G.3.1 DMCG IT POLICY AND PROCEDURE

1.PURPOSE:

The purpose of this policy is to establish for the user appropriate use of DMCG's information technology resources, computers, networking systems, information, and data.

2.SCOPE OF THE PROCEDURE:

All individuals who use DMCG's information technology resources, computers, networking systems, information, Software's, and data whether from on campus or off campus, are responsible for using these resources and systems in an effective and ethical manner.

3.DEFINITIONS:

None.

4.RESPONSIBILITIES FOR APPROVING THE APPLICATION:

- Head of IT
- Directorate of Shared Facilities
- Dean

5.PROCESS:

Technical Mobile Device Policy

- Organization shall ensure that College data and applications are logically separated from the employee's data on a personal mobile device provisioned to access College resources.
- Access controls on the employees' handheld mobile devices will be limited to the College workspace configured to contain Organization's data and applications.
- IT shall have the visibility of users who use personal mobile devices to access College resources.
- IT shall ensure the enforcement of a strong authentication mechanism on the College workspace configured on an employees' mobile device.
- Personal handheld mobile devices shall not store College information locally.
- IT shall maintain a list of authorized apps that can be installed in the configured College workspace.

Technical Implementation Remote Access

- Remote access shall only be permitted through a secure channel /tunnel and be subject to appropriate identification, authentication and encryption controls.
- A list of all external accesses provided shall be recorded and maintained by IT.
- All remote access connections to College network shall be logged and monitored regularly.
- The computing device that has remote access connection to College network shall be configured with a firewall and anti- virus software.

- Remote control software (such as RDP or PC-Anywhere) are strictly prohibited from use on College network without the approval of business stakeholder and IT.
- Virtual Private Network (VPN) traffic to College environment shall be scanned for malware as well as inspected by different security measures such as firewalls, Intrusion Prevention Systems (IPS), etc.
- Vendors requiring remote access to College network shall be provided with required access on 'as-needed' basis for technical support issues etc. and will only be allowed access to specific ports/services during specific duration on the impacted system using filtering controls such as firewalls, IPS', etc. for a limited time period as per management approval.

Password Management Technical Policy

- All the Information Systems shall require identification and authentication through either passwords, pass-phrases, one-time passwords or similar authentication mechanisms
- Multifactor Authentication shall be used for accessing critical systems and other systems where deemed necessary.
- Multifactor authentication shall be used for all administrative access, including domain administrative access.
- All default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems must be changed.
- The passwords stored in the systems/devices/applications should not be kept in clear text.
- Password security policy shall be enforced to all the information systems. In case of a limitation, equal or more stringent controls shall be implemented at the local level.
- All applications procured or developed for the Organization shall have the capability to enforce College password security policy.
- Passwords must never be hard-coded in software developed by or modified by Organization.
- All failed logon attempts of information systems must be logged and monitored.
- The administrator/privileged (such as ‘root’) account/or password shall not be used for day to day/routine activities.
- Super user passwords shall be kept in a sealed envelope in a fire proof safe under the custody of Senior IT Operations Manager.
- Initial temporary passwords shall be conveyed to end users using a secure means by validating the user’s identity and ensuring that passwords and user names are communicated using different channels.
- Temporary passwords should be complex in nature.
- All the respective passwords in case of termination, resignation, role change or retirement shall be changed in case the account is to be kept operational.
- The guest accounts and default accounts supplied by the manufacturers shall be disabled or used only post changing the default passwords.
- An inventory of all accounts with privileged access on production information systems shall be maintained. Service Accounts Management.
- Service accounts must be configured to be distinctly identifiable from user accounts.
- The exact privileges needed for a "service account" to fulfil its intended role shall be identified.

- A detailed purpose description of the service account must be recorded.

