Information System Security policy

Dvara Kshetriya Gramin Financial Services Private Limited

Version 1.0
Internal and Proprietary

PREAMBLE

The Dvara Kshetriya Gramin Financial Services (Dvara KGFS) Private Limited relies intensely on information and information systems in the pursuit of its organizational objectives. If vital information were unavailable, unreachable or disclosed to inappropriate persons, the company could suffer loss of reputation or financial damage.

To sustain and enhance the enviable reputation that the company enjoys, the Executive Management of the company has initiated and continues to support an information security effort to manage both its information and information systems.

The definition and details of the information security policies contained in this document are a step in this direction.

To be effective, information security must be a team effort and shall involve the participation and support of every individual of the company, who deals with information or information systems. To bolster team work, the policies in this document clarify the responsibilities of users as well as the steps they must take to help protect the company's information and information systems.

This document describes ways to prevent and respond to a variety of threats to the information and information systems, including unauthorized access, loss, misuse and denial of use.

Every individual from the company, irrespective of status or designation must comply with the information security policies in this document. Persons who deliberately violate this and other information security statements are liable to face disciplinary action, up to and including termination. The company also reserves the right to injunctive relief if it deems necessary.

The various provisions in the policy have been drafted to make them in alignment with ISO 27001 standards, ISMS (Information Security Management System) guidelines and the prevailing best industrial practices.

Table of Contents

Contents

1. Introduction

The Dvara KGFS's information systems, and the information and data they contain, are fundamental to the company's daily operations and future success. The company shall implement procedures and controls at all levels to protect the confidentiality and integrity of information stored and processed in its systems and ensure that the information is available only to authorized persons as and when required according to the business requirement.

1.1 Information system security policy document

This document provides the framework to ensure the protection of the company's information assets, and to allow the use, access and disclosure of such information in accordance with appropriate standards, laws and regulations as applicable to the company.

All existing company policies related to personnel, administration, protection of confidential information, and other areas shall apply equally to the information systems environment.

1.2 Information system security policy coverage

The security policies and standards contained in this document have been established to cover information and data, software, hardware and networks used by the company at the Head Office (HO), and all of its branches & offices.

This security policy of the company shall apply to any person (management, employees and administrators, contractors and third parties) who access information using the company's business information systems. In particular, the security policy applies to the following information assets of the company.

- All proprietary information that belongs to the company
- Personnel information relating to the employees of the company
- All customer information held by the company
- All supplier, contractor and other third party information held by the company
- All hard copy documents held by the company
- All software assets such as application software, system software, development tools and utilities
- All physical assets, such as computer equipment, communications equipment, media and equipment relating to facilities
- All services, such as power, lighting, HVAC associated with the company's information systems.

1.3 Objectives of Information system security policy

The overall objective of the 'Information System Security Policy' is to provide guidance and direction for the protection of the company's information systems against accidental or deliberate damage or destruction.

The specific objectives of the 'Information System Security Policy' are:

- Alignment of information security with business strategy to support organizational objectives
- Management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level
- Management of performance of information security by measuring, monitoring and reporting information security governance metrics to ensure that organizational objectives are achieved
- Optimization of information security investments in support of organizational objectives.
- To define standards to ensure that the company's information is secure at all times and to create a foundation upon which sound internal control within the computerized environment can be based
- To prevent unauthorized disclosure of information stored or processed on the company's information systems (Confidentiality)
- To prevent unauthorized accidental or deliberate alteration of information (Integrity)
- To prevent unauthorized accidental or deliberate destruction or deletion of information necessary for operations (Availability)
- To ensure that the data, transactions, communications or documents (electronic or physical) are genuine (Authenticity)
- To ensure that a party to a transaction cannot deny having received or having sent an electronic record (Non- repudiation)
- To ensure that all the subjects with access to the information assets of company are identified, authenticated, authorized, accountable and auditable (Identification, Authentication Authorization, Accountability and Auditability)

The policy shall also provide guidance to the company that its information systems comply with relevant laws and regulations and international standards on information security management such as ISO 27001.

1.4 Responsibility for Information security

- All employees, external contractors, and other third parties including outsourced agencies, who require access to the company's information

systems, shall be responsible for ensuring that the information system security policies are adhered to and that they operate systems in such a manner so as to ensure its security.

- Management at all levels shall be responsible for ensuring that staff are aware of, and adhere to, this policy and the standards.

- The IT department shall be responsible for facilitating and driving the overall information security requirements in all departments/branches.

1.5 Ethics in the field of security

The basis for security consists of the shared ethical norms and attitudes relating to ownership, and the respect for each other and each other's possessions that are shared at the work place.
It is ethical to:

- As management, clarify prevailing rules
- As an employee, respect the company's possessions and resources, and make sure that they are used correctly
- Protect sensitive or confidential information

It is unethical to:

- Actively study information one has gained access to by mistake
- Spread information that can in some way hurt others / and the company's interest
- Actively hide one's identity
- Appropriate authority or rights in excess of those granted
- Make private statements or publish private material in the name of the company
- Sharing of user-ids until strictly required and formally authorized.

1.6 Scope of the policy document

The policy document shall be organized under the following sections:

- Information System security policy framework
- Security violations
- Information System security policy statements

The policy is applicable to

- All staff (permanent & on contractual basis) and non-employees (contractors, consultants, suppliers, vendors etc.) of Dvara KGFS and other individuals, entities or organizations that have access to

Dvara KGFS IT systems

- All locations where users have access to various IT Assets and IT Services including locations that have secure areas providing critical IT Assets and IT Service
- All IT Assets and IT Services involving data, applications, network, security devices, servers and other IT system that needs to be appropriately protected from physical and environmental threats
- All Service Providers who render their IT services to Dvara KGFS and have access to Dvara KGFS facility.

1.7 Distribution of the policy document

1. The Information System Security policy is a confidential document and is meant for permitted use. Such permissions shall be accorded by the IT head.

2. Every person in custody of the document has the responsibility for ensuring its confidentiality. The custodian of the document shall ensure that the document is regularly updated with amendments that may be issued from time to time.

2. Information Security Policy

1. The company recognizes its dependency on the information systems for effective operation of its business. It is, therefore, essential that the information (and the infrastructure that supports it) is secure from destruction, corruption, unauthorized access and breach of confidentiality, whether it is accidental or deliberate.
2. The company's information security needs are further driven by the unique requirements of its customers for safeguarding their data. The success of the company's association with its customers hinges on several major assumptions. First, that the resources are both connected and available, and second, that the infrastructure that supports those resources is both resilient and reliable. Translating these assumptions into reality pose a significant challenge to the company.
3. Internally as well, security requirements are of utmost importance. Successful internal co-operation requires that a common security concept prevail in the company. This would, in turn, result in increased customer satisfaction, greater workforce productivity and more cost-effective operations.
4. To fulfill these security and risk management needs, the company requires a board approved Information System security policy and associated procedures.

5. The objective of the policy is to define standards to ensure that the company's information is secure at all times and to create a foundation upon which sound internal control within the computerized environment can be based.
6. The policies and standards in this document apply to all managers and staff, as well as third parties acting at the direction of the company.
7. The policies shall be supported with relevant standards, guidelines and procedures. The policy framework would, inter-alia, incorporate the following:
    - An information security strategy that is aligned with business objectives and the legal requirements
    - Objectives, scope, ownership and responsibility for the policy
    - Information security organizational structure
    - Information security roles and responsibilities that may include information security-specific roles like IT security manager/officer, administrators, information security specialists and information asset-specific roles like owners, custodians, end-users
    - Periodic review of the policy at least annually and in the event of significant changes necessitating revision by the IT department initiated by the IT head.
    - Periodic compliance review of this policy with regard to the adherence of users to information security policies and put up the findings to the information security committee by the Audit Team yearly.
    - Exception policy for handling instances of non-compliance with the information security policy
    - Identification, authorization and granting of access to IT assets (by individuals and other IT assets). Addressing the various stages of an IT asset's life to ensure that information security requirements are considered at each stage of the lifecycle
    - An incident monitoring and management process to address the identification and classification of incidents, reporting, escalation, preservation of evidence, the investigation process Management of technology solutions for information security like a firewall, anti-virus/anti-malware software, intrusion detection/prevention systems, cryptographic systems and monitoring/log analysis tools/techniques
    - Management and monitoring of service providers that provides for overseeing the management of information security risks by third parties
    - Clearly indicating acceptable usage of IT assets including application systems that define the information security responsibilities of users (staff, service providers and customers) in regard to the use of IT assets

- Requirements relating to recruitment and selection of qualified staff and external contractors that define the framework for vetting and monitoring of personnel, taking into account the information security risk
- Strategy for periodic training and enhancing skills of information security personnel, requirement of continuous professional education.
- The level of security required for information and information assets is dependent upon the value of the information or the impact of the loss of assets to the company, the risks to which they are exposed and the extent to which they are affected by legal and regulatory requirements.
- The standards provided in this document shall be implemented for all information systems of the company.
- The company shall review where existing systems do not comply with the standards; the risks associated with non-compliance and the expected life of the system, and determine what action is appropriate.

8. Accountability for security shall be increased through clear job descriptions, employment agreements and policy awareness acknowledgements. The general and specific security roles and responsibilities within their job descriptions shall be communicated to the employees. The job descriptions for security personnel shall also clearly describe the systems and processes they will protect and their responsibility towards control processes. Management shall ensure that all employees, officers and contractors/consultants to comply with security and acceptable-use policies and protect the institution's assets, including information.
9. Given the critical role of security technologies as part of the information security framework, the company shall subject them to suitable controls across their lifecycle like:
    - Guidelines on their usage
    - Standards and procedures indicating the detailed objectives and requirements of individual information security-specific technology solutions,
    - Authorization for individuals who would be handling the technology
    - Addressing segregation of duties issues, appropriate configurations of the devices that provide the best possible security
    - Assessing their effectiveness and fine-tuning them accordingly, and identification of any unauthorized changes.
10. Handling of digital evidence shall be carefully tracked and documented, and it shall be suitably authenticated by concerned personnel as per legal requirements. Since the evidence resides on or is generated by a digital device, a trained information security official or skilled digital

forensics examiner shall be involved in the handling process to ensure that any material facts is properly preserved and introduced. Securing the Company's information assets shall be an ongoing process thus the company shall continue efforts with security and risk management so that it can successfully meet the challenges of future business, gain the benefits of internal and external co-operation, and give each employee the means to fulfill his or her responsibility for security.

2.1 Review of security policy

- Security policy shall be reviewed every 12 months. However, the security policy shall require update/change depending on any organizational or technological changes that might occur specifically to the company operations.
- Revision number represents the number of times a particular policy/domain was modified.
- The implementation of the policy shall be reviewed independently to provide assurance that the practices properly reflect the policy and that it is effective. The internal audit function, an independent officer or an external agency shall carry out such a review on a continuous basis.
- A full-fledged review shall be conducted once in a year by an independent audit function, whether internal or external.
- The review process shall also mandate that the security policies and standards be reviewed and cleared by the Information Security Committee.
- Information system security policy document shall be reviewed by external agency once in 5 years, or as and when there is a major change in existing business processes or IT environment affecting policies and procedures.

2.1.1 Information Security Strategy

Information Security Strategy aims to address the ongoing Information Security concerns revealed through vulnerability Assessment, IS Audit and reported Incidents. This would ensure the Availability, Confidentiality, Integrity and Authenticity of Information/Data which is of paramount importance to the organization.

2.2 Ownership and Maintenance of this Policy

2.2.1 Policy Owner

- The Board is the owner of the security policy.

- The IT Head is responsible for the enforcement and evaluation of the information security policy. He shall recommend changes to the security policy on a periodic basis.

2.2.2 Procedure for Revision of the Policy

1. The new document shall reflect the details about revision number, issue date and effective date. The old document shall be removed from the set of policies documents and maintained separately mentioning the fact that it has been replaced.
2. Inputs and comments from various departments and business units of the company shall be mandatorily taken into consideration during the review of the policy to facilitate requests for changes or reviews of any specific sections of the practice.

2.2.3 Procedure for Communication of the Policy

The Information System security policy shall be formally communicated to all the employees of Dvara KGFS. Communication shall take the following perspective:

- All employees of the company during the formal induction process shall preferably undergo the Information System security policy training.
- Periodic refresher training shall be provided to all the employees of the company with respect to information security roles and responsibilities.
- Training content shall be vetted by the IT head in conjunction with the HR Department.
- In the event of new additions or changes in the policy, the same shall be officially communicated as part of an official announcement or training program.

2.2.4 Policy Exceptions

1. Exceptions to the IS policy shall be granted after company verifies whether there is a genuine need for the exception. Such exceptions generally will be granted by IT Head. However in case of exigencies IT Head can grant such exceptions and subsequently should be ratified by IT Head.
2. Where exemptions are granted, the company shall review and assess the adequacy of compensating controls initially and on an ongoing basis. A sign-off shall be obtained from the IT Head on the exception
3. Any exception or violation of the security policy shall be reported to the IT Head.

4. The policy owner shall also determine the severity of the violation and whether it is accidental or deliberate. If the violation attempt is serious, employee may be subjected to disciplinary and/or legal action, and including termination of employment.

3. Organization of Information Security

3.1 Management Commitment to Information Security

3.1.1 Policy

The management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

3.1.2 Implementation guidance

The management shall:

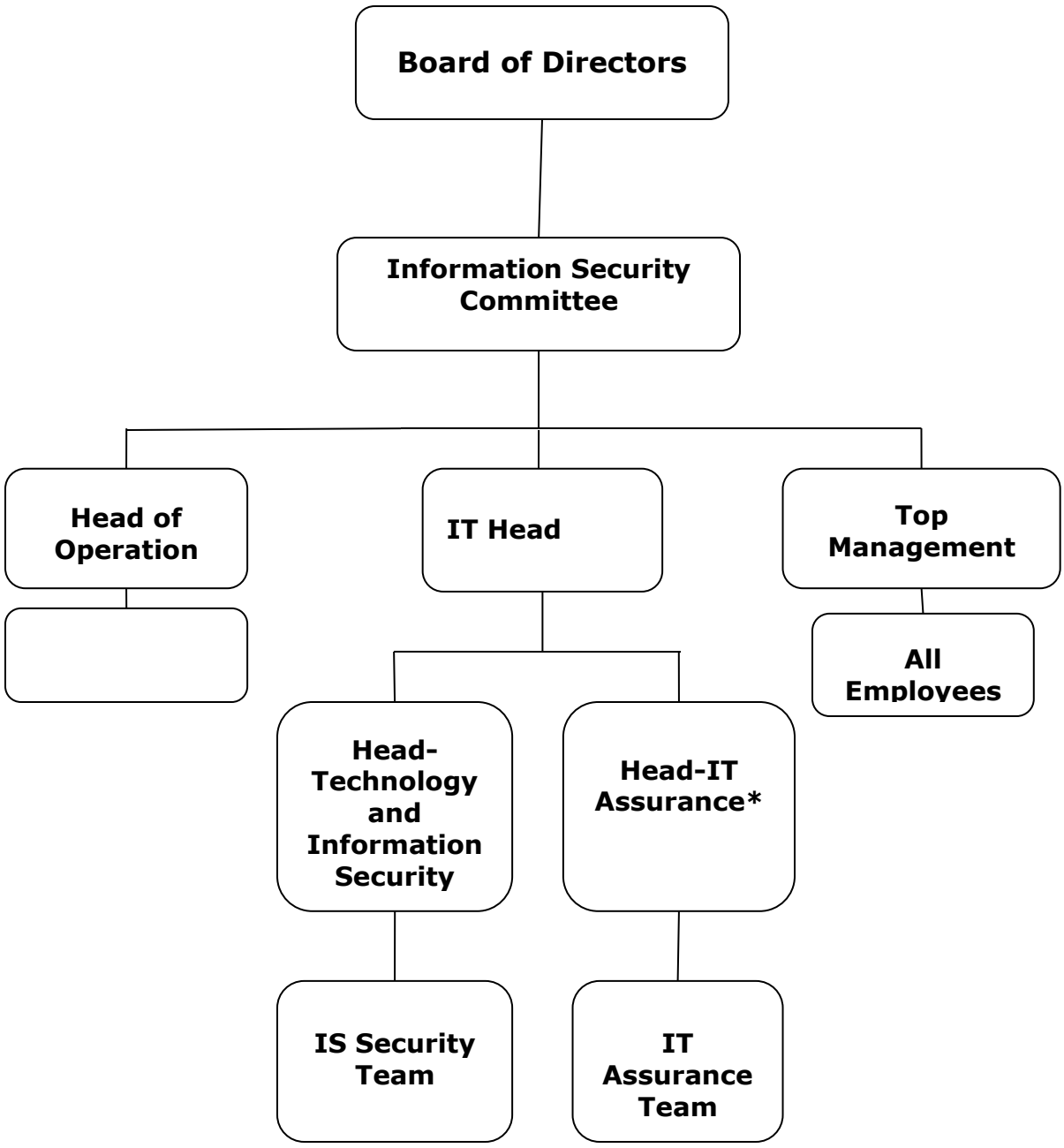
- Set up an information security governance framework consisting of the leadership, organizational structure and processes that protects the company's information and mitigation of growing information security threats
- Ensure that information security goals are identified, meet the organizational requirements, and are integrated in relevant processes
- Formulate, review, and approve information security policy
- Review the effectiveness of the implementation of the information security policy
- Provide clear direction and visible management support for security initiatives
- Provide the resources needed for information security
- Approve assignment of specific roles and responsibilities for information security across the organization
- Ensure classification and assignment of ownership of information assets
- Ensure that periodic risk assessments are performed and ensure adequate, effective and tested controls for people, processes and technology to enhance information security
- Develop processes to monitor security incidents
- Effective identity and access management processes
- Develop meaningful metrics of security performance
- Initiate plans and programs to maintain information security awareness
- Ensure that the implementation of information security controls is coordinated across the organization

- Communicate the security policy and its' adherence requirements to the employees of the company
- The following are the benefits that the company shall expect from the information security governance framework
  - Increased predictability and the reduction of uncertainty in business operations
  - Assurance that critical decisions are not based on faulty information
  - Enabling efficient and effective risk management
  - Protection from the increasing potential for legal liability
  - Process improvement
  - Reduced losses from security-related events and prevention of catastrophic consequences
  - Improved reputation in the market and among customers.
- Identify the needs for internal or external specialist information security advice, and review and coordinate results of the advice throughout the organization. Depending on the size of the company, such responsibilities shall be handled by a dedicated management forum or by an existing management body, such as the board of directors.

3.2 Information Security Organization Structure with Roles and Responsibilities

3.2.1 Purpose

The purpose of information security organizational structure at the company is to ensure the security of the assets of the company. The most important assets of the company are its' people, information and the physical environment comprising infrastructure.
IS security is a business responsibility shared by all members of the organization. The responsibility shall be shared by the following personnel of the company:



3.2.2 Boards of Directors/Senior Management

- The Board of Directors shall be ultimately responsible for information security.
- Senior Management shall be responsible for understanding risks to the company to ensure that they are adequately addressed from a governance perspective.

- The board / senior management shall ensure effective management of risks, including information security risks, by integrating information security governance in the overall enterprise governance framework of the company.
- Board/senior management shall be responsible for approving policy and ensure appropriate monitoring of the information security function.
- The senior management shall be responsible for implementing the board approved information security policy, establishing necessary organizational processes for information security and providing necessary resources for successful information security.
- The senior management shall establish an expectation for strong cyber security and communicate this to their officials down the line.
- The senior management shall establish a structure for implementation of an information security program to enable a consistent and effective solution apart from ensuring the accountability of individuals for their performance as it relates to cyber security.
- The senior management shall ensure that adequate security systems are fully integrated into the IT systems of the company.
- The senior management shall ensure that IT systems of the company are classified based on the risk analysis and specific risk mitigation strategies are in place

3.2.3 Information Security Committee (ISC)

- In order to consider information security from the company-wide perspective a steering committee of executives known as ISC shall be formed with formal terms of reference.
- The Head of IT (IT Head) shall be the member secretary of the committee.

The information security committee structure is provided below:

1. Independent Director - Chairman
2. IT Head- Member
3. Chief Operating Officer (CEO) - Member
4. Operations Head - Member

- The committee shall be responsible for:
- Serving as an effective communication channel for management's aims and directions.
- Ensuring alignment of the security program with the company's objectives.
- Promoting a culture that adheres to good security practices and compliance with policies.
- Developing and facilitating the implementation of information security policies, standards and procedures to ensure that all identified risks are managed within the company's risk appetite
- Approve and monitor major information security projects and the status of information security plans and budgets, establishing priorities, approving standards and procedures
- Supporting in the development and implementation of the company-wide information security management program
- Reviewing the position of security incidents and various information security assessments and monitoring activities across the company
- Reviewing the status of security awareness program
- Assessing the new developments or issues relating to information security
- Reporting to the Board of Directors on information security activities
- Minutes of the security committee meetings shall be maintained to document the committee's activities and decisions and a review on information security shall be escalated to the board on a quarterly basis.

3.2.4 Head of IT (IT Head)

- A sufficiently senior level official, not less than the rank of Chief Manager, shall be designated as the head of IT
- The IT Head shall report directly to and shall have a direct reporting relationship with the top management.
- IT Head shall be responsible for articulating and enforcing the policies that the company uses to protect its information assets apart from coordinating the security related issues / implementation within the company as well as relevant external agencies.
- Other responsibilities of the IT Head include
- Overseeing the security of information and information infrastructure at the company.
- Implementing security policy approved by the management.

- Maintaining security policies.
- Tracking security policy changes.
- Ensuring Information Security training is conducted and creating security awareness among persons of the company in consultation with the HR Department.
- Developing security incident handling procedures.
- Stays updated with the latest developments in the information security field including technology, management practices, and regulations.
- Obtains management support for security activities.

3.2.5 Admin Head

- Ensuring authorized movement of assets within and outside the company by users.
- Ensuring liaison with organizations such as law enforcement agencies, insurance etc.
- Ensuring periodic checks and valid maintenance contracts are available for all critical services and electrical equipment's like generators, fire extinguishers and air conditioners etc.
- Ensuring maintenance of inventory of critical information assets by users.

