with implemented remediation, it should be recorded. Alternative actionsshould be defined by the asset owner based on recommendations by the security officer and the IT department. These new or other remediating actions should then beimplemented. The security officer should track the status of the remediating actions.

20.11 Rescan

Once vulnerability is remediated, a rescan has to be scheduled to verify the remediating actions have been implemented. This scan will be performed using the same vulnerability scanning tools and identical configuration settings as the initial scan. This step is very important to prevent inaccurate results due to configuration errors. Typically a rescan is scheduled after the deadline for implementing remediating actions.

For these scans, the same types of reports generated during the initial scan are created. For follow-up, management and asset owners will be interested to know whether the remediating actions have been effectively implemented and whether any residual risk remains. The IT department will be interested in how effective the remediating actions have been implemented.

The next step is an agreement between asset owners and the security officer on how often such scans will be scheduled. This timeframe should take into account the risk appetite of the organization, as well as the capability of the organization to remediate identified vulnerabilities. In order to establish a mature vulnerability management process, it is recommended to schedule scans frequently, typically on a weekly or monthly basis. This will ensure rapid detection of vulnerabilities, allowing the organization to determine and deploy mitigating controls in a timely fashion.

Correcting vulnerabilities from the initial scan provide good insight into the ability of the (IT) organization to handle requests. Furthermore, lessons learned during the execution of the process should be used to re-evaluate and improve the vulnerability managementprocess.

20.12 Conclusions

Without a vulnerability management process in place, the management of an organization is blind to risks related to the security of the IT infrastructure. Implementing a vulnerability management process is all about managing risk. By having a well-defined process in place, an organization can obtain a continuous view of the risk associated with the presence of security vulnerabilities in its IT systems. This allows management to take well-advised decisions with regards to remediating actions that could be implemented to reduce the risks. In short, any organization that wants to obtain an understanding of the security risks they are facing due to the technology they are using should implement a vulnerability management process.

However, introducing a new vulnerability management process within an organization can also be challenging. In order to ensure a successful vulnerability management program, attention should be paid to a number of aspects. First of all roles and responsibilities should be clearly assigned. Ensure all stakeholders within the organization know what to expect. Then select a vulnerability scanning technology that suits the needs of your organization. Sufficient attention should be paid to the configuration and fine tuning of the vulnerability scanner technology. Finally, when starting out with vulnerability management, it is recommended to limit the scope of the initial vulnerability scans. This prevents initial scans that result in tens of thousands of vulnerabilities.

A better approach would be to only select a limited set of vulnerabilities or only those that are marked as “high risk” by the vulnerability scanner tool.

21 Policy and Procedure: Office Security

21.1 Policy Statement

To ensure that the environment is kept safe everyone who accesses the office must be aware of how they can contribute towards ensuring that the office is a safe place to be. The principle objective is to ensure that unwanted people who would seek to cause harm to individuals or steal property are stopped from entering the building:

21.2 Normal Working Hours (Monday to Saturday 09:00 to 19:00)

- The principle access to the Office for visitors should be through the main entrance doors into the main reception
- No visitors should be allowed to access the building from the rear service access or emergency accesses
- All visitors who are to go beyond the ground floor public areas must be booked in at reception (this is also required for health and safety reasons)
- Members of the public visiting the Building must only be given access to the public areas unless accompanied by a member of staff

- No one should allow anyone who they are unfamiliar with access through any security locked doors or lifts without first checking their identity or purpose
- All security doors should be kept secure so that access is only via a security swipecard. No doors leading to the private areas of the building should be left unbolted, unlocked, or propped open. This also applies to emergency exit doors
- All staff can enter and stay in the building during normal working hours which are09:00 to 19:00 hours

21.3 Visitors check in

- All Visitors must arrive at a designated Check-In entrance (the main reception desk in most locations). All Visitors must present government-issue photo identification at time of Check-In a Visitor cannot sponsor another Visitor.

21.4 Visitor Badges

Visitor Badges must be worn at all time. Visitors requiring access to areas controlled by swipe card access locks should arrange temporary cards with their sponsor.

21.5 Photographs and Cameras

Visitors are not permitted to take photographs inside of premises, unless discussed specifically with sponsoring employees. For instance, photographs are sometimes required for documentation purposes. If employees have any questions about the suitability of photographs, they should consult the Human Resources Department. Dedicated cameras are not permitted onsite. Cell phones and laptops equipped with cameras are permitted, but as previously stated photography are not permitted without permission.

21.6 Information Disclosure

Visitors should not request information that does not pertain to their visit or the work being performed. Confidential or otherwise inappropriate nature, requests for corporate documents, customer information, financial projections, comments on any matter currentlyunder litigation, future products or future corporate direction, or requests for information or statements in the name of the company will be reported to the Office of the CSO.

