G.3.4 IT SECURITY POLICY – DMCG

1.PURPOSE

The purpose of this policy is to identify the rules and procedures for all individuals accessing and using an DMCG's IT assets and resources to ensure efficient security management.

2.SCOPE OF THE PROCEDURE:

The policy addresses all data, programs, systems, facilities, other tech infrastructure, users of technology and third parties in in DMCG.

3.DEFINITIONS:

NIL.

4.RESPONSIBILITIES FOR APPROVING THE APPLICATION:

Head of IT
Director of shared Services
Dean

5.PROCESS:

1.1 Security Policy is a Statement of Management Strategy regarding Security of its Information Assets.

1.2 Information Ownership.

All Organizational data as defined in this policy is owned by **DMCG** and given rights to manage and ensure Data security by Lootah IT Solutions
Here users term referring to Organization accepted users.

The Policy Statements are grouped under the following Headings:

1. Information Security Policy
2. Organizational Policy
3. Personnel Security Policy
4. Physical & Environmental Security Policy
5. Computer & Networks Security Policy
6. System Administration
7. Network Policy
8. Application Development Policy
9. Business Continuity Planning

1.2.1 <u>Information Security Policy</u>

The Following requirements must be met

1. All major information assets should have an asset.
2. The owner should classify the information into one of the sensitivity levels depending on costs,

Organizational Policy, and Operational Needs. He /She is responsible for this Information.

3. The owner shall declare who is allowed access to the data.
4. The owner is responsible for this data and shall secure it or have it secured according to itssensitivity.

1.2.1.1 Classification of Information

A classification system is proposed which classes information into four levels. The lowest – 1, is the leastsensitive and the highest – 4, is for the most important data/processes. If a system contains data or morethan one sensitivity class, it must be classified according that needed for the most confidential data on the system.

1.2.1.1.1 Class -1: Public / Non-Classified Information

Description:

Data on these systems could be made public without any implications for the company (i.e. the data is not confidential). Data integrity is not vital. Loss of service due to malicious attacks is an acceptable danger. Examples: Test services without confidential data, certain public information services. Guidelines on storage: none Guidelines on transmission: noneGuidelines on destruction: none

Class -2: Internal Information Description:

External access to this data is to be prevented, but should this data become public, the consequences are not critical (e.g., the company may be publicly embarrassed). Internal access is selective. Data integrity is important but not vital. Examples of this type of data are internal memos, normal working documentsand project/minutes of meeting and internal telephone books.

Guidelines on storage:

- Information shall be labelled. i.e., the classification level should be written on documents,media (tapes, diskettes, disks, CD's etc.), electronic messages and files.
- IT Systems susceptible to virus attacks should be regularly scanned for viruses. The integrity ofsystems should be regularly monitored.
- Information's or Documents or electronic files should be work from One drive or to be backup to one drive by users to avoid misuse and unauthorized access

Guidelines on transmission:

- This information shall stay within the company, if it must transit public media (e.g. the Internet),itshould be encrypted.
- Internal data shall not be transferred outside the company unless approved by the Department Manager.
- Internal Sharing should only do through OneDrive or SharePoint and should comply with IT policy

Guidelines on destruction: none

2.1.1.1.1 Class -3: Confidential Information

Description:

Data in this class is confidential within the company and protected from external access. If such data were

to be accessed by unauthorized persons, it could influence the company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor or cause amajor drop in customer confidence. Data integrity is vital.

Examples: Salaries, Personnel data, Accounting data, very confidential customer data, sensitive projectsand confidential contracts.

Guideline on storage:

- Information shall be labelled. i.e., the classification level should be written on documents, media (tapes, diskettes, disks, CD's etc.), electronic messages and files.
- IT Systems susceptible to virus attacks should be regularly scanned for viruses. The integrity of systems should be regularly monitored. .IT Systems shall be configured to protect against unauthorized modification of data and programs.
- Information shall be kept under lock and key (e.g., documents in locked cabinets, computers in locked rooms).
- Information's or Documents or electronic files should be work from users assigned One drive or to be backup to one drive by users to avoid misuse and unauthorized access

Guidelines on transmission:

- Passwords should not be transmitted in clear text (electronically or on paper).
- This information shall stay within the company, if it must transit public media (e.g. the Internet), it should be encrypted.
- Internal Sharing should only do through OneDrive or SharePoint and should comply with IT policy

Guidelines on destruction:

- Information shall be securely disposed of when no longer needed (e.g., destruction of old disks and diskettes etc.).