- Plan and participate in BCP/DR activities.
- Ensuring physical and environmental security.
- Advising users to follow clean desk policy where in no confidential document is left in open
- Ensuring smoking, food and drinking beverages are confined to marked areas by users.
- Plan and participate in BCP/DR activities.
- Reviewing security perimeters and protect unguarded areas.
- Ensuring physical security on fax, photocopy and courier services by users.
- Having control procedures for visitors and ensure they are followed strictly.
- Ensuring periodic trainings for all persons of the organization on safety

3.2.6 Head of Human Resource

- Owner of personnel records.
- Ensuring validity of personnel records.
- Safeguarding Payroll records and related information.
- Maintaining employee files.
- Ensuring background security checks are carried out wherever necessary.
- Ensuring implementation of disciplinary process.
- Ensuring "security conformance" is part of every employee's responsibility, by including the Information Security Policy as part of the induction program.
- Ensuring induction program is conducted for all new employees.
- Ensuring periodic trainings for all employees.
- Ensuring Confidentiality Agreement is signed off by all employees.
- Ensuring Non-Disclosure Agreement is signed off by all contract staff.
- Defining roles and responsibilities of all contractors (if any) working with the company.
- Conducting exit interviews, recording employee comments and acting on the information.
- Plan and participate in BCP/DR activities.

3.2.7 Head of Finance

- Safeguarding budgetary records, investor records and financial statements of any form.
- Reviewing the information classification document for Accounts function and ensuring correctness.
- Participating in Information Security Committee meetings.
- Plan and participate in BCP/DR activities.

3.2.8 Head of Departments/Operations

- Maintaining inventory of critical information assets of the concerned department.
- Reviewing the information classification document for correctness.
- Participating in Information Security Committee meetings.
- Plan and participate in BCP/DR activities.
- Ensuring periodic trainings for all personnel in the department on information security.

- Ensuring clean desk and clear screen policy where in no confidential document is left in open.

3.2.9 Company employees

Users shall comply with the following obligations, in addition to those specific to their roles. Non-compliance may lead to disciplinary action. The following responsibilities apply to all the employees of the company:

3.3 Adherence to acceptable IT usage policy

All employees should sign as having read and understood the acceptable IT usage policy and the security obligations stated in it. Acceptable IT usage policy is a legal binding document and adherence to the same is a part of the employment contract.

3.3.10 Intellectual Property Rights (IPR) & Ownership

- All intellectual property created in the course of employment belongs to the company.
- Vendors' or customer's intellectual property/confidential information are the sole property of the vendor provided under the clauses stipulated in the agreements with the same and shall also belong to the company.
- All computer equipment, software and facilities used by the employees are also proprietary to the company, including all documents, materials and email created.
- Client provided equipments or information shall be the sole property of the client and within the company, the same shall be owned and protected by the respective operations head in accordance with clauses and conditions stipulated in the Master Service Agreement and Statement Of Work.
- The company also reserves the right to withdraw any of the facilities provided if it considers that the use of it is unacceptable in any way.

3.3.11 Authorized access

- The knowledge or possession of protectively marked information shall be strictly limited to those personnel who have a need to know and appropriate clearance to that information.
- Employees shall not remove any information or material from the building/site without prior approval.
- Employees shall not attempt to gain unauthorized access and attempt to access information outside of their normal access rights or duties.

- Employees shall be responsible for all actions undertaken using their user-ID.
- Employees shall not send any information marked 'Confidential' to anyone without approval except to cleared/authorized staff.
- The above mentioned points are to be observed in all of the company branches and facilities.

3.3 Allocation of Information Security responsibilities

Responsibilities for the protection of individual assets and for carrying out specific security processes are as under:

Resources	Resource Owner	Responsibility
Hardware	IT Head	▶ Information security in Hardware ▶ Maintain availability ▶ Configuration and change management ▶ Capacity planning ▶ License assurance ▶ Handling technology obsolesce
Application software	IT Head	▶ Information security in Application software ▶ Creation and deletion of user accounts ▶ Granting access to users ▶ Review of user access and privileges ▶ Change and configuration management ▶ Application management Ensure that adequate security precautions are taken during the SDLC

		and the implementation of the application systems. Responsible for all in house developed software/application packages.
System Software & Middleware	IT Head	▶ Information handling in System software & Middleware ▶ Creation and deletion of user accounts ▶ Granting access to users ▶ Review of user access and privileges ▶ Change and configuration management ▶ Backup and restoration
Network security & management software and equipment	IT Head	▶ Information handling in Network security & Management software and equipment ▶ Configuration and change management ▶ Network provisioning ▶ Data encryption over the network ▶ Network monitoring ▶ Network capacity planning ▶ Installation of software, upgrades and patches ▶ Ensure availability ▶ Compliance of licensing requirements ▶ Policy/signature definition and changes

		▶ Backup and restoration
Miscellaneous IT	IT Head	▶ Information security in respective systems ▶ Installation and maintenance of approved software ▶ Review of unauthorized software periodically ▶ Review of the security settings in the relevant system ▶ Compliance with licensing requirements ▶ Provide adequate physical and environmental security standards ▶ Conduct training programs for security awareness ▶ Provide for adequate support and maintenance of equipment concerned
Information Security policy	IT Head	▶ Monitor compliance with security policy ▶ Update policy in accordance with changes to the change in processing environments and other identified security risks on an ongoing basis. ▶ Review of compliance

3.3.1 Compliance with security policy

1. Employees shall ensure that all security procedures within their area of responsibility are carried out correctly. In addition, all areas within the organization shall be considered for regular review on yearly basis, to ensure compliance with security policies and standards. These shall include the following:
   - Information systems
   - Owners of information and information assets
   - Users (including normal and privilege users)
   - Management
2. Resource owners of information systems shall support regular reviews to ensure compliance of their systems with the appropriate security policies, standards and any other security requirements.
3. Ideally an independent agency shall carry out a compliance review.

3.3.2 Review of logs

Critical audit logs recording exceptions and other security-relevant events shall be produced and kept for an agreed period of 10 years to assist in future investigations and access control monitoring. The following logs shall be generated for the purpose of reviews:

Resource	Type of logs	Contents	Review mechanism
All Network/Firewall equipments	Authentication / Authorization router log	User name, IP, time stamp, router name, port number (Both success and failure authentication attempts)	The routers logs shall be reviewed centrally on a quarterly basis
	Accounting logs	Task ID	
Applications Perdix Tally HRMS	Application Logs	User name, resources accessed, accounts locked, etc.	Application logs shall be reviewed on a quarterly basis and the criticality of the same to be ascertained and necessary action to be initiated

Resource	Type of logs	Contents	Review mechanism
Database	Review audit trail for certain specified activities	Login/Logout information, location and time of failed attempts, changes in status, status of any resource etc.	Review specific events to detect any unauthorized activities for such events
OS	SA user log, last log, account log	User id, time stamp, resource accessed	OS logs to be reviewed on a quarterly basis and the criticality of the same to be ascertained and necessary action to be initiated

3.4 Independent review of information security

3.4.1 Purpose

The regular information security audits/risk assessments/BCP activities shall be carried out by a third party Information Security consultant or the company management shall setup an Internal Audit team.

3.4.2 Policy

As part of the IS audits by third party consultants, the following controls shall be adopted:

1. Appropriate confidentiality and non-disclosure agreements shall be signed with the external auditors.
2. Audit requirements shall be discussed with management before deciding the audit scope.
3. Audit scope and deliverables shall be clearly defined and documented.
4. Any access granted to the auditors other than read-only access shall be disabled immediately after completion of the audit.
5. Audit tools, if any, used by or provided to the auditors, shall be protected against misuse and unauthorized access.

3.5 Contact with authorities and special interest groups

3.5.1 Purpose

The purpose of maintaining contacts with authorities is to support information security incident management and the business continuity/contingency planning process.
Membership with special interest forums helps in staying up to date with the best practices and the relevant security information.

3.5.2 Policy

1. A contact list for all the relevant authorities shall be maintained by the administration and the IT team.
2. Employees are encouraged to join special interest groups like security focus, SANS Institute, CERT, ISACA etc. to stay up to date with the relevant security information.

4. Third Party Access/Outsourcing

4.1 Purpose

The purpose is to ensure that all external suppliers who are contracted to supply services to the company shall agree to follow the Information Security policy of the company. An appropriate summary of the Information Security policies shall be formally delivered to any such supplier, prior to the supply of services.
Third parties shall be given access to the company's premises for a number of reasons. Security requirements for each access depend on the type of third party activities.

4.2 Roles

Role	**Description/Responsibility**
Head of Legal Department	Responsible for formulating an NDA template
Operations Head and IT Head	Responsible for ensuring security requirements are included in the contract. Ensure the NDA satisfies departmental needs.

4.3 Policy

1. The company uses third-party service providers in a variety of different capacities. It shall be an Internet service provider (ISP), application or managed service provider (ASP/MSP) or business service provider (BSP).
2. These providers shall often perform important functions for the company and usually may require access to confidential information, applications and systems.
3. Management shall evaluate the role that the third party performs in relation to the IT environment, related controls and control objectives since the third parties are a key component in the company's controls and its achievement of related control objectives.
4. The effectiveness of third-party controls shall enhance the ability of the company to achieve its control objectives. Conversely, ineffective third-party controls shall weaken the ability of the company to achieve its control objectives.
5. These weaknesses shall arise from various sources including
   - Gaps in the control environment arising from the outsourcing of services to the third party
   - Poor control design, causing controls to operate ineffectively
   - Lack of knowledge and/or inexperience of personnel responsible for control functions.
   - Over-reliance on the third parties' controls (when there are no compensating controls within the company).
6. Third-party providers shall affect the company (including its partners), its processes, controls and control objectives on many different levels. Management shall consider effects arising from the following factors
   - Economic viability of the third-party provider
   - Third-party provider access to information that is transmitted through their communication systems and application
   - Systems and application availability
   - Processing integrity
   - Application development and change management processes
   - The protection of systems and information assets through backup recovery, contingency planning and redundancy.
7. The lack of controls and/or weakness in their design, operation or effectiveness at the third party end shall lead to the following issues
   - Loss of information confidentiality and privacy
   - Systems not being available for use when needed
   - Unauthorized access and changes to systems applications or data
   - Changes to systems, applications or data occurring that result in system or security failures
   - Loss of data
   - Loss of data integrity

- Loss of data protection,
- Loss of system resources and/or information assets
- Increased costs incurred by the enterprise as a result of any of the above

8. The relationship between the company and a third-party provider shall be documented in the form of an executed contract.

4.3.1 Third party access

1. Third parties shall be given access to the company premises. NDA's shall be signed with all third parties having access to the company's information processing facility.
2. Third party personnel shall be escorted into the data center and area only after proper authorization formalities have been completed.
3. All information communicated to third parties shall remain within the company unless otherwise deemed necessary. This includes allocation of separate workstations for all third party work and limitation of all the company-related information to these allocated workstations.
4. Third parties shall use only the IT resources, which has been allocated by the IT team for accessing the company's network. In case of granting third party access to the network through their own devices, prior approval of IT Head must be obtained and the log of the same should be maintained.
5. In the event a third party works with a particular department, the access of that user shall be restricted to the particular department only.
6. Remote access is permitted to third parties / vendors based on critical business requirements which demands troubleshooting, systems analysis, up-gradation etc.
7. Remote access shall be granted by the administrator (in-charge of IT) to the third party site (other than Dvara KGFS Premises) or access from laptops. The access shall be reviewed by the IT Head along with the submission of post facto detailed report.

4.3.2 Outsourcing

1. Wherever the company outsources any activity, it shall be ensured that the contract specifies the security requirements, in addition to the regular contractual details. For guidelines on managing outsourcing in general, IT outsourcing policy may be referred.
2. The contracts shall be reviewed to ensure that the following security requirements are documented as part of the contract:
   - General policy on information security.
   - Procedures to protect the company assets.
   - Restrictions on copying or disclosure.

- Controls to ensure return of information/assets in their possession, at the end of the contract.
- Description of service to be made available.
- Acceptable and unacceptable level of services.
- Liabilities of either party in relation to the contract.
- Permitted access methods.
- List of personnel authorized to use the company assets/services, and their rights and privileges with respect to such use.
- The right to monitor, and the right to terminate services in the event of a security incident or a security breach.
- Right to audit contractual responsibilities, or to have the audits carried out by third parties.
- Any training requirements like security awareness, etc.
- Any physical protection controls.
- Responsibilities regarding hardware and software installation and maintenance.
- Arrangements made by third parties for reporting, notification and investigation of security incidents and breaches.

3. The legal department shall ratify/review all contracts to ensure compliance to regulatory and legal requirements. On completion of the contractual agreement the third party is required to return all the company related information.

5. Asset management

The purpose of this policy is to provide a set of guidelines, for protecting assets that are critical to the Dvara KGFS. Dvara KGFS users who may come into contact with any assets or classified information are expected to familiarize themselves with this policy.
The purpose of this classification is

- To identify procedures that shall be in place to protect the confidentiality, integrity and availability of the organization information
- To educate users about the importance of protecting assets.
- To establish procedures that can ensure the continuity of IT services and deliver the assured quality of these IT services.

5.1 Asset inventory

5.1.1 Purpose

The purpose of the classification is to identify all assets specific to the company operations and also the owners for those assets. Assets are identified and classified to ensure that they are protected.

5.1.2 Roles

Role	Description/Responsibility
Asset owner	▶ Responsible for determining data classification levels for each information asset and maintaining the accuracy, completeness and integrity of information. ▶ Ensure that assets are inventoried ▶ Ensure that assets are appropriately classified (High, Medium or Low on the basis of Confidentiality, Integrity and Availability) and protected. ▶ Define and periodically review access restrictions and classifications to important assets. ▶ Ensure proper handling when the asset is deleted or destroyed
IT Head and Regional Head	▶ Responsible for maintaining the asset inventory register and information classification documents of the respective division. ▶ Responsible for quarterly checks of all assets in the division for physical correctness and reporting to the Head-Technology and Information Security.
IT Head	Responsibility for reviewing the implementation of Asset classification and control policy.

5.1.3 Policy

1. In order to have an effective control, the company shall develop a detailed inventory of its information assets. This shall enable the company to classify the assets and determine the level of protection to be provided to each asset.
2. The inventory record of each information asset shall, at the least, include:
   - ▶ A clear and distinct identification of the asset
   - ▶ Its relative value to the organization
   - ▶ Its location
   - ▶ Asset valuation based on CIA (Confidentiality, Integrity and Availability) values
   - ▶ Its security/risk classification
   - ▶ Its asset group (where the asset forms part of a larger information system)
   - ▶ Its owner

- Its designated custodian

3. The company assets shall be classified into one of the following categories:
   - Physical: e.g. Servers, desktops etc.
   - Software: e.g. operating systems, application software.
   - Information: e.g. all soft copies of information.
   - Services: e.g. other services such as Internet connectivity, infrastructure services
   - Company image and reputation: e.g. stamps & seals
   - People: e.g. all employees based on their roles
   - Paper: e.g. hardcopies/documents
4. The division head in each division shall be responsible to maintain the inventory of their assets in the asset inventory register.
5. The asset inventory register shall be used as an input for the risk assessment, which provides the levels of protection that commensurate with the value and importance of the assets.

5.1.4 IT Assets Labeling, Records Retention and Media Handling

IT Assets Labeling

- All assets of Dvara KGFS shall be prominently labeled to ensure that they are given the necessary protection in use, storage and transport.
- All printed items shall contain the appropriate classification label
- All information, data, documents shall be clearly labeled so that all the users are aware of the ownership and classification of the information.
- The labeling should not reveal any information, related to the asset once installed in public/shared facilities

Records Retention

- Records are information created, received, and maintained as evidence and information by an organization or person in pursuance of legal obligation/standard requirement or in the transaction of business.
- Records can be in two forms - soft (digital) and hard (print) copy.
- Records shall be identified as an IT Asset and given the appropriate classification label.
- Retention period for all records shall be clearly identified by the owners and documented.

Media Handling

- Media Handling guidelines shall be developed to prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

- Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.
- Media should be disposed of securely when no longer required, using formal procedures.
- Media shall be handled and disposed as per Dvara KGFS IS Policy.
- Media containing information should be protected against unauthorized access, misuse or corruption during transportation.

6. Human Resources Security

6.1 Purpose

- Access to information processing facilities shall be provided based on job responsibilities and revoked or modified with changes in responsibilities.
- A mechanism must be implemented to address the risks of human error, theft, fraud or misuse of facilities and assist all personnel in creating a secure computing environment.
- Users shall be adequately trained in security procedures and the proper usage of information processing facilities to minimize possible security breaches

6.2 Roles

Role	Description/Responsibility
Head of Personnel	Responsible for ensuring adequate screening, background checks, implementation of termination process and periodic training for all employees in coordination with Head Training college.
IT Administrator	Responsible for ensuring security awareness and compliance of training of all employees and reviewing the screening and termination process.
IT Head	Information security training contents shall be vetted by IT Head in conjunction with the Personnel Department.
Employee/User	All employees and third party users shall sign and abide by the confidentiality agreements.

6.3 Policy

1. Application owners shall grant legitimate user access to systems that are necessary to perform their duties and security personnel shall enforce the access rights in accordance with company's policies.
2. Employees, contractors, third-party employees and any authorized users shall not exploit their legitimate computer access for malicious or fraudulent reasons because of their:
    - Internal access levels
    - Intimate knowledge of financial institution processes
3. Further, the degree of internal access granted to some users shall increase the risk of accidental damage or loss of information and systems.
4. Risk exposures from internal users shall include
    - Altering data
    - Deleting production and back-up data
    - Disrupting/destroying systems
    - Misusing systems for personal gain or to damage the company
    - Holding data hostage
    - Stealing strategic or customer data for espionage or fraud schemes.
5. The following policies shall be developed to mitigate the risk exposure from internal users.
    - Screening process refer section 6.4
    - Terms and conditions of employment refer section 6.5
    - User awareness and training refer section 6.6
    - Disciplinary process refer section 6.7
    - Termination process refer section 6.8

6.4 Screening Process

6.4.1 Purpose

To reduce the risk of human error, theft, fraud or misuse of facilities potential recruits shall be adequately screened, especially for sensitive jobs.

6.4.2 Policy

1. Company shall have a process to verify job application information of all new employees.
2. Additional background and credit checks shall be warranted based on the sensitivity of a particular job or access level.

3. Personnel with privileged access like administrators, cyber security personnel, etc. shall be subjected to rigorous background checks and screening.
4. Company shall ensure that contractors are subjected to similar screening procedures as outlined in the outsourcing policy.
5. There shall be a periodic rotation of duties among users or personnel conducting the verification as a prudent risk measure.
6. Verification checks shall be carried out on all selected job applicants for the company officers and other companying functions. These include checks on:
    - Character references (Business and Personal).
    - Checks to ensure that all joining information such as applicant's curriculum vitae is correct.
    - Confirmation of claimed academic and professional qualifications
    - Verification of records and other employee related details either internally or through reputed third party
    - Identity checks through government issued identification (e.g.: passport)
    - Criminal Background verification for personnel having super user access

6.5 Terms and conditions of employment

6.5.1 Purpose

To reduce the risk of human error, theft, fraud or misuse of facilities all employees shall agree to and sign the terms and conditions of their employment contract.

6.5.2 Policy

1. All employees are required to agree and sign the terms and conditions of their employment which states their and the organization's responsibility for information security. The terms and conditions shall involve:
    - Employees who are given access to sensitive information shall sign a confidentiality or non-disclosure agreement.
    - Employee's legal responsibilities and rights regarding copyright laws and data protection legislation.
    - Action to be taken if the employee disregards the company security requirements.
    - Responsibility of the company in handling the personnel information of the employees created in the course of their employment.

2. Contractors and third party personnel who come in for temporary or long term assignments with the company shall also sign the confidentiality and non-disclosure agreement.
3. Respective officer in charge who engages third parties and their staff shall ensure that relevant policies are made available and may involve Dvara KGFS IT department in explaining the meaning of Information Security Management System Policy to the third parties.
4. Respective officer in charge who engages third parties and their staff shall ensure that suitable background checks are conducted where third-party staffs are to be engaged in critical duties. Background checks applied to third-party staff engaged in Dvara KGFS duties must be of the same type and scope as applied to Dvara KGFS staff.
5. The contractors/personnel involved in any engagement that provides access to Dvara KGFS confidential information shall be bound by a Non-Disclosure Agreement or similar master agreements.
6. The company's Information Systems Security Policy shall also be directly applicable to all third party personnel and contractors.

6.6 User Awareness and Training

6.6.1 Purpose

Users shall be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.

6.6.2 Policy

1. As human link is acknowledged as the weakest link in the information security chain, the company shall implement an initial and ongoing training and information security awareness program to educate its employees.
2. The program shall be periodically updated keeping in view changes in information security, threats/vulnerabilities and/or the company's information security framework.
3. There shall be a mechanism to track the effectiveness of training program through an assessment/test process designed on testing the understanding of the relevant information security policies. These assessments shall be conducted on a periodic basis.
4. The company shall maintain an updated status on user training and awareness relating to information security and the matter needs to be an important agenda item during the ISC meetings.
5. The areas that shall be incorporated as part of the user awareness program include:
    - Relevant information security policies/procedures

- Acceptable and appropriate usage of IT assets
- Access controls including standards relating to passwords and other authentication requirements
- Measures relating to proper email usage and internet usage
- Physical protection
- Remote computing and use of mobile devices
- Safe handling of sensitive data/information
- Being wary of social engineering attempts to part with confidential details
- Prompt reporting of any security incidents and concerns

6.6.3 Frequency of Training

1. Information security training shall be conducted at a minimum of once in six months and records of all trainings conducted shall be maintained by the HR department.
2. Training shall also be imparted as and when there are major changes or amendments to the ISSP. Training schedule shall be prepared and communicated to all personnel and operations heads.

6.6.4 Training Participants

1. All members covered in the security policy scope are required to attend information security training.
2. Information security awareness training shall be mandatorily imparted to all personnel upon induction. The ISSP shall be clearly communicated and sign off to having read and understood and agreeing to abide by the same shall be obtained from all personnel.
3. The head of each department shall ensure that all members from their respective department are periodically trained on information security responsibilities.

6.7 Disciplinary process

6.7.1 Purpose

A formal disciplinary process for employees exists who have committed a security breach.

6.7.2 Roles

Role	Description/Responsibility

Head of Personnel	Ensure fair treatment for employees who are suspected of committing security breach.