21.7 Check-Out

Visitors will check out at the same station where they arrived. All Visitor electronics will be checked out individually as described in the Laptop, Computer and related equipment Check-In/ Check-out Procedure. The checked out Visitor will be taken off the On-Premise List.

21.8 Exit Inspection

Visitors may be subject to a brief search of their laptop bags or other luggage as they exit the premise.

22 Roles and Responsibilities

22.1 Chief Technology Officer (or designee)

- Interpret the policy and standards.
- Ensure policy and standards content is kept current.
- Recommend updates to the policy and related standards in response to changes intechnology, service delivery, or other challenges to the security environment.
- Review Bank IS for compliance with the security policy and standards.
- Develop an escalation process for compliance.
- Help Organization to understand how to comply with the policy and standards.
- Monitor annual compliance by Branches, Regions, and Departments.
- Approve deviations from the standard.
- Conduct audits of offices according to its audit schedule.
- Assign responsibility for IT security to an individual or group with the appropriate training and background to administer those functions and ensure that the individual or group has proper authority to install, monitor, and enforce IT security standards and procedures.
- Ensure IT security policies, procedures, and other documents necessary forthe
- Security program are developed, implemented, maintained, and tested.
- Ensure all Staff/ users of IT resources are trained to follow securitypolicies, standards, and procedures.
- Oversee the company's information technology security program and ensure compliance with the security policy and these IT security standards.

22.2 Technology Services Board / Management

1. Review and approve major policy changes.

22.3 National Heads/ Regional Heads / Branch Heads andDepartment Heads

1. Maintain security of all managed networks such as the VPN, LAN and SoftwareApplication.
2. Design, establish, and maintain the shared IT infrastructure necessary to supportapplications and data within a trusted, branch/ office-wide environment.
3. Review office operations for compliance with the security policy and standards.
4. Help staff and employees understand how to comply with the policy and standards.
5. Conduct audits of offices according to its audit schedule.
6. Submit an annual, signed security verification letter.

24 CYBER SECURITY POLICY

24.1 Policy

A Cyber security policy is a written document in RCMS which outlines how to protect the data frompotential threats and how to handle the situation when they do occur.
The Policy must be updated regularly and In addition to that the Employee's need to be keptupdated on the company's security policies.

24.2 Overview

The Main role of this policy is to ensure that the RCMS will never have any inadequacy of security toany form of data and guarantee the clients, RCMS will never compromise when it comes to data confidentiality.

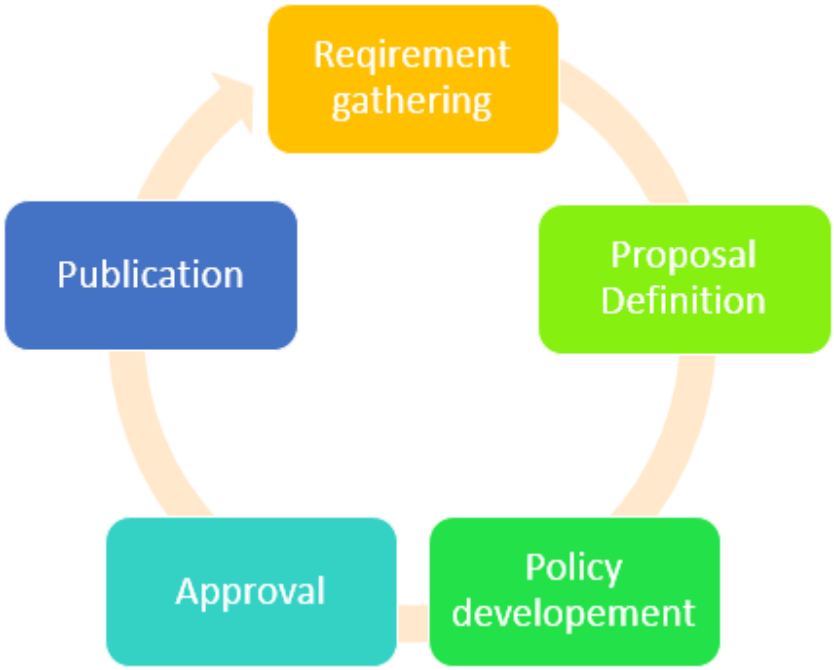
24.3 Scope

This policy applies to all RCMS employees and affiliates, including contractors. It addresses the policy and controls for confidential firm data that is at rest (including portable devices and removable media), data in motion (transmission security), and data standards and management.