Email Technical Policy

- Email Security, Users must:
- Use Password Policies and avoid using personal information (e.g., birthdays, names, mobile numbers.)
- Remember passwords instead of writing them down and keep them secret.
- Change their email password every two months.
- Clean up Inbox by deleting spams and unwanted junk mails
- Either Zip or Use Office 365 One drive to share or attach emails more than 10 MB size
- Users represent our company whenever they use their College email address. They must not:
- Sign up for illegal, disreputable websites and services or Register for a competitor's services unless authorized.
- Send unauthorized marketing content or solicitation emails or Distributing unauthorized emails
- Send insulting or discriminatory messages and content. Intentionally spam other emails.
- Change their Email Signature Set by IT Department or Include any content prohibited
- Sending Mass Mails, Automatic forwarding, without approvals
- Also, Users should always be vigilant to catch emails that carry malware or phishing attempts. We instruct Users to:
- Be suspicious of clickbait titles. Avoid opening attachments and clicking on links when content is not adequately explained (e.g., "Watch this video, it's amazing.")
- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g., grammar mistakes, capital letters, excessive number of exclamation marks.) Mark as spam and block suspicious mails
- Users who don't adhere to the present policy will face disciplinary action up to and including termination. Example reasons for termination are:
- Using a College email address to send confidential data without authorization.
- Sending offensive or inappropriate emails to our Users, customers, colleagues, or partners.
- Using a College email for an illegal activity.
- Appropriate security measures shall be taken to ensure the security of organizational information. Such measures may include Gateway antivirus, anti-spam filtering, email size restrictions, email archiving, email encryption, dynamic email reputation, email firewall and resilient solutions.
- Organization shall deploy stronger levels of authentication for controlling access to electronic messaging services from publicly accessible networks.
- Anti-virus/malware software shall be installed on email servers including SMTP gateway systems that transact with external networks.
- All the emails (inbound and outbound) shall be scanned with automated antivirus/malware systems prior to their transmittal or before reaching the user's inbox.
- All email attachments, regardless of the source or content, shall be scanned for viruses and other destructive programs before being opened or stored on any computer system.
- Administrator accounts are not permitted for electronic messaging purposes. They can be used only for system administration activities (e.g. no email or web surfing).
- The following are the email standards which shall be implemented for all the users as default:

- The maximum size limit of Internal send/receive email including attachments is 10Mb
- The maximum size limit of External send/receive email including attachments is 10Mb, if its more than, then it should be send as link
- The maximum size limit of External send/receive email including attachments for C-level executive's is 10Mb, if its more than, then it should be send as link
- Maximum number of recipients can be addressed in one email = 25
- Email Retention days = Depending on business requirement
- Email Archival days= Depending on business requirement
- Maximum mailbox storage size is 99 GB

Security Patch Management

- The patch management process shall cover all information systems (server operating systems, databases, applications, and network/security devices, etc.)
- All devices / systems and applications belonging to or managed by the Organization shall be patched with latest security patches on Quarterly basis with the exception of the following:
    - A request shall be raised immediately if it's a Zero-Day vulnerability patch.
    - In case of a patch is related to the perimeter & internal network devices, a request shall be raised for its earliest deployment.
- All patch updates will be implemented in accordance with the Organization's Change Management Policy and relevant procedures.
- Latest patches must be obtained from an affiliated and trusted source.
- Respective system administrators shall ensure that adequate roll back procedures are in place prior to the deployment of patches.
- Security patches must be successfully tested prior to their deployment.
- New devices/systems/applications shall be patched to its latest version, prior to device being connected to the College network.
- Appropriate records shall be maintained for every patch deployment change request.
- Ensure timely review of vendor notifications, for release of new patches.
- All devices/systems/applications shall be reviewed for patch deployment on a periodic basis.
- In the event that a patch cannot be applied due to incompatibility issues or bugs, compensatory security controls to mitigate the risk of exploitation of the system must be implemented and documented in the risk register. Devices that cannot be patched shall be reported to Vendors/Manufactures with details of the compensatory control (if any) implemented to reduce the risk.
- Security patch status for all systems and devices shall be communicated to Manufactures on periodic basis.

