INFORMATION SECURITY POLICY

Function	Name	Designation	Sign & Date
Prepared By	Darshak Mistry	Sr. Manager – IT	23/09/2023
Reviewed By	Mr. Pawan Srivastava	Vice President - HR	23/09/2023
Approved By	Mr. Dheer Shah	Chief Finance Officer	6/10/23

CONTENTS

1.0 INTRODUCTION:

The Cyber Security Policy is a formal set of rules by which those people who are given access to company technology and information assets must abide.

The Cyber Security Policy serves several purposes. The main purpose is to inform company users: employees, contractors, and other authorized users of their obligatory requirements for protecting the technology and information assets of the company. The Cyber Security Policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.

The Cyber Security Policy also describes the user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The policy answers these questions, describe user limitations, and informs users there will be penalties that threaten the security of the company computer systems and network.

WHAT ARE WE PROTECTING?

It is the obligation of all users of the company systems to protect the technology and information assets of the company. This information must be protected from unauthorized access, theft and destruction. The technology and information assets of the organization are made up of the following components:

- Computer hardware, CPU, disc, Email, Web, Application Servers, PC systems, Application software, system software etc.
- System software: operating systems, database management system, backup and restore software, communications protocols, and so forth.
- Application Software: used by the various departments within the company. This includes custom written software applications, and commercial off the shelf software packages.
- Network hardware and software: routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

2.0 OBJECTIVE:

The objective of this document is to define Cyber Security Policy that outlines Cyber Security Framework.

3.0 SCOPE:

The scope of this policy is to all Hardware, Software, Network, and all organization operations.

4.0 LEGISLATION:

This cyber security policy defines Cyber Security framework(CSF) in line with Information Technology Act, 2008.

5.0 ORGANIZATION OF INFORMATION SECURITY:

5.1. End User (Employees, Contractors, Contract Workers): End users are responsible to adhere company policy during their day-to-day operations.

5.2. IT Department: Responsible to implement this policy and day to day monitoring for compliance of this policy.

5.3. Head IT: responsible to monitor Cyber Security Framework, monitor vulnerability and implement security system to comply this policy.

5.4. Management (Director): Responsible to provide required resources to comply this policy. Periodic monitoring to check compliance of this policy.

6.0 HUMAN RESOURCE SECURITY POLICY:

Information security is very important to help protect the interests and confidentiality of the company and its interested parties. It can not be achieved by technical means alone and must also be enforced and applied by people, and this policy addresses the same along with Human Resources being the primary objective.

6.1. Prior to Employment:

6.1.1. Screening of the candidate shall be carried out for all the employees and contractors.

6.1.2. Information on all candidates being considered for positions within the organization is collected and handled in accordance with Indian legislation.

7.0 ASSET MANAGEMENT POLICY:

IT Assets includes hardware and software within an organization Information Technology environment and valuable to organization. IT department shall manage the hardware and software throughout its lifecycle. All hardware and software are inventories.

7.1. List of Hardware shall maintained which should include minimum (Unique ID, Make, Model, Serial Number, configuration etc.)

7.2. List of Software shall maintained which should include minimum (Software ID, Make, version, System Owner etc.)

7.3. List of hardware and Software shall be reviewed periodically minimum once in a year.

7.4. The asset inventory list will be required to be updated when ever there is a new hardware/software, updates to Hardware/Software, removal and/or retirement or Hardware/Server.

7.5. The asset inventory list will be duly approved Head IT

8.0 ACCESS CONTORL POLICY:

A fundamental component of our Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Login ID and password implement access control. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

8.1. User System and Network Access:

8.1.1. All users will be required to have a unique Login ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with management & supervisory personnel and/or any other employee whatsoever. All users must comply with the following rules regarding the creation and maintenance of passwords:

- Password must be complex i.e. combination of alphabet, Numbers and/or Special character.
- Password must not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools".
- Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the terminal.
- Password should change in interval of 90 days.
- User accounts shall locked after five failed login attempts.
- Windows system session shall locked if idle time is more than 15 Minutes.