24.4 Policy Makers

The policy comprises of collective operation of all RCMS personnel in structuring the rules which initiates their responsibility in holding the security of data that takes part as their work routine. Asingle sector of RCMS cannot propagate the policy as it must consider the whole of the employee's view in order to implement a transparent and feasible policy. During policy creating following entity typically involves;

a. **Board:** The members of the board render their advice to some form of a review ofpolicies in response to exceptional or abnormal running condition of business.
b. **IT Team:** The IT team usually a biggest consumers of the policy information, as theyinvolve in making standards around the usage of the computer system, especially in security controls.
c. **Legal Team:** This team ensures the legal points in the document and guides RCMS tomaintain their standards.
d. **HR Team:** HR team typically obtains a certified T&C certificate from each employee thatthey read and understand as per the stipulated policy. The HR team deals with reward and punishment related issues of employees to implement discipline.



24.5 Policy Audience

Security policy applies to all senior management, employees, stockholders, consultants, and service providers who use the company assets. The following figure gives an indication to RCMS that would need to read the security policy.

Otherwise stated, the security policy incorporates all employees, hardware, software, consultants, service provider who use company assets such as computer networks data information or any information that is perceived to be valuable to the business.

24.6 Policy Classification

RCMS typically has three policies: Initially they are drafted on paper and then they are implemented as an Employee's routine. Policy generally requires what must be done, rather than how it should be done. Security policies should be informative, regulative, and advisory in a broadmanner, generally, be subdivided into following categories as;

Physical security: It mandates what protection should be wielded to safeguard thephysical asset from both employees and management, applies to the prevail facilitiesincluding doors, entry point, surveillance, alarm, etc.

Personnel management: Responsible in guiding their employees as of how to conductor operate day to day business activities in a secure manner, for instance, password management, confidential information security, etc., applies to individual employees.

Hardware and software: It directs the administrator what type of technology to use and what and how network control should be configured and how it will be applied tosystem and network administrators.

24.7 Policy Audit

Security documents are living documents. Therefore, they must be updated at specific intervals in response to changing business and customer requirements. Once policies are well-established and ready to dictate typical operations, an audit will be performed by Third-parties or inside agencies tocompare existing practices to the intentions of policy. Security policy audits assist the company in understanding the level of threat and acting accordingly. Security audit's goal is to bring all the security policies closer as possible. Auditing is periodically performed to compare existing practicesagainst a security policy to substantiate or verify the effectiveness of security measures. Finally, the goal of a security audit is to provide the company with a verification of best practices already in place. A successful security audit accomplishes the following:
It compares your security policy with the actual practice in place.
It determines your exposure to threats from the inside.
It also determines the exposure of your RCMS from an outside attack.

24.8 Policy Enforcement

Enforcement of security policies ensures compliance with the principle and practices dictated by the company. Because the policy and procedure will not work if they are violated. Enforcement is arguably the most significant aspect of a company; it dissuades anyone from deliberately or accidentally violating the policies rules. System administrator level enforcement ensures proper maintenance and prevents privilege escalation and employee level enforcement sees to that, if thedaily working activities comply with the policy. However, there is proper balance maintained between positive and negative enforcement. The best employees that abide by rules are rewardedtime to time to increase their motivation and boost up their moral in positive enforcement. In negative enforcement, on the other hand, strict compliance of policies takes the form of threat to the employees.

24.9 Policy Awareness

Company employees are often perceived as “soft” target to be compromised, as the human elementsare the least predictable and easiest to exploit. Trusted employees either “disgruntle” or frame to provide valuable information of a company. Therefore, one of the most robust storage to combat this exposure of information by employees is “education.” When employees are duly able to understand that what should or shouldn’t give out confidential information, know the reason why the company internal are less likely to be vulnerable. A good security awareness program must be periodically performed and should include all the existing security policies that are mandated to becomplied from employees’ end. Moreover, awareness programs should also integrate communication and reminders to employees about what they should and shouldn’t reveal to Outsiders. In final words, security policy awareness training and education mitigate the threat ofinformation leakage.

25 DATA ENCRYPTION SECURITY POLICY

25.1 Purpose

The purpose of this document is to provide the RCMS organization with the information required toeffectively and efficiently plan, prepare and deploy encryption solutions in order to secure Legally/Contractually Restricted Information (Sensitive Data) (refer to RCMS – Data Access Policy).

In Worldwide any data can be protected at three different stages which can be at, **Data at rest** which includes the data residing on a wide variety of computer storage and electronic devices, such as network shares, backup storage, hard disk drives, CDs/DVDs, floppy disks, thumb drives, PDAs, smart phones and others, secondly **Data in motion** refers mainly to the data moving through the network and finally when the **Data in use** which includes the data on a computer which is being analyzed or worked on, including creation, retrieval, modification, deletion, saving and printing.

And in our Organization we have chosen the responsibility to protect the **Data at rest** in order to avoid information leakage in primary stage.

25.2 Scope

This information assurance policy applies to all our organization's workforce members who have contact or potentially may have contact with this organization's data, applications, and computing resources.