6.7.3 Policy

1. An efficient disciplinary process shall be used as a deterrent to prevent employees from violating the company's security policy.
2. Violations of the security policy shall include, but are not limited to, any act that:
   - Does not comply with the requirements of this policy
   - Exposes the company to actual or potential loss through the compromise of security
   - Involves the disclosure of confidential information or unauthorized use of the company's information and data
   - Results in loss of the company's information / client's information.
3. Any person who becomes aware of any loss, compromise, or possible compromise of information, or any other incident which has information security implications, must immediately inform SPOC & IT Head who shall initiate immediate action to prevent further compromise or loss.
4. The IT Head shall report suspected IS violation to the Audit team for investigation and further action.
5. The Audit department shall take part in the investigation as required.
6. The SPOC shall report the details of the violation to the relevant asset owner and IT Head, who shall determine if the violation has had an impact on the integrity of the information.
7. The IT Head shall be responsible for coordinating appropriate action to prevent a recurrence of the violation or to focus on security education efforts in the particular area.
8. Non-compliance to the minimum requirements or violation of this information security policy shall result in action that may include, but is not limited to, the following:
   - Suspension
   - Termination
   - Other disciplinary action
   - Civil and/or criminal prosecution
9. The disciplinary process shall not commence without prior verification that a security breach has occurred.
10. In cases of serious misconduct the process shall allow for the instant removal of duties, access rights, and the various allocated privileges.

6.8 Termination process

6.8.1 Purpose

To reduce the risk of theft, fraud or misuse of facilities all terminations shall be appropriately handled.

6.8.2 Roles

Role	Description/Responsibility
HR Head	Responsible for implementation of termination process.
IT Head	Responsible for reviewing the information system security related termination process.

6.8.3 Policy

Clearance Certificate

1. When an employee leaves the company; clearance certificate shall be signed by the concerned Department Head and the e-mail accounts and user-ids shall be disabled by IT, based on intimation from Personnel Department, on or before the termination of the employee.
2. Personnel department along with the supervising manager shall ensure that all the assets allocated to the employee are returned.
3. In the event of notice period, appropriate access control shall be provided to ensure that only the information required for the job function is accessible by the employee.
4. Personnel and the supervising manager shall ensure that all the allocated physical/logical access provided to the employee during the course of employment with the company is removed.
5. IT Head and HR department shall ensure that all IT assets such as laptops, PDA's, access cards, and tokens etc. shall be surrendered by the concerned employee before clearing his/her final settlement.
6. Termination briefing shall be conducted by the HR department to explain the continued responsibilities of terminated employees towards the company as defined in the non-disclosure agreement.

Disabling of user-ID

1. The HR department shall be responsible for disabling the user id, well in time, of the impending exit of the employee.
2. On receipt of this information from the HR Department, the IT team shall disable the company email account pertaining to the employee.
3. However, depending on the gravity of the case, if the employee is being terminated on disciplinary grounds the concerned employee's user-ID and email account shall be disabled immediately. The HR department shall inform the IT team about the particulars of the employee as soon as possible.

7. Physical and Environmental Security

7.1 Purpose

The aim is to protect the business premises and information assets from unauthorized access, damage and interference.
To ensure that only authorized personnel are allowed access to the company premises using appropriate entry controls.

7.2 Roles

Role	Description/Responsibility
Head Administration	Responsible for ensuring the physical and environmental controls.
Users	All employees of the company and supporting function shall visibly display identification cards.

7.3 Policy

1. The confidentiality, integrity, and availability of information shall be impaired through physical access and damage or destruction to physical components.
2. Conceptually, those physical security risks shall be mitigated through zone-oriented implementations.
   - Zones are physical areas with differing physical security requirements.
   - The security requirements of each zone are a function of the sensitivity of the data contained or accessible through the zone and the information technology components in the zone.

- The requirements for each zone shall be determined through the risk assessment.

3. The risk assessment shall include threats such as:
   - Aircraft crashes
   - Chemical effects
   - Dust
   - Electrical supply interference
   - Electromagnetic radiation
   - Explosives
   - Fire
   - Smoke
   - Theft/destruction
   - Vibration/ earthquake
   - Water
   - Criminals
   - Terrorism
   - Political issues (e.g. strikes, disruptions)
   - Other threats based on the company's unique geographical location, building configuration, neighboring environment/entities, etc.

4. Company shall deploy the following environmental controls:

   - Secure location of critical assets providing protection from natural and man-made threats.
   - Restrict access to sensitive areas like data centers, which also include detailed procedures for handling access by staff, third party providers and visitors.
   - Suitable preventive mechanisms for various threats indicated above.
   - Monitoring mechanisms for the detection of compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access log reviews etc.

7.4 Physical Security Perimeter

- All entry and exit points shall be identified and controlled. Reception area at head office shall be manned during the company working hours.
- Entry and exit points across the facilities shall be controlled.
- Data center shall have security cameras facing the server racks and the entry points.

- The cameras shall have recording and retention capacity for 30 days. The cameras shall be reset only after the concerned head has viewed the entire footage.

7.5 Personnel Identification Cards

Identification cards shall be issued to all employees of the company and shall be visibly displayed as a means of physical identification while the employees are inside the company premises.
The Personnel department shall be responsible for managing identification cards, including:

- Maintenance of inventories
- Verification
- Withdrawal for cause
- Replacement
- Reporting of damage, loss or theft

7.6 Entry Restrictions for Visitors

1. All visitors to any of the company's information processing facilities shall be required to sign the visitors register. Visitors shall be restricted to the reception area or conference room unless they are escorted.
2. Dedicated visitor entry register shall be maintained at the HO and branches to record visitor movement within these premises.
3. Company branches shall also maintain visitor/vendor access registers to record movement of vendors/visitors other than company customers within the premises.
4. All visitors to the HO or the branches shall be issued visitor identification tags after their details are entered in the visitor register.
5. Separate registers shall be maintained for visitors and vendors.
6. Visitors/Vendors to the data centre/server rooms shall take prior written confirmation from the IT/Regional Head prior to arriving at the facilities hosting the same.
7. Access to visitors to the data centre/server room shall be controlled based on their purpose and authorized personnel from the company shall always escort visitors.
8. Visitors shall be issued visitor identification badges, which they shall visibly display within the company premises. Visitor badges shall be easily distinguishable from the badges worn by employees.
9. These identification badges shall be collected back from the visitors prior to their departure from the company premises.

7.7 Working in secure areas

1. Third party personnel's shall be provided restricted access to secure areas.
2. Third party personnel based in the company's premises shall only use the IT infrastructure issued by the company.
3. External consultants or third party personnel shall be provided network access only after a proper security assessment of their devices.
4. Device checks shall include checking for the antivirus definition and patch updation status of the device.
5. In the event that network access needs to be provided to external parties, they shall be restricted to a dedicated network like VLAN or Guest Wi-Fi that is isolated from company's internal network and application systems.
6. Access to information equipment by hardware maintenance staff shall be controlled. This shall include proper staff identification, logging of work completed, and supervision to ensure that no modifications are performed to other equipments.
7. In the event of third party personnel being replaced by the outsourced company, the company shall follow a formal procedure before the employee is provided access into the company. Procedure shall include verification of credentials and technical competence of the employee and ensuring that the information security roles and responsibilities are clearly communicated and acknowledged by the employee.

7.8 Equipment security

7.8.1 Purpose

All equipments need to be physically protected from security threats and environmental hazards.

7.8.2 Policy

Equipment Siting and Protection

1. Physical equipments shall be protected to reduce the risks from environmental hazards and to reduce the opportunity of unauthorized access. Equipments shall be sited to minimize the access to the work area.
2. Electrical cabinets shall be locked and accessible only to authorized personnel .The record of the personnel maintaining the keys and list of authorized personnel shall be maintained.

3. Environmental condition shall be monitored to ensure that it does not have adverse effect on the operation of information processing facilities. Air conditioning units shall be checked and serviced periodically across the facilities.
4. All storage media having non-public information shall be stored in a physically secured manner. Administration shall provide adequate lockable cabinets for storage.
5. All equipments shall be maintained regularly as per the manufacturers recommended service intervals and specifications.
6. Premises storing the information processing equipments shall have adequate protection against potential threats such as theft, fire, water seepage, vandalism etc.
7. Maintenance schedules shall be formulated and adhered to with respect to smoke detectors, fire alarms and extinguishers.
8. Water pipes and other associated facilities shall be periodically inspected for leaks or any signs of weakness.
9. Eating, drinking and smoking are prohibited near sensitive equipments and workplaces.

Power Supplies

1. Information processing equipments shall be protected from power failures and other electrical anomalies. Suitable power supply shall be provided for all equipment as per the manufacturers' specifications.
2. All equipment shall be protected from power failures and other electrical anomalies through provisioning of generators and UPS.
3. UPS shall be provided for all critical servers and all desktops.
4. A preventive maintenance of the UPS shall be carried out at least once in 3 months in accordance with the manufacturer's recommendations. The records of the same shall be maintained.
5. Back-up generators shall be used to ensure uninterrupted operations of Information Systems in case of power failure for a prolonged period.
6. All electrical fitting inside the Data Center shall be properly earthed to prevent electric surges.
7. The UPS shall be checked at least once in 3 months for the following as part of the maintenance procedure.
    - Voltage in every battery is not below vendor recommended voltage
    - Battery terminals
8. The UPS units shall have sufficient backup to withstand till the alternative power supply is arranged. The UPS shall be maintained in a secure area, covered under regular maintenance and tested periodically in accordance with the manufacturers' instructions.

Cabling Security

1. All cables, including power and telecommunication cables, carrying data or supporting information services shall be protected from damage or unauthorized interception.
2. Power and communication lines into server rooms and network room shall be underground and/or concealed, where possible, or subject to adequate alternative protection.
3. Network cabling shall be protected from unauthorized interception or damage due to environmental hazards e.g. by using conduit and shall be terminated in one of the secure communication rooms.
4. Communication closets shall be locked to protect from unauthorized access.
5. The physical access to the Data Center room shall be restricted.
6. All network terminals shall be marked and identified. Unused network wall sockets shall be sealed-off and their status shall be formally noted.
7. Unused network ports shall be disabled from the switch level.
8. Security of networking cable shall be reviewed during any upgrades or changes to hardware or premises.

Equipment Maintenance

1. Information processing equipments shall be maintained to ensure their integrity and continued availability.
2. Equipment maintenance plan shall be prepared in accordance with the supplier's recommended specifications. All information processing equipments shall be covered under an appropriate insurance cover against hardware, theft, damage or loss.
3. The repair and service to the information processing equipments shall be carried out by authorized personnel only.
4. Maintenance plans shall be prepared for all the information processing equipments. Records shall be maintained for the faults, corrective maintenance carried out and the equipments sent outside the premises for maintenance.

Movement of Equipment

1. Movement of information processing equipments, information, storage media or software to off-site location or for maintenance activities shall be carried out after obtaining appropriate authorization.
2. Authorized personnel must only be permitted to take equipment outside the premises after documented approval and these personnel shall be responsible for the security of the equipments.
3. Material in and material out registers shall be maintained to log all movements of information processing equipments.

Security of Equipment Off-premises

1. Information processing equipments used outside the company premises to support the business activities shall be authorized by the management.
2. The equipments shall be used only by authorized users and they shall be responsible for safeguarding and securing the same.
3. All equipment, data or software being taken outside the company premises shall have a documented authorization from the asset owner.
4. Relevant legal documentation and clearances shall be ensured to be in order before IT infrastructure and other critical equipments are moved to branch locations.
5. Employees carrying the equipments shall observe manufacturers' instructions regarding the protection of equipment and shall not leave them unattended in public places. During traveling the equipments shall be carried as hand baggage and shall be physically protected from damage, theft, etc.

Secure Disposal or Re-use of Equipment

1. Disposal or re-use of the equipments shall be authorized by the owners of assets. Adequate controls shall be followed during the disposal of the equipments to prevent compromise of the information.
2. Documented authorization from the owner of the equipments shall be taken for disposal or re-use of the equipments.
3. Equipments having storage media shall be disposed only after ensuring that all sensitive data and licensed software have been removed or securely overwritten.

7.9 Environmental Controls

7.9.1 Purpose

Protect information and information processing facilities against environmental exposures that may be due to naturally occurring events.

7.9.2 Roles

Role	Description/Responsibility

Head - Administration	Responsible for ensuring the physical and environmental controls.

7.9.3 Policy

Fire Safety

1. Fire extinguishers shall be installed at appropriate places throughout the company facilities and shall be tested periodically to ensure that they function effectively.
2. All fire extinguishers shall clearly display the last tested, next scheduled test and expiry dates.
3. Fire drills shall be routinely conducted in the HO and the branches.
4. Adequate insurance cover shall be obtained for all the IS resources.
5. Fire cabinets shall be inspected by the IT Head on a weekly basis.
6. All the company facilities shall have an adequate number of fire extinguishers and adequately trained personnel to handle the same in an exigency.
7. Fire extinguishers shall be capable of extinguishing all types of fires.
8. Employees and security personnel shall be suitably trained to use these extinguishers in case of emergency.
9. Fire marshals shall be appointed across the facilities to assist in evacuation of employees in event of fire or any other exigency.

Air conditioning

1. Air conditioning and ventilation controls shall be periodically checked to ensure effective functioning.
2. Periodic checks shall be carried out by air conditioning and refrigeration professionals to ensure that the air conditioning units shall not cause condensation in the server room.
3. AMC with vendor shall be reviewed and any SLA/OLA shall be tracked and reviewed with an established frequency.

7.10 General controls

7.10.1 Purpose

Information and information processing facilities shall be protected from disclosure to, modification of or theft by unauthorized persons.

7.10.2 Roles

Role	Description/Responsibility
Head - Administration	Responsible for ensuring the physical and environmental controls.

7.10.3 Policy

Unauthorized Screen Viewing

The screens on computers used to handle sensitive information, irrespective of location must be positioned such that unauthorized persons cannot readily look over the shoulder of the person using the workstation.

Clear Desk and Clear Screen Policy

1. Adequate controls shall be built to reduce the risk of unauthorized access, loss of, and damage to the information available in the form of paper, stored on computer, removable media, etc. during and after the normal working hours.
2. Admin shall provide adequate physical storage cabinets to users for storing sensitive information under lock and key.
3. Employees shall keep information assets like documents, correspondence, computer media, etc. in a secured place when not in use, especially after working hours.
4. Employees shall protect the personal computers and terminals with adequate controls (workstation locks, passwords, etc.) when not in use and shall log off when leaving the company.
5. While leaving the desk, employees shall lock their computers by pressing Ctrl+Alt+Del and lock or by pressing the windows key + L. If computer/device is idle for 5 minutes, current session should be automatically locked out.
6. Employees shall collect all printed documents (printers, faxes, photocopies) in a timely manner. Printers, faxes and photocopiers in secure work areas shall be checked regularly (at least every day after business hours) for prints which are not collected. The items shall be secured until the proper owners of the documents are available.
7. During any relocation of an employee's workspace, the relocating employee shall ensure all information assets are protected during the moving process. This includes, but is not limited to, computer and hard copy files.
8. During any relocation of an employee's workspace, highly sensitive hardcopy information and laptop computers shall be moved by the information owner rather than allowing them to be integrated and moved with less sensitive articles.

9. Recording equipment like photo, video and audio shall not be permitted within a secure area unless specifically authorized by an appropriate organizational unit.
11. Files and other papers (non-electronic format) that contain sensitive information shall be protected from unauthorized access. Users shall not leave such papers unattended on printer trays, photocopiers or their desks.
12. Information classified as 'Confidential' (in paper format or storage media like CDs, DVDs or Tapes) shall be locked (ideally in a fire-resistant safe or cabinet), when not required.

Smoking Restrictions

1. Smoking is prohibited inside all the company facilities.
2. Smoke detectors shall be installed and made active at all the facilities.
3. Smoking inside the premises shall be treated as a violation of the policy and appropriate action shall be initiated against the offending personnel.

8. Communications and Operations Management

Operations management aims at increasing system availability and ensuring secure functioning of the information processing facility. This covers all hardware, software and network systems.

8.1 Operational Procedures

8.1.1 Purpose

The purpose of operational procedures is to ensure correct and secure operation of information processing facilities.

8.1.2 Roles

Role	Description/Responsibility
IT Head	Responsible for reviewing the implementation and maintenance of procedures.
Team Lead, IT Infrastructure	Responsible for maintaining and following the procedures.

8.1.3 Policy

1. Operational procedures shall be developed for all operations in the server room.
2. Duties of IT team member responsible for various operations shall be segregated and clearly documented. Due diligence and care shall be exercised in the event segregation is not feasible.
3. All systems and network faults shall be logged and corrective action taken and recorded for future inference.

8.2 Change Management

8.2.1 Purpose

Changes to the operating information systems environment, which includes changes to servers, network equipments, software, operational programs and procedures, shall be subject to strict change control.

8.2.2 Roles

Roles	Description/Responsibility
User/Application Administrator(Change originator)	Initiates the change request and performs User Acceptance Testing
IT Head	Responsible for assessing the security concerns due to the proposed change.
CEO or Operational Head	Provide authorization/ratification for the development of the change.
Audit team	Conducts audit on all the Changes/functional change requests.

8.2.3 Policy

1. A change management process shall be established, which covers all types of change including
   - Upgrades and modifications to application and software.

- Modifications to business information.
- Emergency ‘fixes’
- Changes to the computers / networks that support the application

2. The change management process shall be documented, and shall include:
   - Approving and testing changes to ensure that they do not compromise security controls
   - Performing changes and signing them off to ensure they are made correctly and securely
   - Reviewing completed changes to ensure that no unauthorized changes have been made.
3. The following steps shall be taken prior to changes being applied to the live environment:
   - Change requests shall be documented on a change request form and accepted only from authorized individuals and the changes shall be approved by an appropriate authority.
   - The User/Application Administrator shall fill the form giving the change description and gets the CEO/Operational Head approval.
   - The potential business impacts of changes shall be determined (for e.g., in terms of the overall risk and impact on other components of the application) by Operations team and security aspects by IT Head based on which the change requests shall be assessed.
   - The Operations team shall update the Change control log and file the change management form.
   - Once the change is approved, the developer (in-house or outsourced) shall develop the change in the development environment
   - Changes shall be tested in the test/quality environment (which shall be segregated from the live environment) to help determine the expected results.
   - Changes shall be reviewed to ensure that they do not compromise security controls (e.g., by checking software to ensure it does not contain malicious code, such as a Trojan horse or a virus)
   - Fall back procedures shall be established so that the application can recover from failed changes or unexpected results.
4. Changes to the application shall be performed by skilled and competent individuals (change implementer) who are capable of making changes correctly and securely and signed off by an appropriate business official.

8.3 Segregation of Duties

8.3.1 Purpose

The company employees shall be required to handle multiple profiles/responsibilities. Wherever practical, duties of staff shall be segregated to avoid conflict of interests using strict access control mechanisms.

8.3.2 Roles

Role	Description/Responsibility
Operational/Regional Head	Responsible for reviewing the duties of employees and implementing controls to avoid/mitigate segregation of duty conflicts
Audit Head	Responsible for reviewing the design and operating effectiveness of controls used to avoid/mitigate segregation of duty conflicts

8.3.3 Policy

1. The company shall develop segregation of duties matrix to ensure that the same person does not perform conflicting roles at the same time like any two of the following functions:
   - System administration
   - Security administration
   - Network monitoring
   - Security audit
2. In the event when it is not feasible to segregate the duties, the company shall use compensating controls such as, monitoring of activities, audit logs etc. to monitor the activities.

8.4 Capacity Planning and System Acceptance

8.4.1 Purpose

Information processing facilities shall be regularly monitored to ensure continued availability of capacity to meet future requirements, in terms of processing power, bandwidth, storage, etc. There shall be a process for acceptance of new information processing systems, upgrades and new versions of the applications.

8.4.2 Roles

Role	Description/Responsibility
IT Team	Responsible for monitoring the capacity of systems and evaluating new systems.
Audit Team	Responsible for reviewing/monitoring the critical system logs.

8.4.3 Policy

1. All critical systems of the company shall be monitored for continuous optimal performance. This includes monitoring the performance of all servers that have a greater cost and lead time for procurement of new capacity.
2. Critical system logs shall be collected and periodically reviewed.
3. Network monitoring and assessments shall be carried out on a continuous basis.
4. Based on the hardware monitoring activities, projections of future capacity requirements shall be made to ensure that adequate processing power and storage are available.
5. Structured network requirements analysis and configuration process shall be documented and adhered to for setting up and configuring networks and any changes are made based on approval from IT Head.
6. Prior to acceptance of any new system, upgrades and new versions, tests of the new system shall be carried out and results are recorded.
7. The following shall be considered during the evaluation of the capacity of information processing facility:
   - New business requirements.
   - Expansion plans of the company.
   - Contingency plans for information systems.
   - Storage capacity for system and database logs.
8. The acceptance criteria for any new system shall be based on the following:
   - Performance and capacity requirements.
   - Security control measures.
   - Error recovery and restart procedures.

- Impact on the existing systems.
- Training on the new system.

8.5 Backup Policy

8.5.1 Purpose

An effective backup strategy is critical to enable the company to recover from any unplanned business disruption. All sensitive, valuable, or critical information residing on systems shall be periodically backed-up for the purpose of recovery in case of system crash, accidental deletion, disaster etc.

8.5.2 Roles

Role	Description/Responsibility
IT Team	Responsible for performing backup operations and maintaining backup logs. Responsible for onsite and offsite backup integrity and security.
Audit Team	Responsible for reviewing the backup process. Review that the appropriate backups are being taken in accordance with the policy.

8.5.3 Policy

1. Information residing on all the critical servers shall be periodically backed-up.
2. Critical information shall be encrypted during the backup process and shall be securely maintained and periodically tested for integrity.
3. Selected files from backups shall be restored every six months to demonstrate the effectiveness of every backup procedure. Critical information shall also be captured and reviewed once restoration is completed and a sign-off is obtained from the IT and Operational Head. Further, any critical issue noted during the restoration process shall be presented to the board for review and further action as appropriate.
4. Data is backed up for the following servers
    1. MS Exchange server – email server hybrid setup with office 365.
    2. Tally server
    3. Perdix Server
    4. HRMS (iON) Server

Backup schedule for the servers are as follows:

1. Daily backup – 5 tapes
2. Weekly backup – 4 tapes
3. Monthly backup – 12 tapes

Daily backup is taken every Monday, Tuesday, Wednesday, Thursday and Saturday. On Friday – weekly full backups are carried out. The Friday backup tapes are also the DR backup and sent to offsite Bank Storage.