8.1.2. Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting, or modifying a password file on any computer system is prohibited.

8.1.3. Users shall not allowed to Login as a System Administrator. Users who need this level of access to production systems must request a Special Access account as outlined elsewhere in this document.

8.1.4. Employees will be responsible for all transactions occurring during Login sessions initiated by use of the employee's password and ID. Employees shall not Login to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

8.2. SYSTEM ADMINISTRATOR ACCESS:

System Administrators, network administrators, and security administrators will have full access to host systems, routers, hubs, and firewalls as required to fulfil the duties of their job. All system administrator passwords will be DELETED immediately after any employee who has access to such passwords is terminated, fired, or otherwise leaves the employment of the company.

8.3. SPECIAL ACCESS:

Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by the company and require the permission of the user's company IT Manager. Monitoring of the special access accounts is done by entering the users into a specific area and periodically generating reports to management. The reports will show who currently has a special access account, for what reason, and when it will expire. Special accounts will expire every day and will not be automatically renewed without written permission.

8.4. CONNECTING TO THIRD-PARTY NETWORKS:

This policy is established to ensure a secure method of connectivity provided between the company and all third-part companies and other entities required to electronically exchange information with company.

"Third-party" refers to vendors, consultants and business partners doing business with company, and other partners that have a need to exchange information with the company. Third-party network connections are to be used only by the employees of the third-party, only for the business purposes of the company. The third-party company will ensure that only authorized users will be allowed to

access information on the company network. The third-party will not allow Internet traffic or other private network traffic to flow into the network.

This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed.

All requests for third-party connections must be made by submitting a written request and be approved by the company.

8.5. CONNECTING DEVICE TO THE NETWORK:

Only authorized devices may be connected to the company network. Authorized devices include PCs and workstations, Laptops owned by company that comply with the configuration guidelines of the company. Other authorized devices include network infrastructure devices used for network management and monitoring.

Users shall not attach to the network: non-company computers that are not authorized, owned and/or controlled by company.

NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g. Pen drives, thumb drives and writable CD's.

8.6. REMOTE ACCESS:

Only authorized persons may remotely access the company network. Remote access is provided to those employees, contractors and business partners of the company that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the network or a remote network to company network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID.

8.7. UNAUTHORIZED REMOTE ACCESS:

The network attachment (e.g. Switches) to a user's PC or workstation that is connected to the company LAN is not allowed without the written permission of the company. Additionally, users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

8.8. PENALTY FOR SECURITY VIOLATION:

The company takes the issue of security very seriously. Those employees who use the technology and information resources of company must be aware that they can be disciplined and must follow

this policy. Upon violation of this policy, an employee of company may be subject to discipline up to and including termination. The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of the cyber security policy, prior violations of the policy committed by the individual, state of federal laws and all other relevant information. Disciplinary action which may be taken against, and employee shall be administrated in accordance with appropriate rules or policies and the company policy manual.

In case where accused person is not an employee of company the matter shall be submitted to the company director and legal team. The legal team may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violators.

9.0 OPERATIONS SECURITY POLICY:

The Organization's intentions for publishing an Acceptable Use Policy are not to impose restrictions contrary to the Organization's established culture of openness, trust, and integrity. The Organization is committed to protecting its employees, partners, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.
Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of the Organization. These systems are to be used for business purposes in serving the interests of the Organization and our clients and customers in everyday operations
Adequate security is a team effort involving every Organization employee and affiliate who deals with information and information systems. It is the responsibility of every computer user to know these guidelines and conduct their activities accordingly

This Policy applies to employees, contractors, consultants, temporaries, and other workers at Organization, including all personnel affiliated with third parties. This Policy applies to all equipment that is owned or leased by Organization

9.1. General Use and Ownership

9.1.1. While Organization's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the Organization. Because of the need to protect Organization's network, Management cannot guarantee the confidentiality of the information stored on any network device belonging to the Organization

9.1.2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

9.1.3. It is recommended that any information that users consider sensitive or vulnerable should be encrypted in a separate drive

9.1.4. For security and network maintenance purposes, authorized individuals within Organization or any third party authorized by Organization may monitor equipment, systems, and network traffic at any time.