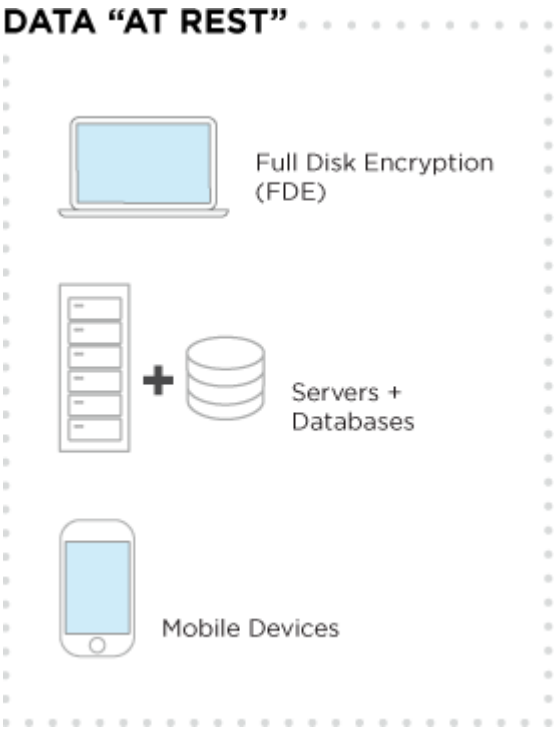
25.3 YUBIKEY

Data encryption at rest is a mandatory step toward data privacy, compliance, and data sovereignty.

We use YUBIKEY as the Encryption product to encrypt and decrypt the data which we protect. The YUBIKEY is managed by our Chief Executive Officer as he is the concerned person who has the key used in a storage encryption solution are secured and managed properly to support the security of the solution.

This process flow is been approved by our CEO and the same is been in effect from 2nd of November, 2018 and after several affirmation and validation the same will be documented and included in our IS policy on 31st of March, 2019 as per our review policy of IS policy is bi-annual, with the fulfillment and acceptance of our entire higher and superior officials and also to employeesconnecting to any RCMS workforce members and network domain to clear any snags found in- between of the process.

25.4 Logic Diagram



Extensive key management is planned and followed which includes secure key generation, use and storage. Initially YUBIKEY will be vaulted and the key for that vault will be in control of the CEO. If a third party want to access our hard disc then he must follow the steps stated below for accessing our data:

Initially the network/Linux admin must register his name and details in ledger before approaching the YUBIKEY.

Later the network/Linux admin needs to get the key for the vault where the YUBIKEY is been vaulted, by unlocking the vault he can able to access the YUBIKEY where 2 KEY's will be available, both serves the same role one is kept as backup key for the other.

Once after the insertion of the YUBIKEY into the system, it asks for 128 bit password to handle the hard disc, this 128 digit password is split up into 2 segments as 64 digits.

This first part of 64 digits password is been controlled by LINUX ADMIN and the second 64 digits is handled by NETWORK ADMIN.
After successful enrollment of this 128 segment the third party can access the hard disc without anyfurther delay.