4th or 5th Friday of every month is considered for Monthly backup. This tape is also sent to offsite for DR purposes. Monthly tapes are kept for 24 months and reused after 24 months for the monthly backups.

5. Backup media shall be tested at periodic intervals to ensure continuous availability. Back-up logs must be stored securely.

8.6 Media Handling

8.6.1 Purpose

It is essential to classify and handle various media in accordance with the classification of information contained in the media. The asset classification and control information has been enumerated in Section 5 of this policy document.

8.6.2 Roles

Role	Description/Responsibility
Asset Owner	Responsible for determining data classification levels for each information asset.
User	All employees and users of the company's information systems must follow the information labeling and handling guidelines.

8.6.3 Policy

Removable Computer Media

1. Removable computer media, such as Compact Disks ('CD'), tapes, printed reports, USB devices, memory sticks etc., shall be protected from damage, theft and unauthorized access.
2. Authorization shall be required for removal of media from the company and a record must be maintained for all such removals.

3. DVD and USB drives shall be restricted on the desktop of users handling sensitive client data / information. The usage of these devices shall be restricted based on user need and after approval from appropriate authority.
4. Media encryption software and physical port control mechanisms shall be adopted by IT to control and regulate the usage of portable media.
5. Only authorized personnel shall have access to CD drives, backup media, etc.
6. Media shall be stored in a safe and secure environment.

Disposal of Media

1. Media storing information shall be disposed securely to prevent unauthorized access to the information during the disposal process. Proper precautions shall be taken to prevent recovery of the data from the disposed media by unauthorized personnel.
2. Magnetic media shall be degaussed before they are disposed of.
3. CD's and other optical media shall be crushed and destroyed.
4. Information in the form of documents, which are confidential and sensitive for the business, shall be disposed of securely. Such documents shall be shredded. The data owner must authorize the destruction of these documents.

8.7 Malicious code policy

8.7.1 Purpose

The purpose of this policy is to:

- Build detection and prevention controls to protect against malicious codes.
- Increase user-awareness to minimize incidents of malicious code infection.

8.7.2 Roles

Role	Description/Responsibility
User	All employees and users of the company's information systems must follow the anti-virus policy.
IT Team	Responsible for maintaining anti-virus software.

8.7.3 Policy

1. The company shall define controls to protect against malicious code using layered combinations of technology, policies and procedures and training.
    - Malicious software is an integral and a dangerous aspect of internet based threats which target end-users and organizations through modes like web browsing, email attachments, mobile devices, and other vectors.
    - Malicious code may tamper with a system's contents, and capture sensitive data. It can also spread to other systems.
    - Modern malware aims to avoid signature-based and behavioral detection, and may disable anti-virus tools running on the targeted system.
    - Anti-virus and anti-spyware software, collectively referred to as anti-malware tools, help defend against these threats by attempting to detect malware and block their execution.
2. The controls shall be of the preventive and detective/corrective in nature. Controls shall be applied at the host, network, and user levels:
    - Controls at the host level shall include:
        - Host hardening including patch application and proper security configurations of the operating system (OS), browsers, and other network software.
        - Implementing host-based firewalls on each internal computer and especially laptops assigned to mobile users.
        - Many host-based firewalls also have application hashing capabilities, which are helpful in identifying applications that may have been trojanized after initial installation.
        - Host IPS and integrity checking software combined with strict change controls and configuration management.
        - Annual auditing of host configurations (Manual and Automated).
    - Controls at the network level shall include:
        - Limiting the transfer of executable files through the network perimeter based on approval.
        - IDS and IPS monitoring of incoming and outgoing network traffic, including anti-virus, anti-spyware and signature and anomaly-based traffic monitors
        - Routing Access Control Lists(ACLs) to limit incoming and outgoing connections as well as internal connections to those necessary for business purposes
        - Proxy servers to inspect incoming and outgoing packets for indicators of malicious code and block access to known or suspected malware distribution servers

        - Filtering to protect against attacks such as cross-site scripting and SQL injection
    - Controls at user level shall include:
        - User education and awareness.
        - Safe computing practices.
        - Indicators of malicious code.
        - Defined response actions.
3. Enterprise security administrative features shall be used daily to check the number of systems that do not have the latest anti-malware signatures.
4. Company shall employ anti-malware software and signature auto update features to automatically update signature files and scan engines whenever the vendor publishes updates. After applying an update, automated systems shall verify that each system has received its signature update. The company shall monitor anti-virus console logs to correct any systems that failed to be updated.
5. The systems deployed for client security shall be delivering simplified administration through central management and providing critical visibility into threats and vulnerabilities. The systems shall also be integrated with existing infrastructure software, such as Active Directory for enhanced protection and greater control.
6. Administrators shall not rely solely on antivirus software and email filtering to detect worm infections. Logs from firewalls, intrusion detection and prevention sensors, DNS servers and proxy server logs shall be monitored on a daily basis for signs of worm infections including but not limited to:
    - Outbound SMTP connection attempts from anything other than the company's SMTP mail gateways
    - Excessive or unusual scanning on TCP and UDP ports 135-139 and 445
    - Connection attempts on IRC or any other ports that are unusual for the environment
    - Excessive attempts from internal systems to access non-business web sites
    - Excessive traffic from individual or a group of internal systems
    - Excessive DNS queries from internal systems to the same host name and for known "nonexistent" host names. Using a centralized means such as a syslog host to collect logs from various devices and systems can help in the analysis of the information
7. Company shall configure laptops, workstations, and servers so that they do not auto-run content from USB tokens, USB hard drives, CDs/DVDs, external devices, mounted network shares, or other removable media. In addition, all removable storage devices must be encrypted and shall require a valid key to access its contents.

8. Company shall configure systems so that they conduct an automated antimalware scan of removable media when it is inserted.
9. Email attachment filtering
    - Company shall filter various attachment types at the email gateway, unless required for specific business use based on approval.
    - Company shall consider only allowing file extensions with a documented business case and filtering all others based on approval.

Anti-Virus Software

1. Industry leading anti-virus software shall be installed on all the servers as well as individual desktops and laptops to control the spread of virus and to ensure timely identification and repair of the virus infection.
2. IT team member shall be positioned across the critical installations and branches to facilitate monitoring and remediation in the event of an infection.
3. Anti-virus software shall be regularly updated, with the latest virus definitions to control the infection and spread of virus on the network. Reports of the same shall be reviewed and maintained.
4. Health status reports of machines shall be taken and reviewed every week to check for possible infections.
5. Employees/users shall be instructed to unplug the system from the network the moment they suspect infection.
6. Virus-infected systems shall be isolated from the network until they have been verified as virus-free.

Unauthorized Software

1. All software shall be obtained in an authorized and legal manner. Unauthorized or pirated software shall not be permitted on the network or computer systems.
2. Regular reviews of the software and the data shall be carried out to identify any unapproved installation software.
3. Any activity with the intention to create and/or distribute malicious programs into the network (for example, viruses, worms, Trojan horses, e-mail bombs, etc.) shall lead to disciplinary and/or legal action.

8.8 Patch management

8.8.1 Purpose

Software patches such as hot fixes and service packs for operating systems and other applications shall be applied to ensure continued availability and protection from malicious attacks.

8.8.2 Roles

Role	Description/Responsibility
IT Team	Responsible for implementing the security patches in coordination with concerned Division/Functional head.
Team Lead – IT Infra	Responsible for ensuring that necessary security patches are applied at regular intervals. Responsible for reviewing the patching process.

8.8.3 Policy

1. A patch management process shall be in place to address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact.
2. There shall be documented standards / procedures for patch management.
3. The standards / procedures for patch management shall include
   - A method of defining roles and responsibilities for patch management
   - Determining the importance of systems (for e.g., based on the information handled, the business processes supported and the environments in which they are used)
   - Recording patches that have been applied (for e.g., using an inventory of computer assets including their patch level)
4. The patch management process shall include aspects like:
   - Determining methods of obtaining and validating patches for ensuring that the patch is from an authorized source
   - Identifying vulnerabilities that are applicable to applications and systems used by the organization
   - Assessing the business impact of implementing patches (or not implementing a particular patch)
   - Ensuring patches are tested

- Describing methods of deploying patches, for example, through automated manner
- Reporting on the status of patch deployment across the organization.
- Including methods of dealing with the failed deployment of a patch (e.g. redeployment of the patch)

5. Methods shall be established to protect information and systems if no patch is available for an identified vulnerability, for example, disabling services and adding additional access controls.
6. The company shall deploy automated patch management tools and software update tools for all systems for which such tools are available and safe.
7. The company shall measure the delay in patching new vulnerabilities and ensure the delay is not beyond the benchmarks set forth by the organization, which shall be less for critical patches, say not more than a week, unless a mitigating control that blocks exploitation is available.
8. Critical patches shall be evaluated in a test environment before being updated into production on enterprise systems.
9. If such patches break critical business applications on test machines, the company shall devise other mitigating controls that block exploitation on systems where the patch is difficult to be deployed because of its impact on business functionality.
10. Patch management solution shall be able to roll back patches, if systems conflicts arise after deployment.
11. Weekly reports shall be reviewed by the IT Head showing the patch status of all systems.
12. Patches for critical systems shall follow the change control process.

8.9 Mobile Computing

8.9.1 Purpose

When using mobile computing devices provided by the company, like laptops and mobile phones, special care shall be taken to ensure that business information is not compromised.

8.9.2 Roles

Role	Description/Responsibility
User	Custodians of mobile devices shall ensure its security.

8.9.3 Policy

1. Laptops shall be issued to employees only based on official need to use one. This shall also depend on the grade of employee fixed and decided by the management of the company from time to time.
2. Employees and outsourced personnel if any shall sign a laptop custody agreement for taking responsibility for the laptop and associated peripherals.
3. Employees / individuals to whom company owned laptops are issued shall be responsible for its safe custody.
4. Laptop shall be used by employees for legitimate business purposes only.
5. Personal laptops for internet access shall be approved only on a case to case basis. The usage of personal laptops in company premises for internet access shall require a formal authorization process to be in place. IT Head shall either permit or deny the use of personal laptops in company premises for internet access.
6. Laptops and peripherals shall not be left on the desk or in the work area or any other visible location overnight. It shall be locked in a secure area at the end of the workday, if it is left in office.
7. Laptops shall not be left unattended in public places
8. The concerned staff shall file a police report immediately in the event a laptop is stolen. The staff shall also notify the IT team, concerned Department head or Regional head as appropriate, within one business day of the theft.
9. Employees shall sign a declaration relating to acceptable use of laptops before laptops are issued to them
10. Laptop details shall be maintained containing name of the staff and details of laptops issued (like make, model, serial number of machine and accessories).
11. Laptop users shall ensure that data is backed up on a server periodically based on need and critical of data.
12. Use of laptops in public places shall be restricted.
13. Internet browsing using public Wi-Fi hotspots is not permitted.
14. Laptop users shall ensure that laptops have power on password enabled and the screen saver password is enabled. Users must ensure that the passwords adhere to the following
    - Minimum Length - 8 characters
    - Complexity - Enabled (for e.g., at least one special character and one numeral)
    - Max password age – 90 days
    - Max failed login attempts – 5

15. Employees are required to encrypt/password protect all company sensitive and restricted data.

16. Antivirus software shall be loaded in the laptops and updates applied periodically, to protect against malicious software.
17. Laptops shall always be personally carried by the user during air travel and shall not be sent as checked in baggage.

8.10 Data Security

8.10.1 Purpose

To ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives

8.10.2 Policy

1. Company shall define and implement procedures to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.
2. The company shall seek to establish uniform risk-based requirements for the protection of data elements.
3. To ensure that the protection is uniform within and outside of the company, tools such as data classifications and protection profiles shall be used.
    - Data classification and protection profiles are complex to implement when the network or storage is viewed as a utility. Because of that complexity, some institutions treat all information at that level as if it were of the highest sensitivity and implement encryption as a protective measure. The complexity in implementing data classification in other layers or in other aspects of an institution's operation may result in other risk mitigation procedures being used. Adequacy is a function of the extent of risk mitigation, and not the procedure or tool used to mitigate risk.
4. Policies regarding media handling, disposal, and transit shall be implemented to enable the use of protection profiles and otherwise mitigate risks to data. If protection profiles are not used, the policies shall accomplish the same goal as protection profiles by delivering the same degree of residual risk without regard to the following
    - whether the information is in transit or storage
    - who is directly controlling the data
    - where the storage may be
5. There shall be secure storage of media and following controls shall be considered for implementation
    - Physical and environmental controls such as fire and flood protection

- Limiting access by means like physical locks, keypad, passwords, biometrics, etc.
- Labeling
- Logged access

6. Management shall establish access controls to limit access to media, while ensuring that all employees have authorization to access the minimum data required to perform their responsibilities.
    1. All users are given access to **One Drive** (One Drive being the home drive) **and N drive** for storing the official documents,
    2. Only primary user has access and can share the files, documents to other users and set permissions.
    3. N Drive is a Group drive and all team members belonging to a particular group have access to that N drive folders. All users in the respective team can store, share files and documents.
    4. Other members can be given permission to access a team's N drive based on need and formal approval by entitled authority.
7. Sensitive information such as system documentation, application source code, and production transaction data shall have more extensive controls to guard against alteration (e.g., integrity checkers, cryptographic hashes). The company shall minimize the distribution of sensitive information, including printouts that contain the information.
8. Periodically, the security staff, audit staff, and data owners shall review authorization levels and distribution lists to ensure they remain appropriate and current.
9. The storage of data in portable devices, such as laptops and PDAs, poses unique problems. In order to mitigate those risks, the company shall typically encrypt sensitive data, host-provided access controls, etc.
10. Company shall have appropriate disposal procedures for both electronic and paper based media.
11. Contracts with third-party disposal firms shall address acceptable disposal procedures.
12. For computer media, data frequently remains on media after erasing. Since that data can be recovered, additional disposal techniques shall be applied to sensitive data like physical destruction, overwriting data, degaussing etc.
13. Company shall maintain the security of media while in transit or when shared with third parties. The company shall include contractual requirements that incorporate necessary risk-based controls, restrictions on the carriers used and procedures to verify the identity of couriers.
14. Company shall encrypt customer account and transaction data which is transmitted, transported, delivered or couriered to external parties or other locations, taking into account all intermediate junctures and transit points from source to destination.
15. Other aspects that shall be considered include

- Appropriate blocking - Fortigate 500D Gateway appliance for internet filtering which has the features of Gateway Antivirus, web filtering, content filtering, URL filtering, and also has application control, intrusion protection.
- Filtering and monitoring of electronic mechanisms like e-mail and printing - Symantec appliance for email gateway which spam mails and unwanted mails to Dvara KGFS domain. It also has the content filtering features enabled. Symantec protection for exchange 2010 has been installed in all the Dvara KGFS exchange transport servers that take care of internal mail flow filtering.
- Monitoring for unauthorized software and hardware like password cracking software, key loggers, and wireless access points.

16. The company shall consider implementing data leak prevention (DLP) solution to enhance its ability to protect its information assets
    - DLP solutions provide a comprehensive approach covering people, processes, and systems that identify, monitor, and protect the following
        - Data in use (e.g., endpoint actions)
        - Data in motion (e.g., network actions)
        - Data at rest (e.g., data storage)
    - DLP solutions enable deep content inspection and with a centralized management framework.
    - DLP solutions include a suite of technologies that facilitate three key objectives:
        - Locate and catalogue sensitive information stored throughout the company
        - Monitor and control the movement of sensitive information across the company's networks
        - Monitor and control the movement of sensitive information on end-user systems
17. Company may consider such solutions, if required, after assessing their potential to improve data security.

8.11 On-going Security Monitoring

8.11.1 Purpose

To identify events and unusual activity patterns that shall impact the security of IT assets.

8.11.2 Policy

1. Company shall have robust monitoring processes in place to identify suspicious events and unusual activity patterns that could impact on the security of IT assets.
2. The strength of the monitoring controls shall be proportionate to the criticality of an IT asset.
3. Alerts shall be investigated in a timely manner, with an appropriate response determined.
4. The company shall consider using the following monitoring processes
    - Activity logging (including exceptions to approved activity), for example, device, server, network activity, security sensor alerts
    - Monitoring staff or third-party access to sensitive data/information to ensure it has a valid business need.
    - Scanning host systems for known vulnerabilities
    - Checks to determine if information security controls are operating as expected and are being complied with
    - Environment and customer profiling
    - Checking for the existence and configuration of unauthorized wireless networks by using automated tools
    - Discovering the existence of unauthorized systems by using network discovery and mapping tools
    - Detecting unauthorized changes to electronic documents and configuration files by using file integrity monitoring software
5. Company's networks shall be designed to support effective monitoring. Design considerations shall include the following:
    - Network traffic policies that address the allowed communications between computers or groups of computers
    - Security domains that implement the policies
    - Sensor placement to identify policy violations and anomalous traffic
    - Nature and extent of logging
    - Log storage and protection
    - Ability to implement additional sensors on an ad hoc basis when required
6. Company shall establish a clear allocation of responsibility for regular monitoring. Adequate processes and tools to manage the volume of monitoring required shall be put in place to reduce the risk of an incident going undetected.
7. Highly sensitive and/or critical IT assets shall have logging enabled to record events and monitored at a level proportional to the level of risk.
8. Users with elevated access privileges shall be subjected to a greater level of monitoring in light of the heightened risks involved.
9. The integrity of the monitoring logs and processes shall be safeguarded through appropriate access controls and segregation of duties.

10. IT team shall review all system accounts including user accounts and disable any account that cannot be associated with a business process and business owner based on the approval of Operation and other Department Head. Reports generated from systems and reviewed by frequently by IT Head shall include:
    - List of locked out accounts
    - Disabled accounts
    - Accounts with passwords that exceed maximum password age
    - Accounts with passwords that never expire
11. IT Team shall establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor.
12. IT Team shall regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.
13. IT team shall monitor account usage to determine dormant accounts that have not been used for a given period, notifying the user or user's manager of the dormancy. After a longer period, the account shall be disabled.
14. On a periodic basis, the Department/Regional Heads shall match active employees and contractors with each account belonging to their managed staff. System/Application administrators shall then disable accounts that are not assigned to active employees or contractors.
15. IT Team shall validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction.
16. Systems shall record logs in a standardized format such as csv entries. If systems cannot generate logs in a standardized format, IT team shall deploy log normalization tools to convert logs into a standardized format.
17. System administrators and information security personnel shall consider devising profiles of common events from given systems, so that they can tune detection to focus on unusual activity, reducing false positives, more rapidly identify anomalies, and prevent overwhelming the analysts with insignificant alerts.
18. The following technologies/factors shall be considered for effective attack detection and analysis:
    - **Intrusion Detection and Prevention System (IDS and IPS)** IPS products that have detection capabilities shall be fully used during an incident to limit any further impact on the organization. IDS and IPS products are often the primary source of information leading to the identification of an attack. Once the attack has been identified, it is essential to enable the appropriate IPS rule sets to block further incident propagation and to support containment and eradication.

19. Company shall also pro-actively monitor various authentic sources like CERT-In, security vendors, etc. for any security related advisories and take suitable measures accordingly.

8.12 Information security reporting and metrics

8.12.1 Purpose

- To monitor the information security condition of the company regularly in order to identify areas of improvement
- To report the effectiveness and efficiency of the information security arrangements to the key stakeholders

8.12.2 Policy

1. Security monitoring arrangements shall be in place to provide key decision-makers and Senior Management/Board of Directors with an informed view of aspects like
    - The effectiveness and efficiency of information security arrangements
    - Areas where improvement is required
    - Information and systems that are subject to an unacceptable level of risk
    - Performance against quantitative targets
    - Actions required to help minimize the risk
        - Reviewing the company's risk appetite
        - Understanding the information security threat environment
        - Encouraging business and system owners to remedy unacceptable risks
2. There shall be arrangements for monitoring the information security condition of the company, which are documented, agreed with top management and performed regularly.
3. Information generated by monitoring the information security condition of the company shall be used to measure the effectiveness of the information security strategy, information security policy and security architecture.
4. Analysis performed as part of security monitoring and reporting arrangement shall include the following:
    - Details relating to information security incidents and their impact
    - Steps taken for non-recurrence of such incidents in the future
    - Major internal and external audit/vulnerability assessment/penetration test findings and remediation status
    - Operational security statistics, such as firewall log data, patch management details and number of spam e-mails

- Costs associated with financial losses, legal or regulatory penalties and risk profile(s)
- Progress against security plans/strategy
- Capacity and performance analysis of security systems
- Infrastructure and software analysis
- Fraud analysis

5. Information collected as part of security reporting arrangements shall include details about all aspects of information risk such as:
   - Criticality of information
   - Identified vulnerabilities and level of threats
   - Potential business impacts and the status of security controls in place.
6. Information about the security condition of the company shall be provided to key decision-makers/stake holders like the board, top management, members of IT Head, and relevant external bodies like RBI etc.
7. Metrics shall be used by the IT team to determine the following
   - Discern the effectiveness of various components of their security policy and programs,
   - The security of a specific system, product or process,
   - Effectiveness and efficiency of security services delivery
   - The impact of security events on business processes
   - The ability of staff or departments within the company to address security issues for which they are responsible.
   - The level of security awareness within the company.
8. The measurement of security characteristics shall allow management to increase control and drive further improvements to the security procedures and processes.
9. Effective metrics shall follow the SMART acronym i.e. specific, measurable, attainable, repeatable and time-dependent.
10. In addition, a comprehensive set of metrics that provide for prospective and retrospective measures, like key performance indicators and key risk indicators, shall be devised.
11. The efficacy of a security metrics system in mitigating risk depends on completeness and accuracy of the measurements and their effective analysis. The measurements shall be reliable and sufficient to justify security decisions that affect the institution’s security posture, allocate resources to security-related tasks, and provide a basis for security-related reports.
12. Some illustrative metrics shall include
    - Coverage of anti-malware software and their updation percentage
    - Patch latency
    - Extent of user awareness training
    - Vulnerability related metrics

8.13 Communications Management

8.13.1 Purpose

To ensure that all exchange of information shall be controlled to prevent loss, modification or misuse of information that can cause harm to the reputation of the company.

8.13.2 E-mail Policy

Purpose

E-mail is the preferred medium of communication. Adequate security measures shall be taken to prevent loss, misuse of information exchanged through electronic mail. The company's e-mail system shall be used only for the conduct of its business. The use of corporate email system for personal purposes shall be restricted. All information and messages stored in it shall be treated in the same manner as business-related information and messages.