2.1.1.1.2 **Class -4: Secret Information**

Description:

Unauthorized external or internal access to this data could be critical to the company. Data integrity is vital. The number of people with access to this data should be very small. Very strict rules must be adhered to in the usage of this data. Examples: Information about major pending contracts/reorganization/financial transactions, Strategic Documents etc.

Guideline on storage:

- Information shall be labelled. i.e., the classification level should be written on documents, media (tapes, diskettes, disks, CD's etc.), electronic messages and files.
- IT Systems susceptible to virus attacks shall be regularly scanned for viruses. The integrity of systems shall be regularly monitored. IT Systems shall be configured to protect against unauthorized modification of data / programs and shall be audited yearly.
- Information shall be kept under lock and key (e.g., documents in locked cabinets, computers in locked rooms).

- Information shall be stored in encrypted format or on removable disks which are physically secured.
- Information's or Documents or electronic files should be work from users assigned One drive or to be regular backup to one drive by users to avoid misuse and unauthorized access

Guidelines on transmission:

- This information shall be encrypted during transmission outside of secure zones.

Guidelines on destruction:

- Information shall be securely disposed of when no longer needed (e.g., destruction of old disks and diskettes etc.).

1.2.2 Organizational Policy

This Policy lays down the rules for protection of organizational data and processes corresponding to the threats / risks involved and the value of the assets.

1.2.3 Personnel Security Policy

The purpose of the personnel security policy should be to establish controls on the hiring, training, and termination of all personnel (e.g., employees, contractors) to enforce compliance with the information security program. In addition, the organization should commit to providing employees and contractors a safe work environment. This includes a work environment that is free of harassmentbased on race, color, religion, sex, national origin, age, or disability.

1.2.4 Physical & Environmental Security Policy

The main objective of this policy is to prevent unauthorized access or damage to IT services. To prevent the loss of, damage to, or compromise to information assets, and interruption to the operational activities of the Organization. The environment control includes activities like data centers shall be protected by appropriate air conditioning and very early smoke detection systems. Temperatures in data centers shall be monitored by Operations staff, and undue variances reported immediately to theOrganization.

1.2.5 Computer & Networks Security Policy

A network security policy delineates guidelines for computer network access, determines policy enforcement, and lays out the architecture of the organization's network security environment and defines how the security policies are implemented throughout the network architecture. Network security policies describes an organization's security controls. It aims to keep malicious users out while also mitigating risky users within your organization. The initial stage to generate a policy is to understand what information and services are available, and to whom, what the potential is for damage, and what protections are already in place. The security policy should define the policies thatwill be enforced – this is done by dictating a hierarchy of access permissions – granting user's access

to only what they need to do their work. These policies need to be implemented in your organization written security policies and in your IT infrastructure – your firewall and network controls' security policies.

1.2.6 System Administration

System administration includes the maintenance and upkeep of servers to ensuring internal systemsare secure and protected from breaches and viruses, system admins are the gatekeepers of an organization and the data within. Its goal is ensuring the systems are running efficiently and effectively.

1.2.7 Network Policy

Network policy is a collection of rules that govern the behaviors of network devices. Our network that runs on policies can be automated more easily and therefore respond more quickly to changingneeds. Many common tasks, such as adding devices and users and inserting new applications and services, can now be easily accomplished. Well-defined policies can benefit a network in the following ways:

Align the network with Operational needs
Provide consistent services across the entire infrastructure
Bring agility through greater automation
Make performance dependable and verifiable

1.2.8 Application Development Policy

This Policy applies to major application system development or enhancement.

1.2.9 Business Continuity Planning

This plan includes the process of creating systems of prevention and recovery to deal with potential threats to our organization. In addition to prevention, the goal is to enable ongoing operations beforeand during execution of disaster recovery.

2 POLICY

2.1 IT Security policy

2.1.1 Levels of Primary security define on Data center and Networking

- First, level Perimeter Level Firewall with Policy
- Second, Manageable Switch level with VLAN Routing and its policy
- Third, end user Device level security with EDR and EPP
- Forth, Application based security

2.1.2 Network and Firewall policy

- Firewall with defined access and routing Policies
- Second Manageable Switch level with VLAN and its routing policy on separations
- Controllable Software Defined Policy

2.1.3 Cloud Datacenter

- Defined security levels depend on its hosting provider
- Defined securities on Hosting basis from the LITS

2.1.4 Access Management policy

General

- Users are unauthorized to enter to organizational network without permissions, finding such access will have carried forward to legal actions
- Organization encourages Users to take advantage of our remote computing capabilities. The ability to connect to the Firm's resources from any approved location, Users must exercise care to ensure the security of data, comply with all software licensing agreements.