9.1.5. The Organization reserves the right to audit networks and systems periodically to ensure compliance with this Policy.

9.2. Security and Proprietary Information

9.2.1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System-level and CBS level passwords should be changed as per Password Policy.

9.2.2. Postings by employees from an organization's email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of the organization unless posting is during business duties.

9.2.3. Use of Organization email for personal use like signing up to a website not relevant for business purposes is strictly prohibited.

9.2.4. All hosts used by the employee connected to the Organization Network shall be continually executing approved virus-scanning software with a current virus database. Any exceptions are to follow change management policy with proper authorization of competent authority.

9.2.5. Employees must use extreme caution when opening email attachments received from unknown senders, including viruses, email bombs, or Trojan horse code. Employees should be responsible for exercising reasonable steps and exercise their best judgment before downloading any email attachment.

9.3. Unacceptable Use

9.3.1. The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

9.3.2. Under no circumstances is an employee of an organization authorized to engage in any illegal activity under national or international law while utilizing Organization owned resources.

9.3.3. The lists below are by no means exhaustive but attempt to provide a framework for activities that fall into the category of unacceptable use.

9.4. System and Network Activities

9.4.1. The following activities are strictly prohibited, with no exceptions:

9.4.2. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Organization

9.4.3. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books, or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Organization or the end-user does not have an active license is strictly prohibited.

9.4.4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws is illegal. The appropriate Management should be consulted before the export of any material that is in question

9.4.5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.)

9.4.6. You are revealing your account password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.

9.4.7. It is using an organization computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.

9.4.8. They were making fraudulent offers of products, items, or services originating from any Organization account.

9.4.9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9.4.10. They are affecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

9.4.11. Port scanning or security scanning is expressly prohibited unless prior notification to IT Department is made.

9.4.12. We are executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's regular job/duty.

9.4.13. They are circumventing user authentication or security of any host, network, or account.

9.4.14. It interferes with or denies service to any user other than the employee's host (for example, denial of service attack).

9.4.15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the network.

9.4.16. Providing information about, or lists of, Organization employees to parties outside the Organization.

9.5. Computer and internet usage

9.5.1. Company employees are expected to use the Internet responsibly and productively Internet access is limited to job-related activities only, and personal use is not permitted.

9.5.2. Job-related activities include research and educational tasks that may be found via the Internet that would help in an employee's role.

9.5.3. All Internet data that is composed, transmitted, and/or received by Organization computer systems is considered to belong to Organization and is recognized as part of its official data. It is therefore subject to disclosure for legal reasons or to other appropriate third parties.

9.5.4. The equipment, services, and technology used to access the Internet are the property of the Organization, and the company reserves the right to monitor Internet traffic and monitor and access data that is composed, sent, or received through its online connections.

9.5.5. All sites and downloads may be monitored and/or blocked by Organization if they are deemed to be harmful and/or not productive to business

9.5.6. The installation of software such as instant messaging technology is strictly prohibited.

9.6. Email and Communications Activities

9.6.1. They were sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

9.6.2. Any form of harassment via email, telephone, whether through language, frequency, or size of messages.

9.6.3. Unauthorized use, or forging, of email header information.

9.6.4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

9.6.5. Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type.

9.6.6. Use of unsolicited Email originating from within Organization's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Organization or connected via Organization's network.

9.6.7. Posting the same or similar non-business-related messages to many Usenet newsgroups (newsgroup spam).

9.6.8. Emails sent via the company email system should not contain content that is deemed to be offensive. This includes, though is not restricted to, the use of vulgar or harassing language/images

9.7. Enforcement

Any employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment. In case of a violation of the Indian IT ACT, Cyber Law, or IPC, local Law authorities will be involved.