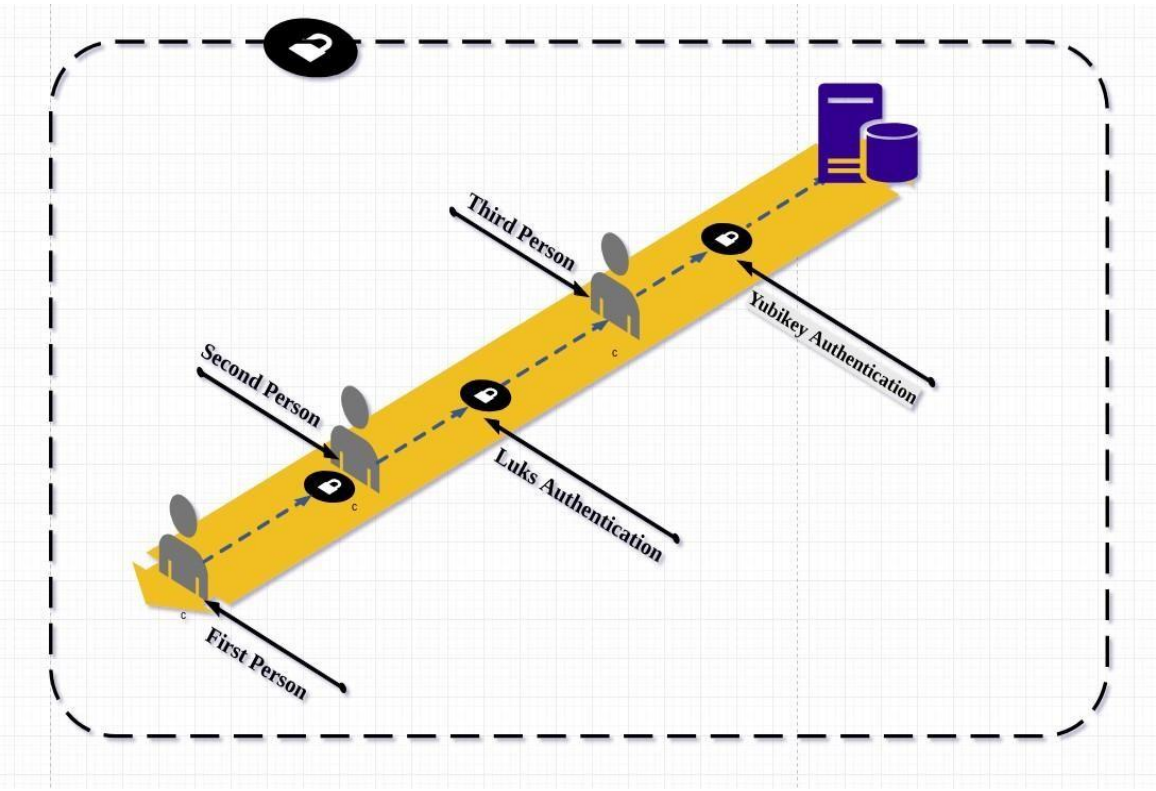


Fig: Structure representing hard disc access

After completion of the authentication process, the YUBIKEY is returned to the CEO and thenetwork/Linux admin should enroll the IN time of the YUBIKEY back to the vault in the ledger.

Network department will ensure that access to encryption keys is properly restricted.Authentication for each process is followed in order to gain access to keys (passwords, tokens, etc.).

25.5 Process flow

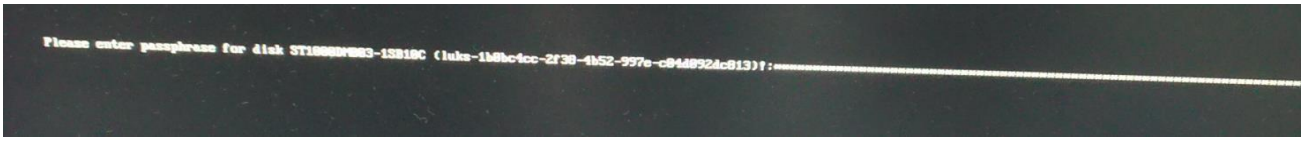
In order to access the hard disc, we are using 2 levels of authentication and they are (i) LUKS (ii)YUBIKEY **i.e.., LUKS-Primary authentication and YUBIKEY- Secondary authentication.**
LUKS-Primary authentication: To encrypt the server we utilize LUKS authentication and in order to access this we need 128 char to finish first level of authentication.

This 128 char is split into 2 segments and first 64 segments is handled by LINUX ADMIN and thesecond 64 segments is handled by NETWORK ADMIN

YUBIKEY- Secondary authentication: This YUBIKEY will be kept and handled by MANAGERLEVEL authority. We need to finish the YUBIKEY level of authentication to enable SERVER LOGIN.

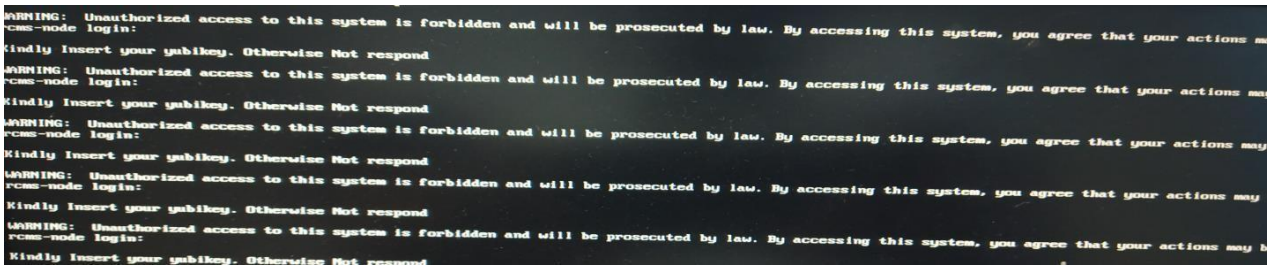
Procedures followed:
Once LUKS is installed it will automatically deduct for LUKS password in order to Login as it encrypts entire block devices and is therefore well-suited for protecting the contents of mobile devices such as removable storage media or laptop disk drives. The underlying contents of the encrypted block device are arbitrary. This makes it useful for encrypting swap devices. This can also be useful with certain databases that use specially formatted block devices for data storage.

Below is the evidence for Luks encryption screen shot.