Web and Remote access

- Users should not allow anyone else to access resources and never access Firm resources from any computer or mobile device not assigned/approved to them from IT Department
- Special care should be exercised when a user-owned computer or mobile device s shared in family or social setting and updated Anti-Virus software must be installed.
- Always make sure VPN Enabled while using remotely.
- Never open any third-party sites or programs which are not granted, while you are on VPN and remote desktop.

2.1.5 Password policy

- Passwords never auto saved or be written down or shared to anyone.
- Passwords should never be typed into a public, friend's or relatives' computer or mobile device.
- Device access (screen lock) pass code must be always maintained on all devices.
- Passwords must never be revealed to anyone for any reason. To do so exposes the authorized user to responsibility for actions (such as deleting files) that the other party takes with the disclosed password.
- All passwords must be immediately changed if they are suspected of being disclosed to anyone.
- Maintain Password Policies, avoid using usernames/mobile number in passwords
- Change passwords periodically It should not contain any word spelled completely.
- A Password must be at least 8 characters long, including: uppercase, lowercase letters, numbers, and characters.
- If users are on admin level, then they need to maintain excel sheet of all organizational passwords and update IT on updating basis

2.1.6 Users Privacy and Usage policy

- Email, Data, Internet access, and Devices should be only used primarily for Organizational purposes.
- Users are not permitted to use Devices, Software's, non-organizational email, and Internet for Personal use
- Streaming or downloading music or Videos or any personal content is strictly prohibited.
- Users are not permitted to save any personal information on Company Devices without prior approvals
- Hacking Company Systems/Networks or intruding company Data are subjected to legal actions
- Users have no right to privacy of any material created, received, or sent via email, fax, use of the Internet, or by any other computer, tab, or mobile device use.
- Organization reserves the right to monitor, log, and review, all email, Internet access and other details of device use.
- Organization reserves the right to access all computers and email accounts without regard for any passwords.
- Usages of others email, other software or hardware access without approvals or accessing others Data

are strictly prohibited.

- Organizational Management is not responsible for any password / item theft from Users.
- If Users Organizational data/email is lost or hacked, IT department must be notified immediately.
- Organizational Data should be on users designated one drive

2.2 Data policy

General

- Data Transfers or its forwarding's are prohibited without Organizational Management approvals - (except for approved IT Backups)
- Apart from Centralized or ERP or software data, Users data are user's responsibility to keep in Secure places like OneDrive and advise IT department to Collect backup on regular basis.

Data Security and Privacy

- Organizational Data may never reside on personal computers or drives except for IT Department approved devices.
- Organizational data stored on USB drives must be encrypted. (Subjected to prior approval)
- Personal data never stored in computers/ Laptops/ TABS, or never reside on the Organization network or email system.
- Confidential attachments must be sent in Adobe Acrobat format using the "Password to Open" feature
- Data Transmission Must be in legal ways and shouldn't be include any third-party persons/Software without prior approvals and to be transmit only through higher authorities Permissions.
- Data copy should be always backup to company One drive or to any permitted devices from IT
- Its user's responsibility to maintain their working files backup at assigned office 365 One drive or to allocated Hard Disk (apart from centrally Managing Software's)
- Functional flow and hierarchies' level of data access is set from organizational level and users need to follow it.
- Any Types of Misuse or tampering of Data will be subjected to legal action

6.Records:

All records related to this procedure will be filed in the respective units.

7.Filing:

The QA & IE Office shall file the master copy of this procedure and IT Department shall file the Soft Copy of this procedure.

8.Attachments:

None

Document History:

Version	Date	Summary of Change	Responsible
V 1.0	Jan 2020	Initial Version	IT Department
V 1.1	March 2021	Content Updated	IT Department
V 1.2	Aug 2022	Reflect the new roles and responsibilities to align with the org chart and authority matrix. Unify the policy format.	IT Department
V 1.3	Oct 2022	Reporting line have been clearly identified	Head of IT