10.0 ANTI-VIRUS POLICY:

Viruses and malware affect the IT Infrastructure of an organization reducing the productivity of its staff. Generally, viruses and worms propagate through the Internet or removable media infected by them. Organization infrastructure is protected as far as removable media is concerned using Antivirus software. Further, the desktops do not have CD Drives, Pen Drive access to run any media from outside. Also, Internet access is controlled by the IT.

This Policy aims to define a process in deploying and managing antivirus programs in the IT Infrastructure of the Organization.

This Policy applies to IT Infrastructure and systems as identified to be connecting to the Organization network and Internet

11.1. General: IT Department will be responsible for deploying antivirus signature on all systems that run the antivirus software. Apart from IT Department, employees at branches also will take due care so that infrastructure is not affected by any virus or malware.

11.2. AV Program Deployment: All the servers will be running an antivirus software program identified, accepted, and procured by Organization Management. In case of any replacement servers or hard disk of any computer/server, or in case of formatting any computer/server, the IT Department will be responsible for re-deploying AV software on these computers/servers. IT Department at Head Office will take necessary upgrades and renewals from the AV Vendor at regular intervals to ensure the antivirus software is up to date.

11.3. AV Program updates: The AV software vendors release antivirus signatures regularly. IT Department will ensure the signature updates are applied to the relevant systems at all departments centrally.

11.4. Host protection: For critical resources of Organization, host-based firewalling, virtual patching, and file integrity monitoring mechanisms are to be placed on maintaining the security and integrity of those systems.

11.5. User's responsibility: Users are responsible for bringing to the notice of the IT department if AV is outdated or not found in their PC.
Further it would be deemed a violation of this Policy for user actions like an attempt to uninstall AV, attempting to modify the security settings or loading the computer in boot mode, or any attempt to kill AV services/processes.

11.6. Enforcement: Any employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

11.0 BACKUP POLICY:

Backup is an important activity towards protecting the data and recovering from a disaster. Backup assures the organizations and other stakeholders to some extent to recover their valuable data. However, certain practices are required to make it more efficient and relevant when needed the most. The Organization has adopted a proper backup strategy to make it more effective and robust.

12.1. General: Servers located at the data centre house the crucial databases are to be backed up on removable media. Full and/or incremental backup will be taken at least once daily. A copy of the full-back is to be kept post annual book closures at a minimum and for every event that is deemed critical – pre-major changes, half-yearly or quarterly book closures as deemed necessary.

12.2. Backup Procedure: Two backups of database will be taken on a daily basis. First, the database shall backed up on backup media at on premise data centre. Also, a full copy of the database will

be kept replicating on another external backup media. After the backup is taken on the removable external hard disks, they will be stored in a secured location under the supervision of competent authority.

12.3. Compliance: A register will be maintained to keep the track of backups being taken. This register will be updated every day after taking the backup. Next day IT Department will check the register to ascertain that backup process went smoothly.

12.4. Monitoring: Backup operator is the first person who will be witnessing the success or failure of a backup session. In case of any malfunction of the backup media, operator will take Corrective actions to take backup on the backup media. In case of a failure at first level, operator will go ahead with second phase of back up, i.e. taking a copy on another server within the data centre.

12.5. Recovery: IT Department will verify the availability of data on the backup media by running recovery procedure on test systems at a regular interval. A recovery register will be maintained for the same along with logs proving the success of the recovery. Post verification of recovery, the data on the test system will be immediately removed/erased such that is it not recoverable.

12.6. Enforcement: Any employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

12.0 DATA CENTRE SECURITY POLICY:

Server room houses all critical servers, which facilitates business transactions for users. There is a single database for all Organization customers, which is referred for any transaction in real time. Because of the data transactions in real time, Organization is enabled to offer many values added services to its customers. However, to provide uninterrupted services to its customers, the critical facility, i.e. data centre should be managed and monitored in the best possible way so as to maintain the Confidentiality, Integrity and Availability of customer records.