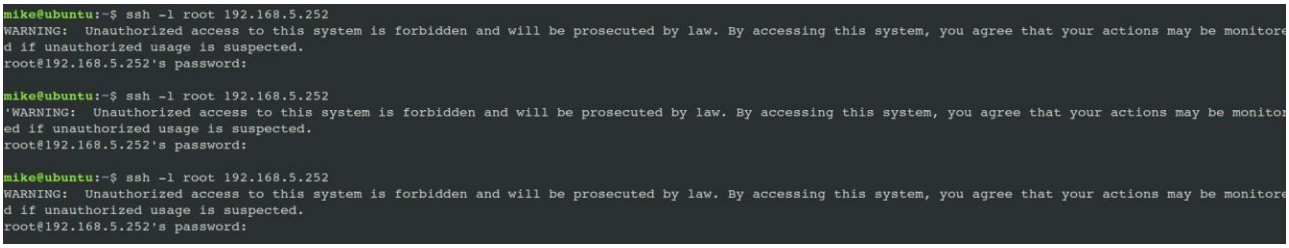


Luks password – 128 characteristics {Linux admin have 64 characteristics + security admin have 64 characteristics)

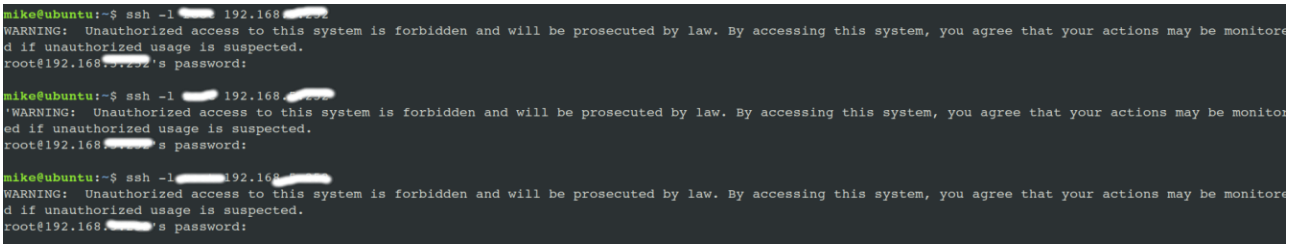
The below image represents the after logging in to LUKS and Waiting for YUBIKEY Access.



YUBIKEY Access for SSH with Password



If we don't own YUBIKEY, SSH will not get accessed.



25.6 Administrative:

The Chief Executive Officer of this organization has the responsibility for the overall administration of this policy. Establishment of the administrative procedures for the compliance with Corporate Policies is the responsibility of the officers and the managers of this organization and all the business units.

26 Definitions

When used in these IT security standards, the following terms are defined terms andwill be proscribed the following meanings:

Access: The ability to use, modify, or affect an IT system or to gain entry to a physical area orlocation.

Application: A computer program or set of programs that meet a defined set of business needs. See also Application System.

Application System: An interconnected set of IT resources under the same direct managementcontrol that meets a defined set of business needs.

Attack: An attempt to bypass security controls on an IT system in order to compromise the data.

Authentication: The process of ensuring the identity of a connected user or participants exchanging electronic data.

Environmental Security: Physical protection against damage from fire, flood, wind, earthquake,explosion, civil unrest and other forms of natural and man-made risk.

Extranet/VPN Connection: Network-level access originating from outside the network. Examplesinclude SSL, IP Sec, "terminal service" or Citrix-like connections.

Firewall: A combination of hardware and software designed to control the types of network connections allowed to a system or combination of systems or that enforces a boundary between 2 or more networks.
Information Technology (IT): Telecommunications, automated data processing, databases, the Internet, management information systems, and related information, equipment, goods, and services.

Information Technology (IT) Assets: The processes, procedures, systems, IT infrastructure, data, and communication capabilities that allows the company to manage, store, and share information inpursuit of its business mission, including but not limited to:

- Applications.
- All data typically associated with IT systems regardless of source. (All data typically associated with IT systems regardless of the medium on which it resides (disc, tape, flashdrive, cell phone, personal digital assistant, etc.).
- End-user authentication systems.
- Hardware (voice, video, radio transmitters and receivers, servers, workstations, personal computers, laptops, and all end point equipment).
- Software (operating systems, application software, middleware, microcode).
- IT infrastructure (networks, connections, pathways, servers, wireless endpoints).
- Services (data processing, telecommunications, office automation, and computerized information systems).
- Telecommunications hardware, software, andnetworks. Radio frequencies.
- Data computing and telecommunications facilities.
- Intelligent control systems such as video surveillance, HVAC, and physical security.

Information Technology (IT) Infrastructure: IT infrastructure consists of the equipment, systems, software, and services used in common across the organization, regardless of mission/program/project. IT Infrastructure also serves as the foundation upon whichmission/program/project-specific systems and capabilities are built. Approaches to provisioning of IT infrastructure vary across organizations, but commonly include capabilities such as Domain Name Server (DNS), Wide Area Network (WAN), Local Area Network (LAN), Secured VPN Network (SVPN) and employee locator systems. Additional common capabilities examples include IT security systems, servers, routers, workstations, networked Supervisory Control and Data Acquisition (SCADA) systems, and networked printers (multifunction devices).