Roles

Role	Description/Responsibility
User	Users must follow the email policy.

Policy

1. The email system is intended for use in the conduct of the company's business. All e-mail messages shall be considered as the company records and there shall be no expectation of personal privacy.
2. The company reserves every right to monitor, examine, block or delete any incoming or outgoing e-mail in the company's network.
3. The company shall reserve the right to inspect and review any data maintained in its e-mail system without prior consent of, or notification to, the employee. However, the Audit Team before conducting such inspections shall obtain approval from the IT Head.
4. IT Head shall disclose contents of e-mail either internally or to external parties, where necessary, for a legitimate business reason or as evidence for legal investigation without further permission of the employee.
5. System administrators shall not be permitted to read another individual's e-mail without the individual's permission or without explicit authorization from IT Head.
6. All e-mail users shall sign and must adhere to an information systems acceptable usage agreement.
7. Users shall have no expectations of privacy of information as well as assurance that information has been properly transmitted in the event

unofficial/non approved e-mail sources are used for transmitting sensitive information.

8. Auto forwarding facility from company's email system to personal email IDs shall not be permitted.
9. All external outgoing Internet e-mails shall carry an automatic standard footer banner. The banner shall indicate that:
   - The mail is intended only for the use of the recipient to whom it is addressed.
   - The mail shall not be acted upon but destroyed promptly if a person, to whom it is not intended, receives it.
   - Opinions, conclusions and other information in the message that do not relate to the official role of the sender shall be understood as neither given nor endorsed by the company The e-mail facility shall not be used for personal gain by any employee.
   - E-mail shall not be used for transmitting non-work related messages, pictures, jokes, programs, chain letters etc.

10. All incoming mails shall be scanned for viruses and spam.
11. The message limits for incoming messages shall be specified if authorized by the systems administrator.
12. The systems administrator shall be responsible for installing necessary security related software updates and hot fixes for the mail server and the mail software in a timely manner.
13. E-mail messages on the mail server shall be backed up on a daily basis. Email server backups shall be taken daily.
14. Users are accountable for any mail/action that can be traced to his/her user ID. Users have a responsibility to keep his/her password strictly confidential.
15. Employees shall take suitable protective action to prevent sending and downloading files with viruses. Although all emails sent and received are automatically scanned for viruses, employees shall refrain from opening dubious attachments.
16. Information that is highly confidential shall not be sent over e-mail unless adequate security measures are taken, like password protection and encryption.
17. Employees are forbidden from using the company's official mail ID's for transmitting offensive messages, inflammatory remarks, damaging statements or any other form of communication which could be considered offensive or vulgar. Employees shall be personally liable for legal prosecution including termination from service if they are caught doing so.
18. The company reserves the right to monitor all communication through the official email system.
19. Employees shall use the standard official disclaimer for all mails sent from the company ID.
20. Employees shall ensure that all unwanted emails are deleted.

8.13.3 Publicly Available Systems

Purpose

Appropriate safeguards shall be taken to protect the integrity of electronically published information in the company websites.

Roles

Role	Description/Responsibility
CEO	Responsible for authorizing all changes to the company's websites.

Policy

1. The list of websites maintained by Dvara KGFS shall be inventoried
2. All changes to the company's website shall be controlled and logged.
3. Periodic security assessments shall be carried out to ensure that the integrity of the site is maintained and cannot be compromised.

8.13.4 Security of Electronic Office Systems

Purpose

Electronic office systems like mobile phone, telephones, and fax machines, lap top etc. shall be controlled to prevent unauthorized disclosure or misuse.

Roles

Role	Description/Responsibility
Head of Administration	Responsible for the availability and safety of electronic office systems.
User	Should ensure authorized business use of electronic office systems.

Policy

Intercom & Direct dialing facilities

Intercom and direct dialing facilities are provided to employees. Employees shall use these facilities for official purpose only. The intercom extension number shall be allotted by the administration department. The intercom

numbers and direct numbers directory shall be updated and made available to employees by the administration department.

Facsimile (FAX)

1. The company provides facsimile facility, which is available within departments. Each message incoming/outgoing shall be attended by administration department. In case sensitive information is to be received, the concerned personnel shall confirm the time from the sender and receive the fax in person.
2. Information transmitted via fax shall include a Dvara KGFSL fax cover page with a disclaimer that the information sent is for the use of the intended recipient only.

Dispatch of mails through postal/courier agencies

1. All dispatch of mails shall be handled by the Administration department. Employees are required to submit the concerned item to the Administration department for dispatch. Records of all couriers shall be maintained by the Administration department.
2. Administration department shall ensure that reliable couriers are used for transport of data.

9. Access control policy

9.1 Purpose

Access to information systems shall be controlled on the basis of business and security requirements.

9.2 Policy

As one of the critical requirements of information security, the company shall implement an effective process for access to its information assets.

1. The user is granted access to the information based on roles and responsibilities and access is granted only on need basis. Access shall be provided to meet following two principles:

- Need-to-know: The user is granted access only to the information that is required to perform the assigned tasks.
- Need-to-use: The user is granted access only to the information processing facilities according to the tasks assigned.

2. There must be a formal user access provisioning and de-provisioning procedure for granting access to information, information processing systems & IT services.
3. All users shall have controlled access (read, write, modify, execute, full control) to information processing systems, in accordance with the user's functional role and information security requirements.
4. For Contract Employees and Consultants, the validation of the ID must be only for the period of contract and must be automatically de-activated thereafter. There must also be a periodic review of the same.
5. A record of disabled accounts must be maintained by the IT Administrator or HR team member concerned.
6. User-ID must be automatically de-activated after five login failures. This user ID shall have session timeout of five minutes.
7. All information processing systems shall be configured to enable fault logging and audit trails.

9.3 User access management

9.3.1 Purpose

To ensure that formal process is in place to control access to information systems and services.

9.3.2 Policy

User access

1. Access to information assets shall be authorized by the company only where a valid business need exists and only for the specific time period for which the access is required.
2. The various factors that shall be considered when authorizing access to user and information assets include:
   - Business role
   - Physical location
   - Method of connectivity
   - Remote access
   - Time
   - Anti-malware and patch updation status
   - Nature of device used and software /operating system

3. The provision of access shall involve various stages like identification and authentication which involves determination of the person or IT asset requesting access and confirmation of the purported identity and authorization. This process shall involve an assessment of whether access is allowed to a user or information asset by the request or based on the needs of the business and the level of information security required.

4. The company shall take appropriate measures to identify and authenticate users or IT assets. The required strength of authentication shall be commensurate with risk. The techniques that shall be considered for increasing the strength of identification and authentication include
    - The use of strong password techniques (i.e. increased length, complexity, reuse limitations and frequency of change)
    - Increasing the number and/or type of authentication factors
    - The recommended password parameters are:
        - Minimum Length - 8 characters
        - Complexity - Enabled (for e.g., at least one special character and one numeral)
        - Max password age – 90 days
        - Max failed login attempts – 5

5. The examples where increased authentication strength may be required, given the risks involved include :
    - Administration or other privileged access to sensitive or critical IT assets
    - Remote access through public networks to sensitive assets and activities carrying higher risk like third-party fund transfers, etc.
6. The period for which authentication is valid shall be commensurate with the risk.
7. The important controls that the company shall consider are:
    - A systematic process of applying and authorizing the creation of user ids and the access control matrix shall be set up
    - Conducting a risk assessment and granting access rights based on the same. For example, contractors and temporary staff would have higher inherent risks
    - Implementing role-based access control policies designed to ensure effective segregation of duties
    - Changing default user names and/or passwords of systems
    - Prohibiting sharing of user ids and passwords including generic accounts
    - Modification of access rights whenever there is a change in role or responsibility and removal of access rights on cessation of employment

- Processes to notify in a timely manner the concerned application owner/Functional head regarding user additions, deletions and role changes
- Periodic reconciliation of user ids in a system and actual users required to have access and deletion of unnecessary ids, if any
- Audit logging of access to IT assets by all users and monitoring of critical access to IT assets on a periodic basis.
- Regular reviews of user access by information asset owners to ensure appropriate access is maintained.
- Considering de-activating user ids of users of critical applications who are on prolonged leave.

8. Company shall consider using automated solutions (Single Sign-On etc.) to enable effective access control and management of user ids. Such solutions shall also be managed effectively to ensure robust access management.
9. For accountability purposes, the company shall ensure that users and IT assets are uniquely identified and their actions are auditable.
10. Transaction processes and systems shall be designed to ensure that no single employee/outsourced service provider could enter, authorize and complete a transaction.
11. Segregation shall be maintained between those initiating static data and those responsible for verifying its integrity. Further, segregation shall be maintained between those developing and those administering application systems.
12. Systems shall be tested to ensure that segregation of duties cannot be bypassed.
13. Mutual authentication system, also called as two-way authentication system shall be considered.
    - Mutual authentication, also called two-way authentication, is a security feature in which a client process must prove his identity to a server, and the server must prove its identity to the client, before any application traffic is sent over the client-to-server connection.
    - Identity shall be proved through a trusted third party and use of shared secrets or through cryptographic means as with a Public Key Infrastructure (PKI)

User registration

1. Access to multi-user information services and other applications shall be controlled through a formal user registration process.
2. User registration forms shall be used to create users in the system.
3. Unique employees IDs shall be assigned to the employees to ensure accountability of individual users for their activities.
4. Employees shall be provided with access privileges which would permit them to carry out their job responsibilities only.

5. Elevated privileges shall be assigned to any user only based on a valid business need and after obtaining requisite approval from the concerned Operations Head and/or IT Head.
6. Employees shall be responsible for all activities performed using their personal IDs.
7. Employees ID shall not be used by anyone other than the individual to whom it has been assigned.
8. Employees shall not allow others to perform any activity using their IDs.
9. Application owners shall explicitly identify documents and systems classified as highly sensitive by carrying out a risk assessment.
10. Employees shall use information processing equipments for authorized business purposes only. Incidental personal use shall be allowed as long as it does not interfere with the business activity and productivity.
11. For employees with similar duties, role based access controls (RBAC) shall be used to assign access to individual accounts based on job descriptions, duties or function.
12. User IDs shall be disabled if any user does not require logon to the system for more than thirty days. After the employee returns, the ID shall be re-enabled based on approval from reporting manager.
13. Distinct IDs shall be assigned to temporary staff, contractors that can be easily identified and shall automatically expire after certain time interval.

Review of Access Rights

- User access reviews shall be carried out quarterly to ensure that only authorized users have access, and privileges allocated to the users are in line with their current roles.
- IT department and/or the business application owner shall review the access rights and privileges of users in the event of promotion, demotion, transfer or termination of employment.
- Privileged accounts (such as administrator accounts, service accounts or other accounts that can override access controls) shall be reviewed by the business / application owners in coordination with IT team periodically and shall be reviewed by the IT Head.
- All default access credentials shall be removed when application moves from pre-production to production environment and same shall be reviewed.

Password Policy

Password Management

1. Initial temporary password shall be provided to the employees and they shall be forced to change it on first logon. All users of information systems must have the responsibility to ensure that strong passwords are chosen.
2. Temporary passwords shall be provided when employees forget their passwords only after identification of the users.
3. New passwords shall be provided to the employees in a secure manner with an appropriate proof-of-identity of the intended employee.
4. Passwords shall be a minimum length of 8 characters and conform to password standards. Passwords shall comprise of letters, numbers and special characters.
5. Password History shall be minimum 5 for the critical applications / services and 3 for the Desktops / non – critical systems
6. Account lock out shall be 5 [failed logons occur due to wrong passwords]
7. Initial passwords shall not be easily associated with the user (e.g., social security number, [Employee] ID number, address, numerical equivalent of name, etc.) or easy to guess words.
8. Passwords shall be changed every 90 days.
9. Passwords shall not be stored in clear text on the computer system.
10. Passwords shall not be transmitted in clear text.
11. Passwords shall not be visibly displayed when being entered in the system.
12. Vendor supplied default passwords shall be modified before the system is used in the operational environment.
13. Password protected screensavers shall be implemented on all PCs and servers. The screensaver must activate after five minutes of inactivity.

Super User password policy

1. SU passwords shall be allocated only to the system owners who have a business need to login as super user. Passwords of all administrative accounts/Super User (SU) shall be kept in a sealed cover with the IT/ Operations Head. The super user password policy shall be as follows.
    - For IT personnel who require the SU password on any critical server or system, there shall be a formal security clearance process.
    - IT Admin shall send a formal request to the IT Head for granting SU privilege to the concerned personnel with proper business justification.
    - Upon approval from the IT Head, the concerned Functional Head shall issue the SU password of a server/system to the employee.
    - Detailed list of personnel provided with SU privileges shall be maintained by the IT Head and reviewed periodically.

- Super user password shall be used by the concerned employee for carrying out his/her job responsibility only. Any other use of the password is not permitted under any circumstances.
- Audit tracking mechanism shall be enabled on the critical servers and detailed activity log of critical servers shall be reviewed on a periodic basis.
- Super user password of employees who no longer has the need for the same shall be revoked immediately. SU passwords shall be changed with immediate effect in this case to prevent misuse or unintentional compromise. The same shall apply in the event an employee with SU privilege resigns or is terminated.
- Violation or unauthorized disclosure of the SU password by any employee would invite severe disciplinary action including and up to termination & legal prosecution.

Password use

1. Employees shall be responsible for selection of password, their use and management as a means to control access to the systems.
2. Employees shall not share their passwords with anyone and shall be responsible to maintain the confidentiality of passwords. Employees must follow the following guidelines:
    - Passwords shall have a minimum length of eight characters.
    - Passwords shall be a combination of alphanumeric characters and special characters.
    - Passwords shall not be easily guessable like, names, telephone numbers, date of birth, etc.
    - Passwords shall be never shared or revealed to anyone else regardless of the circumstances.
    - Normal user passwords shall be changed every 90 days and the passwords of privileged accounts shall be changed every 30 days.
    - Employees shall change their passwords whenever there is an indication of system or password compromise.
    - Any event of password compromise shall be raised as an incident and brought to the attention of the IT Head or Audit team on priority.
    - Employees shall change their temporary passwords on first logon. Passwords shall not be written down.
    - Employees having access to multiple information systems shall maintain different passwords for these systems.
    - Employee account shall be locked after three consecutive unsuccessful logon attempts.

3. Security administrators shall perform password testing on a quarterly basis using password auditing tools. Procedures for using password auditing tools shall be established to ensure that sensitive information is not disclosed and it is only performed by trained personnel.

4. An interactive password management system shall be put in place to ensure quality passwords. Password management procedures shall be developed.

Unattended User Equipment

1. Employees shall be responsible for safeguarding the information assets installed in their areas.
2. Active sessions shall be secured by locking the workstation, password protected screen saver, etc.
3. Network printers shall be appropriately secured. Employees shall ensure that any sensitive information being printed on the printer shall be closely supervised.

9.4 Application Access Control

9.4.1 Purpose

To prevent unauthorized access to information held in information systems. Security facilities shall be used to restrict access within all the application systems of the company.

9.4.2 Logical Access

Logical access controls shall be implemented on data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques shall include user-ids, passwords, smart cards or other biometric technologies.

Logical access to software and information shall be restricted to authorized users and include the following controls:

- Restrict user access to information and application system functions, in accordance with their corresponding job profiles and are approved by application owners.
- Access to database shall be restricted to only IT Administrators.
- Access must be restricted for any utility and operating system software that is capable of overriding system or application controls.
- Computers, databases and applications that store user account and password information shall restrict access to the information to only authorized personnel. This access shall be reviewed quarterly and coincide with a technical review of the host, server and user store.
- Operating systems providing authentication services must not transmit passwords in clear text. Passwords must not be visibly displayed on the system when being entered.

- Sensitive operating system files, which are more prone to hackers, shall be protected against all known attacks using proven tools and techniques. The users shall not be able to modify them without the permission of system administrator.

9.4.3 Information access restriction

Users of application systems, including support staff, shall be provided with access to information and application system functions in accordance with a defined access control policy, based on individual business application requirements. Application of the following controls shall be considered in order to support access restriction requirements:

- Providing menus to control access to application system functions
- Restricting users' knowledge of information or application system functions which they are not authorized to access, with appropriate editing of user documentation
- Controlling the access rights of users, e.g. read, write, delete and execute
- Ensuring that outputs from application systems handling sensitive information contain only the information that is relevant to the use of the output and is sent only to authorized terminals and locations, including periodic review of such outputs to ensure that redundant information is removed

9.4.4 Isolation of Application servers

1. It is recommended that all unnecessary services on the application server such as ftp, telnet shall be disabled. Secure Shell (SSH) shall be used instead of telnet. The application servers shall be isolated from the e-mail servers.

9.5 Corporate Internet Usage Policy

9.5.1 Purpose

The company shall develop controls to establish effective internet security. The company's internet systems shall be used for official and authorized purposes only. Incidental and occasional personal use of internet is permitted, provided that it does not interfere with the legitimate interest of the company.

9.5.2 Roles

Role	Description/Responsibility
User	Follow the internet usage policy.

9.5.3 Policy

1. Access to internet shall be made available to employees only as per business need and the same shall be used only for business purposes.
2. Internet access shall be provided only after a risk assessment has been carried out by the IT Team to enforce any restrictions if applicable and also only if their role requires personnel to access internet for their job functions.
3. Use or downloading of tools not related to work are disallowed. These applications pose a potential virus and security threat to system functionality and compatibility concerns, in addition to professional integrity and legal implications.
4. Users provided with the internet facility shall have only http / https services. Services like telnet, FTP shall be disabled by default and require approval for use from the IT Head.
5. All internet connections shall pass through a firewall and/or a proxy server.
6. Internet usage within the office premises or through office assets shall not be available for any unauthorized/ unethical activities. Unauthorized use of Internet shall include, but is not limited to:
   - Using the internet for personal entertainment, personal business or profit, and publishing personal opinions.
   - Soliciting money, personal gain, or any transactions conducted in an illegal manner.
   - Attempting to gain or gaining unauthorized access to any computer system of the company or any other organization.
   - Sending racial, sexually abusive, threatening, defamatory or harassing messages.
   - Sending, transmitting or distributing proprietary information, data or other confidential company information.
   - Performing deliberate acts (non-business related use) that waste computer resources like uploading and downloading large files, accessing streaming audio and/or video files, playing games on the Internet and engaging in online chat groups.
   - Introducing computer viruses, worms, or Trojan horses.
   - Downloading obscene written material or pornography.
7. Connecting to internet through PDA's, mobile phones is strictly prohibited in the data center and other sensitive installations of the company.

8. Access to the internet from the company owned laptop or through the company owned connections shall adhere to the same policies as those within the company facilities.
9. Any software needed for business purposes, can be installed by IT Team, provided:
    - The software has been verified by IT/Operations Head for use within the company.
    - The software has been scanned for viruses using the latest virus definition files.
    - The conditions for use of software have been met.
10. All software shall be installed after adhering to the licensing requirements and obtaining proper approvals.
11. Trial version of any software in use shall be deleted after the trial period or the software shall be procured to comply with the licensing requirements.
12. The Audit team shall periodically review workstations to verify that only approved and licensed software has been installed and running.
13. While using internet, all staff shall maintain the highest standards of professional conduct. The company shall not tolerate unprofessional use of the internet, such as any activities related to chain letters, other solicitations, pornography, and offensive/threatening communications etc.
14. Any employee who violates this policy shall be subject to disciplinary action, legal prosecution including termination from service.

10. Network security controls

10.1 Purpose

The purpose of network security controls is to ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

10.2 Roles

Role	Description/Responsibility
Team Lead – IT Infra	Responsible for the safeguarding of information in networks and the protection of the supporting infrastructure.

IT Team	Responsible for ensuring the safeguarding of information in networks and the protection of the supporting infrastructure.

10.3 Policy

1. The company shall build defense in depth (i.e. multiple layers of defenses) to obtain the optimal level of security for protecting its perimeter and computing environment.
2. To control the flow of traffic through network borders and to police its content looking for attacks and evidence of compromised machines, Boundary defenses shall be multi-layered using the following devices

   ► Firewalls
   ► Proxies
   ► Network based Intrusion Prevention Systems and Intrusion Detection Systems.

3. Effective multi-layered defenses of perimeter networks shall be created to help lower the number of successful attacks, thereby allowing security personnel to focus on attackers who have devised methods to bypass boundary restrictions.
4. The company shall perform the following actions prior to configuring the network:
   ► Identifying the various applications and systems accessed via the network
   ► Identifying all access points to the network including various telecommunications channels like Ethernet, wireless, frame relay, dedicated lines, remote dial-up access, extranets, internet
   ► Mapping the internal and external connectivity between various network segments
   ► Defining minimum access requirements for network services
   ► Determining the most appropriate network configuration to ensure adequate security and performance for the company
5. In addition to the above, the following controls shall be implemented for improving the security of networks:
   ► Maintaining inventory of authorized and unauthorized devices and software.
   ► Secure configurations/hardening shall be performed for all hardware and software on Laptops, Workstations, and Servers and Network Devices such as Firewalls, Routers and Switches.
   ► Well-tested and documented security baselines for various systems shall be maintained.

► identifying all connections to critical networks and conducting risk analysis including necessity for each connection. All unnecessary connections to critical networks shall be disconnected.
► Implementation of the security features recommended by device and system vendors.
► Establishing strong controls over any medium that is used as a backdoor into the critical network. If backdoors or vendor connections do exist in critical systems, strong authentication
shall be implemented to ensure secure communications.
► Implementation of internal and external intrusion detection system, incident response system and establishing 24x7 incident monitoring.
► Performing technical audits including vulnerability assessment of critical devices and networks, and any other connected networks, to identify security concerns.
► Conducting physical security surveys and assessing all remote sites connected to the critical network and evaluating their security.
► The Company shall also identify and assess any source of information including remote telephone / computer network / fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points.
► The Company shall identify and eliminate single points of failure.
► The Company shall establish a rigorous, ongoing risk management process.
► The Company shall establish a network protection strategy and layered security based on the principle of defense-in-depth.
► Additionally, each layer shall be protected against other systems at the same layer.
► The Company shall establish system backups and disaster recovery plans.
► The Company shall conduct trainings to minimize the likelihood that the company personnel inadvertently disclosing sensitive information regarding critical system design, operations, or security controls through social engineering attempts.
► Any requests for information by unknown persons/source need not be entertained.
► Network control functions shall be performed by individuals possessing adequate training and experience.
► Network control functions shall be separated, and the duties shall be rotated on a regular basis, where possible.
► Network control software shall be used to restrict operator access from performing certain functions (e.g., the ability to amend/delete operator activity logs).
► Network operation standards and protocols shall be documented and made available to the operators, and shall be reviewed periodically to ensure compliance.