13.1. General: Data centre is the core of all Organization business activity. It is paramount to protect this critical location against any confidentiality, integrity, or availability threat. If any of these three aspects is compromised, Organization may lose its valuable customers, their confidential data and reputation in business segment. Data Centre will be monitored and managed for access, physical and environmental and availability.

13.2. Access controls: No un-authorized person will enter the data centre at any point in time. Only IT Administrators and external support persons along with IT Department personnel are allowed an entry in this critical area. An access register will be maintained inside the data centre, where details about persons and their activities in the data centre will be registered.

13.3. Physical controls: IT Administrators should monitor the temperature and electrical parameters inside the data centre at least once in a day. In case of any malfunction of any physical control inside the data centre, IT Admins should alert the respective internal as well as external parties for necessary action.

13.4. **Physical controls would include but not limited to following**

13.4.1. Physical access requires authorization and is monitored.

13.4.2. All employees and visitors must visibly wear official identification while onsite.

13.4.3. Visitors must sign a visitor's register and be escorted and/or observed while onsite.

13.4.4. Premises are monitored by CCTV

13.4.5. Entrances are protected by physical barriers designed to prevent unauthorized entry

13.4.6. Safeguards related to environmental hazards

13.4.7. Network cables are protected by conduits and, where possible, avoid routes through public areas.

13.5. **Logical Controls:** Data centre connected to all external locations through Wide Area Network. To reduce the access to data centre, IT Administrator will use tools to monitor devices inside the data centre and monitor and rectify any fault while sitting outside the data centre. If required, IT Admins will also inform external service providers for support calls and liaison with external locations.

13.6. **User Encryption for External Connections:** Access to organization Services is through a secure communication protocol only. If access is through a Transport Layer Security (TLS) enabled connection, that connection is negotiated for at least 128-bit encryption. The private key used to generate the cipher key is at least 2048 bits. TLS is implemented or configurable for all web-based TLS-certified applications deployed at Organization's DR Site. It is recommended that the latest available browsers certified for Organization programs, which are compatible with higher cipher strengths and have improved security, be utilized for connecting to web enabled programs. For Organization Services where HTTP connections with the third-party site are permitted by Organization, Organization will enable such HTTP connections in addition to the HTTPS connection.

13.7. **Enforcement:** Any employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

13.0 COMMUNICATION SECURITY POLICY:

Email correspondence plays a major role in business communication. Organizations communicate with its customers, branches, and other organizations to communicate vital and important messages. To derive the best benefits of email systems, it is required to adhere to good practices while communicating through emails. This Policy lists down required practices for email usage.

14.1. **Appropriate Use:** Organization employees are expected to use technology responsibly and productively as necessary for their jobs. Internet access and email use is for job-related activities; however, minimal personal use is acceptable.

14.2. Employees may not use Organization's Internet, Email or other electronic communications to transmit, retrieve or store any communications or other content of a defamatory, discriminatory, harassing or pornographic nature. No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, or sexual preference may be transmitted. Harassment of any kind is prohibited.

14.3. Disparaging, abusive, profane or offensive language and any illegal activities—including piracy, cracking, extortion, blackmail, copyright infringement and unauthorized access to any computers on the Internet or Email—are forbidden.

14.4. Copyrighted materials belonging to entities other than Organization may not be transmitted by employees on the company's network without permission of the copyright holder.

14.5. Employees may not use Organization's computer systems in a way that disrupts its use by others. This includes sending or receiving excessive numbers of large files and spamming (sending unsolicited Email to thousands of users).

14.6. Employees are prohibited from downloading software or other program files or online services from the Internet without prior approval from the IT department. All files or software should be passed through virus-protection programs prior to use. Failure to detect viruses could result in corruption or damage to files or unauthorized entry into company systems and networks.