Information Technology (IT) Risk Assessment: Risk assessment is a process by which we determine what IT Assets exist that require protection, and to understand and document potential risks from IT security failures that may cause loss of information confidentiality, integrity, or availability. The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets.

Internal System or Network: An IT system or network designed and intended for use only by Radiant Cash Management Services. Pvt. Ltd., employees.

Intrusion Detection Systems (IDS): Software and/or hardware designed to detect an attack on a network or computer system. A Network IDS (NIDS) is designed to support multiple hosts, whereas a Host IDS (HIDS) is set up to detect illegal actions within the host. Most IDS programs typically use signatures of known cracker attempts to signal an alert. Others look for deviations of the normal routine as indications of an attack.

Intrusion Prevention Systems (IPS): Software and/or hardware designed to prevent an attack on a network or computer system. An IPS is a significant step beyond IDS because it stops the attack from damaging or retrieving data. Whereas ID passively monitors traffic by sniffing packets off of a switch port, an IPS resides inline like a firewall, intercepting and forwarding packets. It can thus block attacks in real time.

Malicious Code: Software (such as a Trojan horse) that appears to perform a useful or desirable function, but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

Malware: A general term coined for all forms malicious software including but limited to computer viruses, worms, Trojan horses, most root kits, spyware, dishonest adware, crime ware and other malicious and unwanted software.

Mobile Device: A small-sized computing device that may have a display screen, touch input or a keyboard, and/or data storage capability. Examples include laptops, Personal Digital Assistants (PDAs), smart phones, tablet PCs, accessible equipment, and portable data storage devices such as tape drives, zip drives, removable hard drives, and USB data storage devices.

Multi-factor Authentication (MFA): A security system or mechanism in which more than one form of authentication is implemented to verify the legitimacy of a transaction. In contrast, single factor authentication involves only a User ID/password.
In 2-factor authentication, the user provides dual means of identification, one of which is typically aphysical token, such as a card, OTP and the other of which is typically something memorized, such as a security code.
Additional authentication methods that can be used in MFA include biometric verification such as keyboard cadence, finger scanning, iris recognition, facial recognition and voice ID. In addition to these methods, device identification software, smart cards, and other electronic devices can be usedalong with the traditional user ID and password.

Network: A term that describes an approach to link together computers and their peripherals in order to communicate among them and with outside parties.

Network Device: A device available to other computers on a network. Example includes servers, firewalls, routers, switches, workstations, networked Supervisory Control and Data Acquisition (SCADA) systems, and networked printers (multifunction devices).
Password: A unique string of characters that, in conjunction with a logon ID, authenticates a user's identity.

Penetration Test: A deliberate probe of a network or system to discover security weaknesses. The test attempts to leverage identified weaknesses to penetrate into the organization. The test exploits the vulnerabilities uncovered during a vulnerability assessment to avoid false positives often reported by automated assessment tools.

Physical Security: Physical security describes measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media in an IT facility. Record Units of related data fields such as groups of data fields that can be accessed by a program and that contain information on a specific item or an individual.

Risk: The potential that an event may cause a material negative impact to an asset.

Risk Assessment. The process of identifying and evaluating risks assessing potential impact.
Risk Management: Identification and implementation of IT security controls to reduce risks to an acceptable level.
Secure Segmentation: Secure segmentation is defined as implementing methods that allow for secure communication between various levels of segmented environments. These environments typically involve 4 basic segment groups:
Outside (Trust no one)
Services (Trust limited to defined segmentation lines)
Internal (Trust limited to defined group)
External users (Trust limited to defined group)
The methods for securing these segments may include but are not limited to firewall and switch/router configurations and router/switch ACLs, IPS, IDS etc.

Security: The protection afforded to IT systems and data in order to preservetheir availability, integrity, and confidentiality. The ability to protect:
The integrity, availability, and confidentiality of information held by the organization.
Information technology assets from unauthorized use or modification and from accidentalor intentional damage or destruction.
Information technology facilities and off-site data storage.
Computing, telecommunications, and applications relatedservices.
Internet-related applications and connectivity.

Security Controls. The security requirements and methods applied by agencies to manage ITsecurity risk as defined in security standards.

Security Domain: An environment or context that is defined by security policy, a security model, orsecurity architecture to include a set of system resources and the set of system entities that have the right to access the resources.

System: Any collection of people, processes, and technology needed to deliver a service, capability, or functionality.