This policy applies to:

- LAN and WAN network infrastructure at Primary and DR site deployed and maintained by Dvara KGFS
- Relevant third party personnel responsible for administering and maintaining Dvara KGFS IT infrastructure
- All Infrastructure Coordinators and Infrastructure Specialists administering and maintaining the network infrastructure viz. LAN and WAN
- All IT assets used to build the network viz. network devices, communication links and assets that use the network viz. servers, desktops, smart devices owned by Dvara KGFS.

10.3.1 Segregating Server and User Segments

1. A list of mission critical servers or servers processing sensitive information shall be prepared.
2. List of critical servers shall be periodically reviewed and updated by IT Head. All critical servers shall be separated from LAN users by creating dedicated server segments on firewalls by the IT Team.
3. The user segment and the server segments must be distinct and access between them must be controlled.
4. Servers segments shall be segregated and secured from user LAN by firewalls and continuously monitored by IT team for any malicious or abnormal traffic.
5. In addition to firewall rules, all critical servers shall have restrictive access control policies configured which provide access to users on "Need to know" and "Need to Access" basis only.
6. Internet facing servers and servers accessed by external parties like the Extranet etc. shall be hosted on a separate segment.
7. Utility servers shall be on a separate segment. (Server Segment)
8. Application and database servers shall be protected by placing them on separate protected segment. This segment shall be accessible to authorized users only.
9. Intrusion Prevention System (IPS) shall be strategically installed at network segments to monitor the traffic flowing, to and from critical servers.

10.3.2 Segregation of Development & Production Facilities

1. Production systems shall be segregated from development and testing systems to mitigate unwanted modifications to live systems.
2. Development and testing personnel shall not have direct access to production systems. If required, such access shall be through strict authorization and access control.
3. Development, UAT and Production environment shall be segregated from each other with adequate access rights.

10.3.3 VPN Connectivity

1. Any approval for Remote access via Internet to Dvara KGFS IT systems shall be granted by IT/Operations Head.
2. Remote access to network resources must be done using the SSL / IPsec VPN infrastructure provided by Dvara KGFS. SSL must always be used for remote desktop protocol or SSH.
3. Secure remote access must be strictly controlled via strong authentication.
4. IT Head shall conduct quarterly audit of the VPN users.
5. The use of remote access to Dvara KGFS IT systems is strictly prohibited without a reasonable and documented business reason illustrating the necessity to complete job responsibilities.
6. Laptops or desktops must comply with host integrity checks before access is provided. All hosts that are connected to Dvara KGFS internal networks via remote access must use up-to-date anti-virus signatures.
7. Split tunneling must be disabled, whereby employees and contractors' computer remotely connected to the Dvara KGFS corporate network, cannot connect to any other network simultaneously.
8. The VPN system shall automatically disconnect sessions upon reaching an idle time of 15 minutes.
9. Remote access for vendors shall be enabled to the test and development environment upon receiving a written request, with adequate business justification and approved by IT/Operations Head.
10. It is prohibited to copy, move, or store Dvara KGFS data into local hard drives and removable media while using remote access to IT systems. Such data includes but not restricted to configuration files, database files, transaction records etc. Company shall consider the usage of DLP (data leakage prevention) solutions to monitor and restrict such copying of data.

10.3.4 Network Servers (e.g.: Mail, File and Print Servers)

1. A detailed inventory with s/w and h/w configuration details shall be maintained by the respective administrators.

2. The network services, application or other utility software getting installed in a server, shall be identified, approved and documented.
3. Hardware redundancy mechanisms shall be adopted for all major application and network servers.
4. Disk Mirroring (writing data to two separate hard drives simultaneously), Disk duplexing (installing two hard drives and two disk drive control cards) or redundant drive arrays (RAID) shall be used for all the servers which have requirement for high availability.
5. The Administrator shall take necessary action to protect information contained in a Server that has reached its end of life e.g. erase or reformat disks etc.
6. The purpose of each Server on the network shall be identified and how the Server would be used shall be documented.
7. Following issues shall be considered while deploying network server:
   - The categories or classification of information that shall be stored in the server.
   - The security requirements for that information.
   - The network services that shall be provided by the network server.
   - The security requirements for the network services.

10.3.5 Installing Network Operating Systems

1. A documented procedure for installing a network Operating System shall be developed and followed.
2. All critical parameter settings, scripts and configuration files used during installation of a network operating system shall be documented.
3. A trusted and more stable version of the operating system shall be installed, wherever possible to prevent easier cracking of passwords or security breaches.
4. Default passwords shall be immediately changed as part of the installation process.

10.3.6 Updating the Network Operating System

1. The respective administrators (Network, Security and System) shall be responsible for installing necessary security-related software updates in a timely manner.
2. The installation of updates shall take into account the following security issues :
   - Any temporary vulnerable state that may arise during the update process
   - Unavailability of services due to inappropriate scheduling of updates
   - Impact on other dependent services due to untested updates

- Unauthorized change due to inadequate change management process

3. Authorized sources of security advisory feeds e.g. mailing lists, vendor publications, vendor web sites, etc. for information about security problems and software updates shall be maintained and regularly monitored.
4. Procedures shall be implemented to control the installation of software on operational systems.

10.3.7 Securing Application Services

1. Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.
2. Information involved in application service transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

10.4 Network management controls

Network management controls shall be established to protect networks from attacks by hackers / unauthorized users from within and outside. The company shall implement the following network management controls:

- The hardware configuration of the critical network servers shall be documented.
- The network services installed on a server shall be identified and documented. This shall help to identify any unauthorized services running on the server.
- Disk mirroring (writing data to separate hard drives simultaneously), Disk Duplexing (installing two hard drives and two disk drive control cards) or drive arrays shall be used for the servers housing critical data such as the file server or where applicable.
- The IT team shall take necessary action to protect information contained on a server that is no longer in use e.g. erase and reformat disks.
- No servers shall be exposed directly to the internet. All servers under the company's custody shall be placed on internal zone of firewall.
- Servers, which are required to be accessed from the Internet, shall be deployed securely and their IP addresses shall be noted. Security of these servers shall be controlled by the IT team.
- Documented guidelines for hardening network operating systems shall be developed and followed.
- System default settings shall be reviewed prior to installation to determine potential security holes. Settings that could potentially

compromise security shall be changed prior to the system being placed in a production environment.

- Default passwords shall be changed as part of the installation process.
- Each network user shall have a unique user account and password.
- All user accounts shall be associated with an applicable, informative full name and description.
- 'Guest' accounts shall be disabled.
- Password controls
- The number of unsuccessful login attempts allowed for a user account shall be limited to five. Any further attempts to login shall be rejected.
- User accounts, which are inactive for a period of 30 days, shall be disabled.
- The minimum length of passwords shall be set as 8 characters.
- The operating system shall force users to change the password at the time of initial logon, where possible.
- A password expiration period of 90 days shall be set in the System
- Password 'recycling' shall be prevented. Histories of last 5 passwords or passwords entered during the last 12 months shall be retained.
- Appropriate file and directory permissions shall be set up in the operating system so that users are restricted to information and data on a 'need to know, need to do' basis.
- The systems administrators shall be responsible for installing necessary security-related patches, service packs and other software updates in a timely manner.
- A list of sources (mailing lists, vendor publications, vendor web sites, etc.) for information about security problems and software updates for the network operating systems shall be developed.
- The system administrators shall regularly monitor these information sources.

10.5 Network login process

The following controls shall be established by the company to control network login:

- The login process shall not provide any help messages, which may aid an unauthorized user.
- After successful login, every user shall be given information reflecting the last login time and date and details of any unsuccessful login attempts since the last successful login, wherever possible.
- A warning banner shall be displayed at login to any system. This shall constitute a special notice, that includes:
  - The system is to be used only by authorized users.

- The user represents that he/she in an authorized user by continuing to use the system.
- Use of this system constitutes consent to monitoring.
- The legal department in consultation with the IT/Operations Head shall verify the possible legal issues related to the text put in the banner.
- The banner shall not include any system or application identifiers, which may provide valuable information to a possible intruder e.g. hardware and operating system present on the host, information about the Company or other internal matter.
- All unsuccessful login attempts shall be recorded.

10.6 System and Network Logging

1. A table of sample log categories and types of log information within each category are listed below:

Log Category	**Types Of Log Information**
Users	Details of failed logon attempts, attempted logins to privileged accounts, users created
Networks	Service initiation requests: name of the user/host requesting the service; network traffic; new connections.
Applications	Applications and services specific information e.g. mail logs, ftp logs, web server logs, firewall logs, router logs

2. Only authorized users shall have access to utilities that reconfigure logging mechanisms.
3. The log files shall be protected from being accessed or modified by unauthorized users.
4. A quarterly review of the logs shall be performed by the IT Head.

10.7 Mobile Computing and Communications

1. Access to the company's system through mobile computing / teleworking shall be restricted and only be granted after approval from IT/Operations Head.
2. Data encryption and cryptographic technique shall be implemented to ensure secure transmission of data and information.
3. Trainings shall be conducted for mobile computing users to raise awareness on risks.
4. Wireless LAN access shall be restricted and allowed to users\locations only after authorization from the IT team.

5. Records for access allocation and revocation from the company network systems for mobile / teleworking users shall be maintained. The information for revoking the access shall be provided by the Dept Heads.

10.8 Network device protection

Network devices shall have an appropriate level of security to prevent unauthorized access to the company's network. These devices shall be placed in physically secure locations.

10.8.1 Router protection

1. Routers and consoles shall be housed in a physically secure location.
2. IP spoofing shall be prevented for boundary routers by using the following controls:
   - All inbound packets with a source address originating from the company's internal network shall be dropped.
   - All outbound IP packets with source addresses other than the internal network shall be dropped.
   - All unnecessary ICMP traffic shall be dropped
3. Routers shall be configured to ensure that a user has to enter a login Id and password to gain access to the command prompt through an encrypted session like SSH.
4. Any user who gains access to the command prompt shall not have administrator privileges by default.
5. Router passwords shall be stored (e.g. in router configuration files) in a secured form (such as MD5 Encryption or protected file).
6. Router passwords shall be changed every 90 days.
7. Routers shall have appropriate login banners.
8. All routers being monitored via SNMP shall have non-default SNMP community strings.
9. Routers not being monitored via SNMP shall have SNMP disabled.
10. Routers shall be set to a console session time out of 15 minutes and shall be connected using SSH.
11. Access to the router configuration files shall be restricted to authorized individuals.
12. All maintenance fixes shall be applied on the routers during non-peak or off business-hour times.
13. Routers shall have a backup of the latest configuration.
14. The router audit logs shall be monitored on a daily basis.
15. Any changes to the router configuration must be approved by the Dvara IT team prior to implementation.

10.8.2 Switches Protection

1. Switches shall be housed in a physically secure location.
2. Any user who gains access to the command prompt shall not have administrator privileges by default.
3. Password shall be changed every 90 days.
4. Switches shall have appropriate login banners
5. Switches shall be set to a console and VTY session time out of 5 minutes (if possible).
6. The switch related configuration would be restricted to authorized individuals.
7. All maintenance fixes shall be applied on the switches during non-peak or off business-hour times.
8. The switch related configuration information would be properly documented and stored.

10.9 Segregation of Networks

1. The Company's Data Center shall not be accessed by any personnel including third parties at any point of time without approval. The network shall be logically segregated from the corporate LAN. Servers within the Data Center shall be further segregated based on operational requirements. The Company network shall be segregated based on criticality of traffic.
2. All systems shall be placed in logically different network segments.
3. IT infrastructure shall be capable of supporting logical segregation.
4. Manageable network switches shall be used at all organizational premises.
5. Access to application and other related servers shall be permitted through firewalls only.
6. Any changes to the network architecture must be approved by the Dvara KGFS IT team.

10.10 Firewall policy

1. Firewalls are security systems that control and restrict both internet connectivity and internet services. Firewalls shall be used establish a perimeter where access controls are enforced. The firewall policy described below states the management's expectation for how the firewall shall function. The policy address the following aspects

- Firewall topology and architecture and type of firewalls being utilized,
- Physical placement of the firewall components.
- Permissible traffic and monitoring firewall traffic
- Firewall updating

- Coordination with security monitoring and intrusion response mechanisms, responsibility for monitoring and enforcing the firewall policy
- Protocols and applications permitted
- Regular auditing of a firewall's configuration and testing of the firewall's effectiveness, and contingency planning.

2. The company shall select the firewall based on the following characteristics of the security zone,

- The amount of traffic
- The sensitivity of the systems and data
- Applications

3. The types of firewalls include

- Packet filter firewalls
- Stateful inspection firewalls
- Proxy server firewall
- Application level firewall

4. Acceptable inbound communication types for the company shall be explicitly defined in the firewall policies.
5. As the firewall is usually one of the first lines of defense, access to the firewall device itself shall be strictly controlled.
6. Company shall reduce its vulnerability to attacks through network configuration and design, sound implementation of its firewall architecture that includes multiple filter points, active firewall monitoring and management, and integrated security monitoring.
7. The following controls shall be implemented by the company at the firewall level:

- Using a rule set that disallows all inbound and outbound traffic that is not specifically allowed
- Using NAT and split DNS to hide internal system names and addresses from external networks
- Using proxy connections for outbound HTTP connections and filtering malicious code
- Hardening the firewall by removing all unnecessary services and appropriately patching, enhancing, and maintaining all software on the firewall unit
- Restricting network mapping capabilities through the firewall, primarily by blocking inbound ICMP (Internet Control Messaging Protocol) traffic
- Backing up firewalls to internal media and not backing up the firewall to servers on protected networks
- Logging activity, with daily administrator review and limiting administrative access to few individuals
- Using security monitoring devices and practices to monitor actions on the firewall and to monitor communications allowed through the firewall

- Administering the firewall using encrypted communications and strong authentication, accessing the firewall only from secure devices, and monitoring all administrative access
- Making changes only through well-administered change control procedures and based on approval of Dvara KGFS IT team.

8. The firewall shall be configured for authorized outbound network traffic to contain that a compromised host inside the network, prevent it from communicating outbound to their controller.
9. Only authorized services shall be allowed in the firewall and all other services shall be blocked (default to denial).
10. The reason for each firewall rule shall be documented as comments along with the name of the personnel who added/modified the rule along with change request and approval for the same.
11. The following are the acceptable outbound connections

- SMTP to any address from the SMTP mail gateway(s)
- DNS to any address from an internal DNS server to resolve external host names
- HTTP and HTTPS from an internal proxy server for users to browse web sites
- NTP to specific time server addresses from an internal time server(s)
- Any ports required by Anti-Virus, spam filtering, web filtering or patch management software to only the appropriate vendor address/addresses to pull down updates

12. To the extent that filtering is done on a signature basis, review of signatures shall be performed on a periodic basis.
13. Perimeter routers and firewalls shall be configured to enforce policies that forbid the origination of outbound communications from certain computers. Additionally, proxy servers shall be configured to identify and block customer data and other data that are not to be transmitted outside the secure domain.
14. The application servers and other related servers shall not be exposed to the internet directly.
15. Firewall shall have adequate capability to support the sustained high traffic throughput.
16. Access to firewall shall be restricted to authorized personnel.
17. All suspicious activity which might be an indication of unauthorized usage or an attempt to compromise security measures shall also be logged.
18. Logs shall be reviewed periodically to ensure that the firewalls are operating in a secure manner.
19. Failed attempts to log directly into the firewall system shall be immediately notified to the firewall administrator in the form of an automated alarm, either by email, pager or any other means.
20. The firewall system administrator shall review log files on a daily basis and investigate any unusual activity.

21. Firewall logs shall be periodically backed up and archived for a period of minimum six months.
22. The firewall application shall always have the latest vendor issued patches installed.
23. The firewall administrator shall evaluate each new release of the firewall software to determine whether an upgrade is required. However the firewall administrator shall verify with the vendor whether such an upgrade is really required and take the approval of Dvara KGFS IT Head before proceeding with the same.
24. After any upgrade, the firewall shall be tested to verify the proper functioning prior to going operational.
25. Any feature in the firewall that is not needed, including used shells and applications shall be disabled.
26. A complete system backup of the firewall configuration shall be taken before migration to production environment.
27. Complete Firewall configuration backup would be taken whenever any changes are made to the firewall.
28. Backups shall be performed when the firewall system traffic is low. This shall ensure that the throughput of firewall is not degraded during business hours.
29. In case of a firewall break-in, the firewall administrator(s) are responsible for reconfiguring the firewall to address any vulnerability that was exploited.
30. Any changes to the firewall configurations and/or rule set must be formally approved by the Dvara KGFS IT team.

10.11 Wireless security

1. To mitigate risks associated with the wireless data communication, the company shall use encryption to authenticate users and devices and to shield communications.
2. The company shall also evaluate the risk and implement appropriate additional controls. The additional controls may include one or more of the following:
    - Treating wireless networks as untrusted networks, allowing access through protective devices similar to those used to shield the internal network from the Internet environment
    - Using end-to-end encryption in addition to the encryption provided by the wireless connection
    - Using strong authentication and configuration controls at the access points and on all clients
    - Using an application server and dumb terminals

- Shielding the area in which the wireless LAN operates to protect against stray emissions and signal interference
- Monitoring and responding to unauthorized wireless access points and clients

3. All wireless Access Points / Base Stations connected to the corporate network shall be registered and approved by IT Head of the company.
4. The Access Points / Base Stations shall be subjected to periodic penetration tests and audits.
5. Updated inventory on all wireless Network Interface Cards used in corporate laptops or desktops shall be maintained.
6. Access points/Wireless NIC shall not be installed /enabled on the company's network without the approval of IT Head.
7. Company shall ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need.
    - The company shall deny access to those wireless devices that do not have such a configuration and profile.
8. Company shall ensure that all wireless access points are manageable using enterprise management tools.
9. Network vulnerability scanning tools shall be configured to detect wireless access points connected to the wired network. Identified devices shall be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points shall be deactivated.
10. Company shall use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromise.
11. In addition to WIDS, all wireless traffic shall be monitored by wired IDS as traffic passes into the wired network.
12. Where a specific business need for wireless access has been identified, company shall configure wireless access on client machines to allow access only to authorized wireless networks.
13. For devices that do not have an essential wireless business purpose, company shall disable wireless access in the hardware configuration (BIOS or EFI), with password protections to lower the risk that the user shall override such configurations.
14. Company shall regularly scan for unauthorized or mis-configured wireless infrastructure devices, using techniques such as "war driving" to identify access points and clients accepting peer-to-peer connections. Such unauthorized or mis-configured devices shall be removed from the network, or have their configurations altered so that they comply with the security requirements of the organization.

15. The company shall ensure all wireless traffic leverages at least AES encryption used with at least WPA2 protection.
16. The company shall ensure wireless networks use authentication protocols such as EAP/TLS or PEAP, which provide credential protection and mutual authentication.
17. Company shall ensure wireless clients use strong, multi-factor authentication credentials to mitigate the risk of unauthorized access from compromised credentials.
18. Company shall disable peer-to-peer wireless network capabilities on wireless clients, unless such functionality meets a documented business need.
19. Company shall disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.
20. Company shall configure all wireless clients used to access other critical networks or handle organization data in a manner so that they cannot be used to connect to public wireless networks or any other networks beyond those specifically allowed by the company.
21. A periodic review of MAC id's and DHCP IP reserved list must be performed to ensure that only authorized users have ability to connect to Dvara KGFS network and access the internet.
22. Dvara KGFS IT team shall approve any changes to the authorized wireless access point list.
23 VPN Policy
    - VPN use is to be controlled using either a one-time password authentication Active Directory Integrated.
    - When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
    - Dual (split) tunneling is NOT permitted; only one network connection is allowed.
    - VPN gateways will be set up and managed by Dvara KGFS IT team.
    - All computers connected to Dvara KGFS internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (Symantec End Point protection 12.1); this includes personal computers.
    - The VPN Firewall is limited to an absolute connection time of 24 hours.
    - Users of computers that are not Dvara KGFS owned equipment must configure the equipment to comply with company's VPN and Network policies.
    - Only Forti Client approved VPN clients shall be used.

10.12 Remote access

1. The management shall establish policies restricting remote access and be aware of all remote-access devices attached to their systems. These devices shall be strictly controlled.
2. While using TCP/IP Internet-based remote access, company shall establish a virtual private network over the Internet to securely communicate data packets over this public infrastructure.
3. The company shall implement the following controls for remote access:

- Disallowing remote access by policy and practice unless a compelling business need exists and requiring management approval for remote access
- Regularly reviewing remote access approvals and rescind those that no longer have a compelling business justification
- Appropriately configuring and securing remote access devices
- Appropriately and in a timely manner patching, updating and maintaining all software on remote access devices
- Using encryption to protect communications between the access device and the company and to protect sensitive data residing on the access device
- Periodically auditing the access device configurations and patch levels
- Using VLANs, network segments, directories, and other techniques to restrict remote access to authorized network areas and applications within the institution
- Logging remote access communications, analyzing them in a timely manner, and following up on anomalies
- Centralize modem and Internet access to provide a consistent authentication process, and to subject the inbound and outbound network traffic to appropriate perimeter protections and network monitoring
- Logging and monitoring the date, time, user, user location, duration, and purpose for all remote access including all activities carried out through remote access
- Requiring a two-factor authentication process for remote access (e.g., PIN based token card with a one-time random password generator, or token based PKI)
- Implementing controls consistent with the sensitivity of remote use. For example, remote use to administer sensitive systems or databases may include the controls like restricting the use of the access device by policy and configuration, requiring

authentication of the access device itself and ascertaining the trustworthiness of the access device before granting access

4. Intrusion detection systems and virus scanners able to decrypt the traffic for analysis and then encrypt and forward it to the VPN endpoint shall be considered as preventive controls.
5. The company shall terminate all VPNs to the same end-point in a so called VPN concentrator, and shall not accept VPNs directed at other parts of the network.