7.1.1. Every employee of Organization is responsible for the content of all text, audio, video, or image files that he or she places or sends over the company's Internet and email systems. No email

or other electronic communications may be sent that hide the identity of the sender or represent the sender as someone else.

7.1.2. Prohibited Use: The Organization email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair colour, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Organization employee should report the matter to their supervisor immediately.

7.1.3. Organizational Use: Organization email system should have anti-spam, antivirus and attachment scanning to protect any unwanted malicious content (like malware, executables, etc.) to enter the Organization via Email.

7.1.4. Monitoring: Organization employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Organization may monitor messages without prior notice. Organization is not obliged to monitor email messages.

7.1.5. Enforcement: Any employee found to have violated this Policy may be subject to disciplinary action, up to and including termination of employment.

14.0 SYSTEM ACQUISITION DEVELOPMENT AND MAINT POLICY:

To ensure that security is an integral part of information systems across their entire lifecycle, including those that provide services over public networks, that information security is integrated into the system development lifecycle, and to ensure the protection of data used for testing.

This System Acquisition, Development, and Maintenance Security Policy applies to all business processes and data, information systems and components, personnel, and physical areas of The organization.

15.1. Information Security Requirements Analysis and Specification:

15.1.1. When developing, acquiring, or making major changes to an information system, Information Owners and Service Owners should:

- Prepare a Statement of Sensitivity to determine the confidentiality, integrity, and availability requirements of the system.
- Apply security controls based on a Threat and Risk Assessment.
- Document the role and responsibilities related to information system security management.
- Document specific procedures and standards used to mitigate risks and safeguard the information systems.
- Document and communicate procedures for security-related events and incidents.

15.2. Security Requirements of Information Systems:

15.2.1. Information security requirements must be considered in the acquisition of new information systems or enhancements to existing ones.

15.2.2. Identification and management of information security requirements and associated processes should be integrated into the early stages of information systems projects.

15.2.3. Information security requirements and controls should reflect the business value of the information involved and the potential negative business impact which might result from lack of adequate security.

15.0 SUPPLIER SECURITY:

Information security requirements will vary according to the type of contractual relationship that exists with each supplier and the services delivered.

16.1. Supplier Information Security Applied:

16.1.1. Supplier who deploys resources and having access to information assets or information processing facilities shall be subjected to background screening depending on the engagement nature and duration of the engagement with vendor.

16.1.2. The information security requirements and controls must be formally documented in a contractual agreement which may be part of, or an addendum to, the main commercial contract.

16.1.3. Separate Non-Disclosure Agreements must be used where a more specific level of control over confidentiality is required.

16.1.4. Appropriate due diligence must be exercised in the selection and approval of new suppliers before contracts are agreed.

16.1.5. The information security provisions in place at existing suppliers (where due diligence was not undertaken as part of initial selection) must be clearly understood and improved where necessary.

16.1.6. Remote access by suppliers must be via approved methods that comply with our information security policies.

16.1.7. Access to company information must be limited where possible according to clear business need.

16.1.8. Basic information security principles such as least privilege, separation of duties and defence in depth must be applied.

16.1.9. The supplier will be expected to exercise adequate control over the information security policies and procedures used within sub-contractors who play a part in the supply chain of delivery of services to BDR.

16.1.10. The supplier shall conduct background check of their supply chain as required and make copy of report available to BDR.

16.1.11. BDR will have the right to audit the information security practices of the supplier and, where appropriate, sub-contractors.

16.1.12. Incident management and contingency arrangements must be put in place based on the results of a risk assessment.

16.1.13. Awareness training will be carried out by both parties to the agreement, based on the defined processes and procedures.

16.2. Acceptable use for suppliers and supplier personnel Ethical or Legal Activities

BDR resources must be used for ethical and legal activities only but not for unethical or illegal activities which include, but are not limited to:

16.2.1. The intentional creation, downloading, viewing, storage, copying, or transmission of sexually explicit, sexually oriented, gambling or hate materials is not permitted.