Tablet PC: A portable general-purpose computer contained within a single small form factor LCD display sized to approximately match that of a traditional writing paper tablet. A tablet PC utilizes a touch screen as the primary input source. Typically either wireless (802.11) or mobile (4G) networks are used for connectivity with limited physical port options. Examples of Tablet PC's include: iPad, HP Elite book, Samsung Galaxy Note, Sony Tablet S, Toshiba Thrive, Acer Ionia, KindleFire, other OEM tablet, etc.

Threat: Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Token. A security token may be either a dedicated hardware device or software-based installation on an electronic device which is used for identity proofing in multi-factor authentication.

Trusted System or Network: IT system or network that is recognized automatically as reliable, truthful, and accurate without continual validation or testing.

Untrusted: Characterized by absence of trusted status Assumed to be unreliable, untruthful, and inaccurate unless proven otherwise.

Vulnerability: Relates to risk of attack. In IT terms, vulnerability describes points of risk to penetration of security barriers. Awareness of potential vulnerability is very important to designing ever more effective defense against attack by unauthorized parties.

Vulnerability Assessment: A comprehensive analysis that attempts to define, identify, and classify the security holes (vulnerabilities) in a system, network, or communicationsinfrastructure within the assessment scope.

27 Revision History

Date	Version No	Action taken
8-Mar-23	11.9	updated in section 2 Applications and systems that process, store, or transmit data are monitored, logged, and retained for one year when used by general and privileged users
15-Feb-23	11.8	Addition of rollback policy i.e. 13.8 under the change management policy section 13.
20-Jan-23	11.7	Updated in sec 10.1 report include to section.
6-Jan-23	11.6	Changes in section 6.7.4 As per InfoSec policy review has been conducted bi-annually. Respective Administrators/Personals/Heads should conduct review and should submit review report without failure as instructed.
10-Nov-23	11.5	Addition of IT Asset Planning and Acquisition i.e. 18.2 in asset management policy.
Mar-21	11.4	Changes in section 2.1 Password construction Rule, 10.3 Report to Include
30-Mar-19	11.3	CYBER SECURITY POLICY, 24.1 Policy, 24.2 Overview, 24.3 Scope, 24.4 Policy Makers, 24.5 Policy Audience, 24.6 Policy Classification, 24.7 Policy Audit, 24.8 Policy Enforcement, 24.9 Policy Awareness, 25 DATA ENCRYPTION SECURITY POLICY, 25.1 Purpose, 25.2 Scope, 25.3 YUBIKEY, 25.4 Logic Diagram, 25.5 Process flow, 25.6 Administrative
15-Sep-16	11.2	Updated password policy control i.e. 2.1 Password Policy. 12.2.3 RBAC revised with Annexure IV, Updated vulnerability scanners i.e. 20.3 to the IS policy and procedures.
Mar-16	9.0	Addition of New Table along with sections i.e. 16- Mobile Device Management (MDM), The revision was designed to close the gap between the existing standards and current industry security best practices to mitigate the breadth and sophistication of IT security threats arising out of usage of Mobile Devices for business purposes.
Sep-15	8.0	Addition of New Table along with sections i.e. 17-HR Recruitment policy, as the HR functions got centralised using the HRM application.
Mar-15	7.0	Addition of New Table along with sections i.e. 20-Vulnerability Management Process- The revision was designed to close the gap between the existing standards and current industry security best practices to mitigate the vulnerabilities in IT identified and the risks of these vulnerabilities evaluated.
Sep-14	6.0	Removed language redundant with Information Technology Security standards.
Mar-14	5.0	Addition of New Table along with sections i.e. No 13-Change Management-Many of the security controls and the organization of the updated standards are based on IT security best practice frameworks from the recognized IT standards bodies and accordingly Change Management describes such a process, in brief. Change in software development can be a change in specifications, user requirements, design change, code change or so on and the same requires documentation.
	4.0	Addition of new sections under table no 15 i.e.15.2 MySQL with DRBD/Pacemaker/Coro sync/Oracle Linux 6.5, 15.3 Server HA Components architecture, The revision was designed to close the gap between the existing data replication system and target architecture planned in HA.
Mar-13	3.0	Addition of New Table along with sections i.e. 18.IT Asset Management- The revision was designed to in order to maintain accurate inventory of IT Asset which is an important business practice that involves, licensing information, maintenance, and protection of hardware and software assets utilized by the organisation.
Sep-12	2.0.	Revised format; added language to policy- simplified and clarified language throughout.
Mar-12	1.0	Initial effective date.
30-Sep-11	1.0	Policy adopted.

27.1 Contact Information

For questions about this policy, please contact the Chief Technology Officer / Consultant. For technical security questions or to request a Design Review, please contact the IT Department at Head Office, Chennai.

27.2 Approving Authority

Approved by the Chairman and Managing Director
Prepared by the Chief Technology Officer Date: 31.03.2023.