10.13 Security against Denial of Service Attacks

1. Company shall be responsive to unusual network traffic conditions/system performance and sudden surge in system resource utilization which could be an indication of a DDoS attack.
2. The company shall deploy appropriate tools to effectively detect, monitor and analyze anomalies in networks and systems.
3. As part of the defense strategy, company shall install and configure network security devices for reasonable preventive/detective capability.
4. Potential bottlenecks and single points of failure vulnerable to DDoS attacks shall be identified through source code review, network design analysis and configuration testing.
5. Company shall consider incorporating DoS attack considerations in their ISP selection process.
6. An incident response framework shall be devised and validated periodically to facilitate fast response to a DDoS onslaught or an imminent attack.
7. Company shall be familiar with the ISPs' incident response plans and suitably consider them as part of their incident response framework.
8. To foster better coordination, company shall establish a communication protocol with their ISPs and conduct periodic joint incident response exercises.

10.14 Cryptographic Controls Policy

10.14.1 Purpose

Encryption shall be used for Dvara KGFS IT Department's sensitive information that is stored in non-secure locations or transmitted over external networks.

The purpose of this policy is to include requirements for managing cryptographic keys though their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys.

- Cryptographic controls can be used to achieve different information security objectives, e.g.:
- Non-repudiation: using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action;
- Authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.
- Confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;
- Integrity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information;

10.14.2 Policy

1. The encryption techniques and algorithms shall be identified, evaluated and agreed before implementing them in the organization.
2. Transmission of sensitive and confidential data with external parties shall be authenticated by use of digital certificates.
3. The key length for encryption shall be at least 128 bits.
4. Application services shall make use of secure authentication methods, e.g. using public key cryptography and digital signatures to reduce the risks. Also, trusted third parties can be used, where such services are needed.

10.14.3 Regulations

1. Encryption algorithms are governed by various rigorous international controls on the export, import, use and transfer of products containing an encryption capability.
2. The permissibility of use shall be established for the purposes and locations intended.
3. Controls over the use of encryption changes rapidly and if required, expert advice shall be taken before making any decisions in using the encryption, selecting appropriate cryptographic controls to meet the Information Security Management System policy objectives.

4. Dvara KGFS shall consider its needs for keeping copies of keys or parts of keys used for cryptographic controls, either for their own use or to satisfy legal requirements.

10.14.4 Use of certificates

Digital certificates shall be used in transactions where there is need for authentication, non-repudiation and encryption.

10.14.5 Use of Security Tokens

1. Two factor authentication mechanisms using secure tokens shall be considered to authenticate users trying to access critical applications.
2. Two factor authentication tokens issued to customers/partners for authentication to gain access to Dvara KGFS IT infrastructure should follow Third Party & Outsourcing Services Policy or Asset Management Policy in case of loss of equipment.

11. Information Systems Acquisition, Development and Maintenance

11.1 Purpose

The systems acquisition development and maintenance policy is intended to ensure that changes are applied in a controlled and consistent manner so that stability and security of the systems are not compromised.

11.2 Role

Role	Description/Responsibility
IT/Operations Head	Responsible for changes are applied in a controlled and consistent manner so that stability and security of the systems are not compromised.

11.3 Policy

1. Information security shall be considered at all stages of an information asset's life-cycle like planning, design, acquisition and implementation, maintenance and disposal.
2. The company shall apply systematic project management oriented techniques to manage material changes during these stages and to ensure that information security requirements have been adequately addressed.
3. The company shall put in place planning and design level controls to ensure that
    - Information security is considered in the overall information systems architecture
    - The implemented solutions are in compliance with the information security policies and requirements of the company.

11.4 Planning / Requirement Phase

1. The business (the requesting department) is expected to provide the approved Business Requirements. All requirements need to be measurable and testable and relate to the business need.
2. A risk analysis shall be performed to determine the threats associated and the corresponding security and quality controls required for the requested system or system application under development.
3. It shall be ensured that there is a balance between user requirements and Security & Quality controls.
4. Specifications for the new system shall be documented to provide the in-house development team or vendor with specific requirements. This enables Dvara KGFS in identifying, reviewing and testing the security functionalities of the system or software.

11.5 Acquisition/ Design /Development Phase

1. The following points shall be considered at a minimum while preparing the detailed requirements for the system application:
    - Impact on existing systems
    - Security vulnerabilities involved when connecting with other systems and applications
    - Operating environment security
    - Cost of providing security to the system over its life cycle (includes hardware, software, personnel and training)

2. While purchasing a system or software, the security requirements shall be specified in the Request for Proposal and the selection criteria shall be based on secure functionality.
3. There shall be a separation between the production, test and development environments.
4. All development and new systems shall be checked for malicious and mobile code embedded within the software.
5. Application controls shall be designed into all application systems to prevent loss, modification or misuse of user data. These controls shall include:
   - Validation of input data;
   - Control of internal processing;
   - Message Integrity;
   - Validation of output data
6. Where software development is outsourced, the following points shall be considered:
   - Licensing arrangements, code ownership and intellectual property rights
   - Certification of the quality and accuracy of the work carried out
   - Escrow arrangements in the event of failure of the third party
   - Rights of access for audit of the quality and accuracy of work done
   - Contractual requirements for quality of code
   - Meeting compliance regulations
7. The physical characteristics of the system are designed during this phase. The operating environment is established, major subsystems and their inputs and outputs are defined, and processes are allocated to resources. Everything requiring user input or approval must be documented and reviewed by team leader and peers. The physical characteristics of the system are specified and a detailed design is prepared. Subsystems identified during design are used to create a detailed structure of the system. Each subsystem is partitioned into one or more design units or modules. Detailed logic specifications are prepared for each software module.
8. The detailed specifications produced during the design phase are translated into hardware, communications, and executable software by coding/building the system, etc. Software shall be unit tested, integrated, and retested in a systematic manner after the coding is complete.
9. Trainings and Manuals
   - **Manual**: The updated system manual should be available for both users and technical team to use and/or support the system effectively.
   - **Training**: The business/functional trainings to be provided for business users, UAT In-charge, Application Support and Technical training to be provided for other peers-in-Development, Application Support, and Technical Support/Operation, etc., for managing and supporting the system

10. Client server interaction between the servers should be thoroughly tested through simulation before system is handed.

11.6 Testing Phase

1. All modifications, enhancements and installation of new systems shall be subject to testing for sanity, capacity, peak loading, etc.
2. The appropriate users shall do design testing and unit testing on the new systems prior to installation into the production environment.
    - **Test Cases & Unit Test**: The developers should prepare the test cases and do the adequate unit tests of their work before placing the work to the team leader (Nominated by the Project Head).
    - **System Integration Test**: The team leader should review/update test cases and test to ensure various components of the system are integrated and functioning as per the functional requirements.
3. Where production data is copied or used in the test system, it must be subject to a similar level of controls as the live version.
4. Separate authorization shall be required every time the operational data is used for testing.
5. Use of sensitive customer information or confidential information shall be avoided.
6. Sensitive operational information or personal information shall be depersonalised/ scrambled.
7. Copying or use of operational information shall be logged to provide an audit trail.
8. Operational information shall be erased from a test application system immediately after the testing is complete.
9. User Acceptance Testing-During User Acceptance Test, actual business user shall tests the system to ensure that the business requirements, as defined in the requirements document, are satisfied by the developed or modified system.
10. The implementation of operating systems, patches/upgrades, or standards non-companying systems in which there were no-customizations, will skip the detailed testing, however must undergo compatibility check or certification (from vendor) to ensure that the production environment shall not be disturbed if implemented.

11.7 Implementation Phase

1. Before the implementation of any new system, a security procedure document shall be prepared for the new system. (It should contain hardware specification, prerequisites, implementation steps for client,

server (UNIX, Windows, etc.), database, proposed system architecture showing interaction with other subsystems and data flow, application server, system parameters setup, access control configurations, other security setup, roll-out plan, information required for support, etc.)

2. For software packages, system default settings shall be reviewed prior to installation to determine potential security holes.
3. The system or system modifications shall be installed and made operational in a production environment using approved 'Implementation Specification'. The phase is initiated after the system has been successfully tested and accepted by the user and concerned parties during User Acceptance Phase. This phase continues until the system is operating in production in accordance with the defined user requirements.
4. Different implementation approach such as Pilot, Soft Live, Parallel Run or Complete Live shall be selected depending on the project nature and complexity.

11.8 Operations/Maintenance Phase

1. The IT team or vendor shall maintain the system and perform identified IT Operations activities, and will support the users of the system.
2. The system shall be monitored by the users (those who use the system) for continued performance in accordance with user requirements.
3. All requisite procedures for operational tasks shall be documented. Access to this documentation shall be restricted.
4. All changes to the system shall be carried out in line with the Change Management Procedure and approved by Dvara KGFS IT team.
5. Libraries containing application source code, production executable, and systems audit tools shall be secured from unauthorized access and only an authorized librarian shall have "read-write" access to these libraries.
6. The development staff shall not have access to operational systems. For occasional and essential support purposes, the development staff may be granted special access for a limited period of time.
7. The necessary privileges given during the development phase for service and administration accounts should be revoked before the go live stage.
8. System utilities like compilers, source code, and editors shall be disabled from the operational systems.
9. An audit log shall be maintained of all updates to operational systems and system applications.

11.9 Disposition Phase

1. The Disposition phase is the last phase of SDLC when the system is disposed of and the task performed is either eliminated or transferred to other systems.
2. The business user shall request for disposition of a system with a valid reason, and the reason shall be studied and recommended by the IT Head and approved by Dvara KGFS CEO.
3. The disposition activities should ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information may be reactivated in the future if necessary, or the data is effectively migrated to another system or archived in accordance with applicable records management regulations and policies, for potential future access.
4. Disposal or re-use of systems shall be in accordance with its classification.
5. Disposal or re-use of systems shall be recorded and the asset register shall be updated accordingly.

11.10 Controlled Environment

The company shall ensure that separate development, test and production environments exist for the business application systems.

- The test and development applications shall be accessible only by the test and development team (in-house or vendor)
- The test environment shall be isolated from the development environment to prevent any unintentional modifications of the application under development or the system itself.
- The designated IT team shall move modified source code after completion of development, unit testing and integration testing to the application server.
- Only the authorized personnel from IT team or authorized vendor shall have write access to the application executables and libraries in the production environment.
- Dvara KGFS IT team shall be responsible for monitoring all activities performed by outsourced software development firms engaged by the company.
- All outsourced development shall be reviewed and approved by IT/Operations Head.
- Different logon procedures shall be used for production and development systems, to reduce the risk of confusion.

11.11 Migration Controls

1. A documented roadmap / migration plan / methodology for data migration shall be created to cover the following
   - Verification of completeness, consistency and integrity of the migration activity
   - Pre- and post-migration activities along with responsibilities and timelines for completion of same.
2. Explicit sign offs from users/application owners shall be obtained after each stage of migration and after complete migration process.
3. Audit trails shall be maintained to document the conversion, including data mappings and transformations.
4. The following key aspects shall be considered by the company during migration:
   - Integrity of data
     - Indicating that the data is not altered manually or electronically by a person, programme and substitution or overwriting in the new system.
     - Integrity also includes error creep due to factors like transposition, transcription, etc.
   - Completeness
     Ensuring that the total number of records from the source database is transferred to the new database (assuming the number of fields is the same)
   - Availability of data under conversion
     Ensuring that data is backed up before migration for future reference or any emergency that might arise out of the data migration process
   - Consistency of data
     - The field/record called for from the new application shall be consistent with that of the original application.
     - This shall enable consistency in repeatability of the testing exercise
   - Continuity
     Ensuring that the new application shall be able to continue with newer records as addition (or appendage) and help in ensuring seamless business continuity
5. The last copy of the data before conversion from the old platform and the first copy of the data after conversion to the new platform shall be maintained separately in the archive for any future reference.
6. The error logs pertaining to the pre-migration/ migration/ post migration period along with root cause analysis and action taken shall be available for review.
7. The company shall migrate the complete transaction data and audit trails from the old system to the new system. In case complete migration is not possible the company shall have the capability to access

the older transactional data and piece together the transaction trail between older and newer systems, to satisfy any supervisory/legal requirements that may arise.

11.12 Change Request

1. Any changes to software applications shall be only implemented on the basis of formal change requests, which shall be authorized as per change management process.
2. Changes to the systems shall only be implemented on the basis of a formal change request form. CEO or Operation Head shall approve all change requests.
3. The change request form shall contain a brief description of the changes requested, the date on which the request was made, prioritizing of the request, tracking and controlling modifications and assigning a unique number to each change request.
4. The IT team shall retain all change request forms, program change test plans and testing results consistent with company's record retention standards.

11.13 Source Code Management

Access to source codes of software shall be controlled. The following are the controls that the company shall implement:

- There shall be one repository for production source code, maintained in an authorized code management system. Developers shall retrieve the source code from this repository when modifying programs.
- A backup copy of the application source code, maintained in secure media, shall be properly safeguarded in a secure off-site location.
- Only authorized IT personnel shall have access to the application source code repository.
- All modifications or customizations carried out on the application shall have strict version control.
- Application-wise records of modifications made till date shall be maintained to have a snapshot of various changes made to the source codes.
- Test and development team personnel shall be allowed read only access to the application source code repository.
- Only authorized IT personnel shall have update access to the production source code repository.

11.14 Version Control

Software versions shall be controlled in order to ensure that changes are applied to the correct releases and versions of software. The following are the controls that the company shall implement

- Software shall be held in secure libraries in a secure server and the libraries shall be qualified using the release and / or version number to distinguish different versions.
- Modified programs and the application software shall be assigned a higher version number following a change.
- The content of each version shall be documented providing a brief description of the system elements that are included.
- System documentation shall be subjected to version control and versions of documentation shall be related to the corresponding application versions.
- Version controls shall be periodically reviewed by the IT Head to ensure that they remain effective.
- The Data Owner shall ensure that all application changes / updates/ patches are installed in a timely manner.

11.15 Retention Requirements

The minimum retention requirements involving system development and maintenance policies shall be followed.

- The IT team shall retain all change request forms and change documentation.
- The data owner shall also retain a copy of the change request form.
- In addition to the change request forms, all program change test plans and test results shall be retained.
- The current version and immediate prior production versions of each application, if any shall be retained. All prior versions shall be archived to backup media.

11.16 Implementation of New Technologies

1. The company shall carry out due diligence with regard to new technologies to reduce any additional risk exposures.
2. The company shall authorize the large scale use and deployment in production environment of technologies after taking into consideration the following
    - The technology should have matured to a state where there is a generally agreed set of industry-accepted controls

- Robust diligence and testing has been carried out to ascertain the security issues of the technology
- Compensating controls are sufficient to prevent significant impact and to comply with the company's risk appetite and regulatory expectations.

3. A signoff shall be taken from the Audit team before moving the system to production to evaluate if all the security controls implemented in the system is operational.
4. Any new business products introduced along with the underlying information systems shall be assessed as part of a formal product approval process which incorporates the following
   - Security related aspects
   - Fulfillment of relevant legal and regulatory prescriptions
5. Company shall develop an authorization process involving a risk assessment balancing the benefits of the new technology with the risk.

11.17 Vulnerability Assessment

1. The company shall scan for vulnerabilities and address discovered flaws proactively.
2. The company shall take the following measures to address the vulnerabilities:
   - Automated vulnerability scanning tools shall be used against all systems on a periodic basis.
   - Company shall ensure that vulnerability scanning is performed in an authenticated mode (i.e., configuring the scanner with administrator credentials) at least quarterly.
   - The company shall consider the following scanning methods to overcome limitations of unauthenticated vulnerability scanning
     - Scan using the agents running locally on each end system to analyze the security configuration
     - Remote scanners that are given administrative rights on the system being tested
   - The company shall compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or by documenting and accepting a reasonable business risk.
   - Acceptance of business risks for existing vulnerabilities shall be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed increasing the risk.

- Vulnerability scanning tools shall be tuned to compare services that are listening on each machine against a list of authorized services.
- The tools shall be also tuned to identify changes over time on systems for both authorized and unauthorized services.
- The information security team shall maintain the updated status regarding numbers of unmitigated, critical vulnerabilities, for each division and plan for mitigation.
- The information security team shall periodically share vulnerability reports indicating critical issues with senior management for effective mitigation.

11.18 Audit Trails

1. Company shall ensure that audit trails exist for IT assets satisfying the company's business requirements including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution.
2. The audit trails shall include:
   - Transactions with financial consequences
   - The opening, modifications or closing of customer accounts
   - Modifications in sensitive master data
   - Accessing or copying of sensitive data/information
   - Granting, modification or revocation of systems access rights or privileges for accessing sensitive IT assets
3. Audit trails shall be secured to ensure the integrity of the information captured, including the preservation of evidence.
4. Retention of audit trails shall be in line with business, regulatory and legal requirements.
5. The following activities shall be performed for securing the integrity of log files:
   - Encrypting log files that contain sensitive data or that are transmitting over the network
   - Ensuring adequate storage capacity to avoid gaps in data gathering
   - Securing back-up and disposal of log files
   - Logging the data to write-only media like a write-once/read-many (WORM) disk or drive
   - Setting logging parameters to disallow any modification to previously written data
6. The following additional controls shall related to logging shall be considered:

- All remote access to an internal network, whether through VPN, or other mechanism, shall be logged verbosely
- Operating systems shall be configured to log access control events associated with a user attempting to access a resource like a file or directory without the appropriate permissions
- Security personnel and/or administrators designated in this regard shall identify anomalies in logs and actively review the anomalies, documenting their findings on an ongoing basis
- Company shall have least two synchronized time sources in its network from which all servers and network equipment retrieve time information on a regular basis, so that timestamps in logs are consistent
- Network boundary devices, including firewalls, network-based IPSs, and inbound and outbound proxies shall be configured to log verbosely all traffic (both allowed and blocked) arriving at the device
- Company shall consider deploying a Security Information and Event Management (SIEM) system tool for log aggregation and consolidation from multiple machines/systems and for log correlation and analysis

7. Furthermore, event logs may be correlated with information from vulnerability scans to fulfill the following objectives
   - The activity of the regular vulnerability scanning tools themselves is logged.
   - Correlate attack detection events with earlier vulnerability scanning results to determine whether the given exploit was used against a known-vulnerable target.
8. Application systems shall be designed and installed to capture and maintain forensic evidence in a manner that maintains control over the evidence, and prevents tampering and the collection of false evidence.
9. In instances where processing systems and related audit trails are the responsibility of a third-party service provider,
   - The company shall ensure that it has access to relevant audit trails maintained by the service provider.
   - The company shall also ensure that the audit trails maintained by the service provider meet the company's standards.

12. Security Incident Management

12.1 Purpose

The purpose of incident management is to ensure a consistent and effective approach to the management of incidents including communication on events / incidents. By implementing incident handling procedures, the company shall

guide the employees/contractors to restore normal operations quickly and efficiently consequent to an incident. The incident management procedures shall ensure that

- Competent personnel handle the issues related to incidents within the organization.
- Incidents shall be reported through appropriate management channels as quickly as possible.
- Contact details of authorities, external interest groups or forums that handle the issues related to incidents are maintained.

Information Security Event is an identified occurrence of failure of system/ service /operation /function/network resulted on account of a possible breach of information security policy or absence/failure of necessary safe guards or a previously unknown situation, which is security relevant.

An **information security incident** is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security of the organization.

12.2 Roles

Role	Description/Responsibility
Incident Management Committee (IMC)	The IMC defines procedures to proactively address potential threats/ risks arising out of incidents. The effectiveness of the incident management process /procedure shall be reviewed by IMC annually. All major incidents shall be reported to IMC in detail and all minor incidents shall be reviewed by IMC. CEO- Chairman IT Head- Member Operations Head- Incident Response Leader CFO- Member
Incident Response Leader	Responsible for evaluating and resolving the incident and coordinates the escalation process with the help of IRC. In consultation with IT Head, Incident Response Leader may decide to commission special audit/ inspection of application/ circumstance leading to the incident.

Divisional Heads/ Regional Heads	Divisional Heads/ Regional Head shall be accountable for the response/resolution and closure of incident in their respective area.
IT Head	IT Head shall be consulted for closure of the incident and shall report the incidents to the higher management. IT Head has to ensure that employees are aware of the incidents through periodic training / circulars etc. Training materials need to be updated in coordination with the HR team.
Representative from Audit Team	Need to attend the IMC meeting, based on the type of the incident.
Incident Response Coordinator/Single Point of Contact	Incident Response Coordinator/Single Point of Contact is the designated First point of contact for reporting of events. IRC has to work in coordination with the Incident Response Leader and shall be responsible for communicating/reporting the incidents to other stake holders in IRT. ► IRC shall prepare the Incident Report Form after the resolution of the incident narrating the steps taken to mitigate the issue in consultation with IRL and other division heads. ► IRC is responsible for maintaining and updating the list of all emergency contact details of the entire Incident Response Team, vendors, suppliers, service providers etc.
Employee/User	Incident identification/reporting – Ensuring suspected incidents that are identified are reported

12.3. Policy

1. A robust incident management process shall be in place to maintain the capability to manage incidents within the company, to enable containment of exposures and to achieve recovery within a specified time period.
2. Company shall have clear accountability and communication strategies to limit the impact of information security incidents through defined mechanisms for escalation and reporting to the board and senior management and customer communication.
3. Incident management processes shall also assist in compliance with regulatory requirements.
4. The company shall pro-actively notify CERT-In/IDRBT/RBI regarding cyber security incidents.
5. Major activities that shall be considered as part of the incident management framework include:
    - Developing and implementing processes for preventing, detecting, analyzing and responding to information security incidents
    - Establishing escalation and communication processes and lines of authority
    - Developing plans to respond to and document information security incidents
    - Establishing the capability to investigate information security incidents through various modes like forensics, evidence collection and preservation, log analysis, interviewing, etc.
    - Developing a process to communicate with internal parties and external organizations (e.g., regulator, media, law enforcement, customers)
    - Integrating information security incident response plans with the organization's disaster recovery and business continuity plan
    - Organizing, training and equipping teams to respond to information security incidents
    - Periodically testing and refining information security incident response plans
    - Conducting post-mortem analysis and reviews to identify causes of information security incidents, developing corrective actions and reassessing risk, and adjusting controls suitably to reduce the related risks in the future
6. All security incidents or violations of security policies shall be brought to the notice of IT, Operations and Audit Head, and the Board based on severity of the incident.

13. Disaster Recovery and Business Continuity Management

13.1 Purpose

The purpose of Disaster Recovery and Business Continuity Management process is to reduce the disruption caused by disasters and security failures to an acceptable level through a combination of preventive and recovery controls.