16.2.2. The intentional creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, illegal weapons, terrorist activities, and any other illegal or otherwise prohibited activities is not permitted.

16.2.3. The unauthorized acquisition, use, reproduction, transmission, or distribution of any BDR defined controlled information including, but not limited to, software and information that includes privacy information, copyrighted, trademarked, or otherwise protected intellectual property (beyond fair use), proprietary data, or export-controlled software or data is not permitted.

16.2.4. Engaging in any unauthorized fundraising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity is not permitted.

16.3. Unacceptable activities

The following activities are, in general, prohibited, unless specifically allowed during the course of legitimate job responsibilities (e.g., systems administration staff may be required to disable the network access of a host if that host is disrupting services).

The list below is by no means exhaustive but attempts to provide a framework for activities, which fall into the category of unacceptable use.

16.4. Prohibited Uses of the Internet

16.4.1. Create, download, upload, display, or access knowingly, sites that contain pornography or other "unsuitable" material that might be deemed illegal, obscene, or offensive.
16.4.2. Subscribe to, enter, or use peer-to-peer networks, or install software that allows the sharing of music, video, or image files.
16.4.3. Subscribe to, enter, or -utilize real-time chat facilities such as chat rooms, text messenger, or pager programs.
16.4.4. Subscribe to, enter, or use online gaming, or betting sites.
16.4.5. Subscribe to, or enter "money-making" sites, or enter, or use "money-making" programs.
16.4.6. Run a private business.
16.4.7. Download any software that does not comply with the organization's software policy.

16.5. Cloud services

BDR clearly recognize the risks associated with the cloud systems, so the access to and management of BDR cloud data may be managed appropriately. BDR information security policy must be implemented as part of the agreement. BDR will also ensure that information security objectives are set for third parties who provide components of the cloud service to customers and that they carry out adequate risk assessment in order to achieve an acceptable level of security.

16.6. Due diligence

Before contracting with a supplier, it is incumbent upon BDR to exercise due diligence in reaching as full an understanding as possible of the information security approach and controls the company has in place. It is important that the documented Supplier Due Diligence Assessment Procedure is followed so that all the required information is collected, and an informed assessment can be made.

This is particularly important where cloud computing services are involved, as legal considerations regarding the location and storage of personal data must be considered.

16.7. Addressing security within supplier agreements

Once a potential supplier has been positively assessed with due diligence the information security requirements of BDR must be reflected within the written contractual agreement entered. This agreement must consider the classification of any information that is to be processed by the supplier (including any required mapping between BDR classifications and those in use within the supplier), legal and regulatory requirements and any additional information security controls that are required.

For cloud service contracts, information security roles and responsibilities must be clearly defined in areas such as backups, incident management, vulnerability assessment and cryptographic controls.

Appropriate legal advice must be obtained to ensure that contractual documentation is valid within the country or countries in which it is to be applied.

16.8. Evaluation of existing suppliers

For those suppliers that were not subject to an information security due diligence assessment prior to an agreement being made, an evaluation process must be undertaken in order to identify any required improvements.

16.0 INFORMATION SECURITY INCIDENT MANAGEMENT POLICY:

This section provides some policy guidelines and procedures for handling security incidents. The term "Security Incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the company network. Following are the few examples of security incidents.

- Illegal access of the company computer system. For example, a hacker logs onto a production server and copies the password file.
- Damage to a company computer system or network caused by illegal access. Releasing a virus or worm would be an example
- Denial of service attack against a company web server. For example, a hacker initiates a flood of packets against a Web Server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against other computer outside of the company network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Employees, who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to their manager immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

17.0 STEERING COMMITTEE CHARTER

The Information Security Committee exists to provide recommendations to company executive management about all information security efforts undertaken by company. The committee also coordinates and communicates the direction, current state, and oversight of the information security program company has established information security steering committee to review of information security policy as per appendix BDR/IT/POLICY/001/Appendix-1