13.2 Risk Assessment and Impact Analysis

Risk Management is the process of identifying vulnerabilities and threats to an organization's information resource in achieving business objectives and deciding what countermeasures, if any, to take in reducing risk to an acceptable level based on the value of the information resource to the organization. The Company shall adopt a comprehensive ***Risk Assessment approach*** in protecting the Risks associated with information processing facilities based on the Value of an asset, the vulnerabilities it is exposed to and the likelihood of occurrence of a threat along with potential impact to the companying operations shall be systematically calculated and treated.. Business Impact Analysis (BIA) is the most important phase in the Business Continuity Planning exercise. In order to be fully effective, a Business Continuity Plan (BCP) must have its recovery time frame and priorities defined by the needs of the department and functions that operate within the organization. By understanding the potential impact of an incident on each process, the organization can prioritize its processes for recovery.

13.2.1 Roles

Role	Description/Responsibility
IT Team	Responsible for conducting periodic Risk Assessment and Impact Analysis.
IT/Operations Head	Responsible for reviewing and approving the Risk Assessment and Impact Analysis results.

13.2.2 Policy Frequency

The Risk Assessment and impact analysis shall be carried out as and when there is a major change to the IT infrastructure, introduction of new operations, migration of operations to new facilities or at least once a year. An external consultant may be hired for the task if, required.

13.2.3 Strategy

The Recovery Strategy adopted must be documented and approval obtained from management. A final risk assessment summary must be presented as part of the Risk Assessment report, which is then used for Disaster Recovery and Business Continuity Planning.

13.2.4 Approach

In order to gather the required information and to facilitate identification, comparison and prioritization of business processes, one-on-one meetings are conducted with the help of BIA templates. The interviews are conducted with all Department Heads /Functional / Other Heads for discussing and analyzing the pre-filled BIA templates.

The survey is designed to collect the following information:

- Business Processes.
- Critical Recovery Time.
- Resources for critical processes.
- Identification of existing alternatives for the resources for critical processes.
- Process interdependencies.
- Various impact of process failure.

The respondents are asked to identify all the business processes within their departments and identify their Critical Recovery Time to evaluate the impact on the Company in the event of disruption of the business processes when they are needed the most. The various impacts due to the unavailability of business processes are rated as High, Medium and Low. This information is subsequently ratified with the head of the respective department. A BIA report is made and submitted to management for approval.

13.3 Disaster Recovery and Business Continuity Plan

Disaster Recovery and Business continuity planning is a process designed to reduce the Company's risk for an unexpected disruption of the critical functions/operations necessary for the survival of the organization.

13.3.1 Roles

Role	Description/Responsibility
IT Team	Responsible for maintaining Disaster Recovery and Business Continuity Plan.
IT/Operations Head	Responsible for reviewing , approving Business Continuity Plan and DR Drill activities

13.3.2 Policy

- The plan shall be developed to restore the business operations in the required timeframe following interruptions due to failure of critical processes.
- Disaster Recovery and Business Continuity Plan must include all issues related to recovery of information systems and data, which are critical for business operations. Further, each plan must specify the conditions for activating the plan and the individuals responsible for executing the plan.
- BCP/DR plan shall also factor in and provision for any unforeseen outages across the facilities of the Company.
- Disaster Recovery and Business Continuity Plan shall be issued to identified and authorized personnel only. Adequate education activities must be conducted to create understanding and awareness about the business continuity plan.
- Disaster Recovery and Business Continuity Plan shall include the roles and responsibilities to be performed by the contingency team members, in the event of a contingency.
- Alternate and temporary locations which are used for Business Continuity Planning purposes shall have security controls which are consistent with the main site. The same shall be reviewed and approved in consultation with Information Security Committee.
- Disaster Recovery Strategies

Prior to selecting a Disaster recovery (DR) strategy, an individual Disaster recovery planner should refer the key metrics of recovery point objective and recovery time objective for business processes:

Recovery Point Objective (RPO) –The acceptable latency of data that will be recovered. The Recovery Time Objective (RTO) is the time within which a business process must be restored, after a Major Incident (MI) has occurred, in order to avoid unacceptable consequences associated with a break in business continuity. RTO is the as time between the point of a service disruption due to some form of disaster and the point in time at which critical business and technical resources are operationally available for service delivery to an acceptable level. For example, if a Data Center failure occurs, the time between the point of failure and the point at which branch is ready to service the customer can be taken as RTO.
Recovery Time Objective (RTO)–The acceptable amount of time to restore the function
The Recovery Point Objective (RPO) is expressed backward in time (that is, into the past) from the instant at which the Major Incident (MI) occurs, and can be specified in seconds, minutes, hours, or days. The recovery point objective (RPO) also is thus the maximum acceptable amount of data loss.

RPO and RTO are the measures of recovery objectives before and after the occurrence of disaster, respectively. Smaller values are more desirable for both RPO and RTO.

The amount of Data Loss, in the event of a disaster is difficult to predict, as it is dependent on

- The nature of the disaster &
- The time period of occurrence.

With the given technical setup, based on volume of log data created during an average business day if the log data files (in sequence) are available at the DR Site, the corresponding transactions can be recreated. Thus the amount of transaction data lost is the amount of log data files lost at the Primary Site or the log data files not copied/available at the DR Site since copying/transferring log files is the easiest and simplest method to keep the database at DR site as synchronized as possible with primary database.

All copies of Business Continuity Plans shall be distributed to concerned Managers/Officers whenever the plans are updated or modified.

13.4 Disaster Recovery and Business Continuity Plan Testing

13.4.1 Purpose

Testing is an essential element in the BCP/DR effort and is performed to ensure that critical functions can, in fact, be accomplished according to the plan and that all components of the plan (i.e., personnel, hardware, software, logistical, and administrative, etc.) function as expected.

13.4.2 Policy Frequency of Testing

The Disaster Recovery and Business Continuity Plan shall be tested whenever the entire plan is reviewed. Plan is reviewed annually but is not limited to the same.

13.4.3 Mock Drill

The disaster recovery plan shall be tested from time to time using scheduled mock drills. A mock drill usually will not affect active / production operations. It will be a simulator for conducting live/ actual DR drill. Mock drills help establish the possible impacts, operational issues, application performance etc. The outcome of the mock drill and precaution measure will be taken and necessary updation will be considered in the actual/live drill.

However, if it is known that operations will be affected, the drill should be carefully scheduled such that the effect is minimal and is done during a permissible window. These activities should be regarded similar to regular equipment maintenance activities that results in operations downtime. The experience of the mock drill should be updated in the disaster recovery plan document and the review will be conducted by IT Head.

13.4.4 Documentation of Test Results

During every phase of the test, detailed documentation of observations, problems and resolutions are maintained. Documentation includes the following:

- Personnel availability, responsiveness, and qualifications.
- Instruction and procedure adequacy, and ease of use.
- Transportation support availability and adequacy.
- Vendor and supplier responsiveness.
- Back-up programs, data, documentation, and system recovery procedures.
- Task list of problems to resolve.
- Sign-off shall be obtained from IT/Operations Head and the Business.

14. Compliance

14.1 Introduction

The design, operation and use of information systems shall be subject to regulatory and contractual requirements to avoid legal impact. Compliance to security policy shall be demonstrated to implement secure processes.

14.2 Use of Authorized Software

1. A list of all software approved for usage in the Dvara KGFS shall be maintained by IT/Operations Head.
2. Users are permitted to use only approved software. Use of any other software, without authorization from IT /Operations Head shall be strictly prohibited.
3. No unlicensed software, shareware (beyond its period of free use), public domain software or pirated software shall be used on the company's computer equipment.
4. Software, once installed on a system, shall not be copied other than for backup purposes.
5. Personal and private CD writers, Zip drives, DAT drives, pen drives shall not be allowed in office premises unless authorized by the IT Head.
6. Personnel who breach information security by using unauthorized software shall be subjected to strict disciplinary action.
7. The Audit team shall head the periodic review that is conducted to ensure that no unauthorized software is being used. All software found in violation shall be removed immediately.

14.3 Purchase and Regulation of Software Use

1. All requests for purchasing of software shall be sent to IT/Operations Head. The decision for purchasing of software shall be taken by the respective division heads with necessary permission from CEO.
2. As appropriate, licenses shall be obtained for all standard products.
3. Each department shall be responsible for ensuring that all requirements of the license agreement are confirmed to. These agreements may specify specific user restrictions such as the number of copies allowed to be installed, the number of machines the software can be installed or the number of concurrent users of the software allowed at any one time.
4. The concerned divisions shall conduct periodic reviews to monitor software usage to confirm adherence to the regulations.

5. Number of sessions or number of named users shall be tracked, where possible, in an automated manner (e.g. SMS), to comply with software license agreement.

14.4 Legal

14.4.1 Purpose

The design, operation and use of information systems shall be subject to regulatory and contractual requirements to avoid breaches of regulatory or contractual obligations.
This section provides the guidelines to company to take necessary actions for identifying and addressing the operational and legal risks (related to IT) to which the company is exposed.

14.4.2 Roles

Role	Description/Responsibility
IT Head	Ensure that, ▶ The legal risks arising from cyber laws are identified and addressed. ▶ The concerned functions are adequately staffed ▶ The staffs are trained to carry out the relevant tasks. ▶ Incorporate legal risks as part of operational risk framework ▶ Take steps to mitigate the risks involved in consultation with legal department of the company.
Audit Team	▶ Ensure legal compliance in the company ▶ Advise the business groups on the legal issues arising out of the use of IT with respect to the legal risk identified and referred to them by the operational risk group. ▶ Define security requirements for compliance to local regulations for data protection and privacy.

14.4.3 Policy

Due to the increased number of cybercrimes, the impact of cyber laws is critical and the company shall aim to minimize any risk arising.

The company shall comply with the rules and regulations of Information Technology Act, 2000 (IT Act, 2000) which was enacted to handle IT related issues and the IT Amendment Act, 2008 which addressed more issues such as cybercrimes.

14.4.4 Critical aspects in handling operational and legal risks

1. As legal and operational risks are same, the company shall take necessary actions to cover these risks by documentation, particularly where the law is silent. The documentation done by the company shall be the solution to the legal risks that may arise in their companying activities.
2. The company shall be exposed to operational risk (direct or indirect), resulting in loss due to inadequate or failed internal processes, people and systems or from external events.
3. The company shall keep in view the specific provisions of IT Act, 2000 (as amended in 2008), various judicial and quasi-judicial pronouncements and related developments in the cyber laws in India as part of legal risk mitigation measures.
4. Further, the company shall keep abreast of latest developments in the IT Act, 2000 and the rules, regulations, notifications and orders issued there pertaining to company transactions and emerging legal standards on digital signature, electronic signature, data protection, cheque truncation, electronic fund transfer etc. as part of overall operational risk management process.

14.4.5 IT related legal compliance

1. Relevant statutory, regulatory, and contractual requirements for all the information system processing facilities shall be documented. Compliance management shall be reviewed on an annual basis.
2. From a legal perspective, security procedure adopted by the company for authenticating users shall be recognized by law as a substitute for signature. In India, the Information Technology Act, 2000, in Section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. Any other method used by the company for authentication shall be recognized as a source of legal risk and a risk assessment pertaining to the same shall be performed by the company.
3. Results of risk assessment to the critical application systems and servers shall be ratified with the legal department before the same is closed by the IT Head.
4. Adequate risk control shall be instituted by the company for the internet companying operation to ensure that customer accounts confidentiality

and secrecy are protected as per IT Act 2000 Section 3(2) (Para 7.5.1 – 7.5.4).

5. Legal department shall work with the IT Head, marketing and the companying operations department to ensure that customers are clearly notified of the timeframe and the circumstances in which any online stop – payment instructions could be accepted as per IT Act 2000. The same shall be consulted and made part of the process in the event that the stop payment facility is made available through the internet companying.
6. Before using trademarks, logos, images or publications belonging to a third party, authorization shall be obtained from the owners. The software copyright license agreement with the vendor shall be fully complied with. The staff shall be made aware of copyright policy and advised not to commit any breach of the same. Appropriate controls shall be implemented to ensure that the maximum number of users permitted to use the software is not exceeded. Periodical checks shall be carried out to ensure that only authorized software and licensed products are installed in the company.
7. Breach or failure of security systems, procedure shall be reported to RBI. RBI shall reserve the right to commission special audit/inspection based on the severity of the breach. Legal department and the IT/Audit team shall facilitate RBI for the investigation.

.

14.4.6 IT Act 2000

1. The company shall adhere to the following controls in various departments and functions with respect to IT Act 2000:
2. The company shall designate a network and database administrator with clearly defined roles.
3. The company shall have a security policy duly approved by the board of directors. There shall be a segregation of duty IT Head dealing exclusively with information systems security and IT department which actually implements the computer systems. Further, the Audit team shall audit the information systems.
4. The company shall introduce logical access controls to data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards or other biometric technologies.
5. At the minimum, the company shall use the proxy server type of firewall so that there is no direct connection between the Internet and the company’s system. It facilitates a high level of control and in-depth monitoring using logging and auditing tools. For sensitive systems, a stateful inspection firewall shall be used which thoroughly inspects all packets of information, and past and present transactions

are compared. These generally shall include a real time security alert.

6. PKI (Public Key Infrastructure) is the most favored technology for secure Internet companying services. However, as it is not yet commonly available, The company shall use the following alternative system during the transition, until the PKI is put in place:
7. Usage of SSL (Secured Socket Layer), which ensures server authentication and use of client side certificates issued by the company themselves using a certificate server.
8. The use of at least 128-bit SSL for securing browser to web server communications and, in addition, encryption of sensitive data like passwords in transit within the company itself.
9. All unnecessary services on the application server such as FTP (File Transfer Protocol), telnet shall be disabled. The application server shall be isolated from the e-mail server.
10. All computer accesses, including messages received, shall be logged. Security violations (suspected or attempted) shall be reported and follow up action taken shall be kept in mind while framing future policy. The company shall acquire tools for monitoring systems and the networks against intrusions and attacks. These tools shall be used regularly to avoid security breaches. The company shall review the security infrastructure and security policies regularly and optimize them in the light of operational requirements and changing technologies. The IT team and HR team shall educate the end-users on a continuous basis.
11. IT Team shall be responsible to undertake periodic penetration tests of the system, which shall include:
    - Attempting to guess passwords using password-cracking tools
    - Search for back door traps in the programs
    - Attempt to overload the system using DDoS (Distributed Denial of Service) & DoS (Denial of Service) attacks
    - Check if commonly known holes in the software, especially the browser and the e-mail software exist
12. The penetration testing may also be carried out by engaging outside experts (often called 'Ethical Hackers')
13. Physical access controls shall be strictly enforced. Physical security shall cover all the information systems and sites where they are housed, both against internal and external threats.
14. The company shall have proper infrastructure and schedules for backing up data. The backed-up data shall be periodically tested to ensure recovery without loss of transactions in a time frame as given out in the company's security policy. Business continuity shall be ensured by setting up disaster recovery sites. These facilities shall also be tested periodically.

15. All applications of the company shall have proper record keeping facilities for legal purposes. It may be necessary to keep all received and sent messages both in encrypted and decrypted form.
16. Security infrastructure shall be properly tested before using the systems and applications for normal operations. The company shall upgrade the systems by installing patches released by developers to remove bugs and loopholes, and upgrade to newer versions which give better security and control.

14.4.7 Penalty for IT Related Offences

IT related legal issues expose the company to legal liabilities which the company shall manage accordingly. Following are the civil and criminal liability as per the amendment in the IT Act, 2000.

- The civil liability shall consist of exposure to pay damages by way of compensation up to 5 crore under the amended IT Act and beyond five crore would result in a court of competent jurisdiction.
- Criminal liability to the top management of the company given the provisions of Chapter XI of the amended IT Act and the exposure to criminal liability could consist of imprisonment for a term which could extend from three years to life imprisonment as fine. Further, various computer related offences are listed under this legal provision.

14.5 Audit

14.5.1 Purpose

The purpose of the Information Security Audits is to ensure compliance to Information Security Policies through a system of formal planned documented audits of all elements of Information Security.

14.5.2 Compliance with the security policy

1. Information Security Audit of all departments shall be carried out periodically. Audits shall be planned to minimize risk of disruptions to the business processes.
2. The Audit team shall be responsible for conducting the audit to check compliance to security policy.
3. Department managers shall follow all escalation and/or reporting processes when noncompliance or exceptions to the company's security policy are noted.

4. Department managers shall regularly review processes and procedures within their area of responsibility to ensure security responsibilities and duties are carried out in accordance with the IS policy.
5. Review and audit results along with corrective actions shall be documented.

14.5.3 Audit Reporting and Non - conformance Closure

An audit report shall be prepared by the Audit team listing non-conformances and observations (if any). Audit report shall be submitted to the IT Head and Executive management for further action.

14.5.4 Technical compliance

Penetration testing

1. Penetration testing is defined as a formalized set of procedures designed to bypass the security controls of a system or organization for the purpose of testing that system's or organization's resistance to such an attack.
2. Penetration testing can take several forms but, in general, a test consists of a series of "attacks" against a target. The success or failure of the attacks, and how the target reacts to each attack, shall determine the outcome of the test.
3. The overall purpose of a penetration test is to determine the subject's ability to withstand an attack by a hostile intruder. As such, the tester shall be using the tricks and techniques a real life attacker might use. This simulated attack strategy allows the subject to discover and mitigate its security weak spots before a real attacker discovers them.
4. Penetration testing shall be performed to uncover the security weaknesses of a system and to determine the ways in which the system can be compromised by a potential attacker.
5. Since penetration test seldom is a comprehensive test of the system's security, it shall be combined with other monitoring methods to validate the effectiveness of the security process.
6. Penetration testing shall be conducted at least on an annual basis.

Audits

1. Company management shall be responsible for demonstrating that the standards it adopts are appropriate for the institution.
2. Auditing compares current practices against a set of policies/standards/guidelines formulated by the company, regulator including any legal requirements.

3. Audits shall not only look into technical aspects but also the information security governance process.

Assessment

1. The company shall regularly assess information security vulnerabilities and evaluate the effectiveness of the existing IT security risk management framework, make any necessary adjustments to ensure emerging vulnerabilities are addressed in a timely manner.
2. This assessment shall also be conducted as part of any material change.
    - An assessment is a study to locate security vulnerabilities and identify corrective actions.
    - An assessment differs from an audit by not having a set of standards to test against. It differs from a penetration test by providing the tester with full access to the systems being tested.
    - Assessments may be focused on the security process or the information system. They may also focus on different aspects of the information system, such as one or more hosts or networks.
3. The Audit work shall be performed by appropriately trained and independent information security experts/auditors.
4. The strengths and weaknesses of critical internet based applications, other critical systems and networks shall be identified before each initial implementation, and at least annually thereafter.
5. Any findings shall be reported and monitored using a systematic audit remediation or compliance tracking methodology.
6. Robust performance evaluation processes shall be set up to provide the company with feedback on the effectiveness of cyber security policy and technical implementation.
7. The company shall self-identify issues, conduct root cause analyses, and implement effective corrective actions that address individual and systemic problems.
8. Self-assessment processes that are part of the cyber security program shall include routine scanning for vulnerabilities, automated auditing of the network, and - assessments of organizational and individual business line security related performance.
9. Company shall manage the information security risk management framework on an ongoing basis as a security programme following project management approach, addressing the control gaps in a systematic way.

10. Technical compliance check shall be carried out every quarter for all critical systems. Automated vulnerability assessment tools shall be used to identify the vulnerabilities in systems and that the controls are effective to prevent unauthorized access to the information systems.
11. Access to the system audit tools shall be restricted. Such tools shall be kept separate from the operational systems and not held in user areas.

Appendix 1: Glossary of terms

Abbreviation	Term
Dvara KGFS	Dvara Kshitriya Gramin Finance Services
HO	Head Office
ISMS	Information Security Management System
IT Head	Information Security Committee
CFO	Chief Financial Officer
BCP	Business Continuity Planning
DR	Disaster Recovery
IPR	Intellectual Property Rights
ISP	Internet Service Provider
ASP	Application Service Provider
MSP	Managed Service Provider
BSP	Business Service Provider
PII	Personally Identifiable Information
OS	Operating System
NAC	Network Access Control
ACS	Access Control Server
DLP	Data Leak Prevention
SIEM	Security Information And Event Management
RBAC	Role Based Access Control
SU	Super User
SSH	Secure Shell
DMZ	Demilitarized Zone
ICMP	Internet Control Messaging Protocol
WIDS	Wireless Intrusion Detection System
BIOS	Basic Input / Output System
VPN	Virtual Private Network
WORM	Write Once/Read Many
IST	Indian Standard Time
SSL	Secure Sockets Layer
EV-SSL	Extended Validation - Secure Sockets Layer
MITM	Man-In-The-Middle
PC	Personal Computer
CD	Compact Disc
DVD	Digital Versatile Disc
NDA	Non-Disclosure Agreement

PDA	Personal Digital Assistant
ISDN	Integrated Services Digital Network
VSATS	Very Small Aperture Terminals
SDLC	Software Development Life Cycle
DG	Diesel Generator
UPS	Uninterrupted Power Supply
RDBMS	Relational Database Management System
RHEL	Red Hat Enterprise Linux
SANS	Sysadmin, Audit, Networking, And Security
CERT	Computer Emergency Response Team
ISACA	Information Systems Audit And Control Association
VLAN	Virtual Local Area Network
AMC	Annual Maintenance Contract
SLA	Service Level Agreement
OLA	Operational Level Agreement
USB	Universal Serial Bus
SQL	Structured Query Language
DNS	Domain Naming System
SMTP	Simple Mail Transfer Protocol
SATA	Serial Advanced Technology Attachment
DLP	Data Loss Prevention
LAN	Local Area Network
MD5	Message-Digest 5
VTY	Virtual Teletype
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
AES	Advanced Encryption Standard
TLS	Transport Layer Security
WPA2	Wi-Fi Protected Access 2
MAC	Media Access Control
TACACS+	Terminal Access Controller Access-Control System
RADIUS	Remote Authentication Dial In User Service
MIS	Management Information System
RBI	Reserve Bank Of India
IPSec	Internet Protocol Security
DES	Data Encryption Standard
IP	Internet Protocol
PKI	Public Key Infrastructure
FTP	File Transfer Protocol
DDoS	Distributed Denial Of Service

DoS	Denial Of Service
HVAC	Heating, Ventilation, And Air Conditioning
IT	Information Technology
HR	Human Resource
CEO	Chief Executive Officer
SMS	Short Message Service
OTPs	One Time Passwords