Vulnerability Management

- Vulnerability scans shall be performed at least once every year to ensure the enforcement of the vulnerability management process, Systems at high risk should be addressed first. Vulnerabilities shall be identified through but not limited to as following:
    - Technical Assessment
    - Compliance Assessment

  - Security Architecture Review
  - Security Incident Report Review
- Scope of the vulnerability scan and the type/methods of scans performed shall be determined.
- The Organization shall perform at least one penetration test every year; penetration tests shall cover all layers. It will only be performed by designated personnel/team on authorized Date and Time.
- The Organization shall identify risks associated with potential vulnerabilities and the appropriate course of action to be taken to mitigate those risks.
- System/Asset owner will be responsible for the remediation actions and to mitigate the identified vulnerabilities.
- IE shall keep track of planned remediation actions in order to follow up on their implementation status.
- Application security tests shall cover, at a minimum OWASP top ten application security risks (i.e. SQL injection, Cross-site scripting, Buffer overflow).

Technical Policy for Removal Media

- USB media, CD/DVD Drives and Memory card slots shall be blocked by default on all user information assets.
- USB Ports (for mass storage) shall be configured to automatically enforce encryption of the removable media before data can be copied on it.
- All systems (laptops, workstations and servers) shall be configured to prevent content auto-run for removable media.
- User assets shall be installed with antivirus systems, which is configured to scan every removable storage media when connected.

Technical Policy Removable backup tapes

- Authorization shall be required for removable backup tape media (backup tapes) removed from the Organization and a record of such removals should be kept in order to maintain an audit trail.
- All removable backup tape media should be stored in a safe, secure environment, in accordance with manufacturers' specifications.
- In case of media in transit, packaging should be adequate to protect it from any physical damage.
- Cryptographic techniques should be used to protect data on removable backup tape media.
- To mitigate the risk of media degrading while stored data are still needed, the data should be transferred to fresh tape media before it gets unreadable.
- Adequate number of backup tapes shall be identified and stored to have minimum impact in case of any disruption.
- Based on the retention requirement, the contents of backup tapes should be moved to fresh backup tapes before its end of life.

IT security Policy

- 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

- 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

- Cloud Datacenter has its own defined security levels depends on its hosting
- 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.

Users Privacy and Usage policy

- Email, Data, Internet access, and Devices should be only used primarily for business purposes.
- Users are not permitted to use Devices, Software's, non-College 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's 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; Data are strictly prohibited.
- Organizational Management is not responsible for any password / item theft from Users
- If Users College data/email is lost or hacked, IT department must be notified immediately

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
  - Users Need to use users OneDrive as their backup system and make sure its running otherwise immediately Inform IT

-
  - Apart from OneDrive's if any data found IT won't be responsible for its security or retention
- Security and Privacy
  - College Data may never reside on personal computers or drives except for IT Department approved devices.
  - College 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 Users responsibility to maintain their working files backup at Company office 365 One drive or 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 actions

Internet Usages Policy

- Internet, Data and email use is subject to organizational policies.
- The display or transmission of sexually explicit images/messages or illegal communication or transmission. Other such misuse Includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassment or showing disrespect for others. Users are expressly forbidden to access Internet sites where potentially offensive material is located. Downloading or viewing Pornography, Movies or other questionable material is not allowed and may be subject to review and subsequent disciplinary action.
- Any Police case or Legal action on such above cases, the user undersigned will be responsible, and actions will be taken accordingly
- Access to sites deemed inappropriate by management is strictly prohibited. These sites include, but are not limited to sites such as (Illegal/Obscene/offensive, Gaming, Streaming audio, and video including radio stations, Torrents, and similar ones)
- Users are permitted to use the Internet for personal use provided such use is limited in use and should done on free time.
- Gaming, streaming audio, torrents and video, and audio and video downloading are strictly prohibited.
- Social Media, Audio and videos should only use for business purposes.

IT Asset Management Policy

- Getting Hardware
  - Users need to get approval and IT Department will procure through Purchase depends on the requirement study

- Vendor and purchase
  - Vendor management are carried by Procurement Division where, the list of vendors and its support should maintain in IT Department
- Asset movement
  - All Assets are recorded against location/user/department basis, so if any Asset movement, user should take prior approval from IT Management through users concerned HOD, in case of failure to submit asset movement, action will be takes accordingly
- Use of Hardware
  - If a Devices is lost, misplaced, or stolen, IT department should be notified immediately.
  - Users are strictly not allowed to share IT resources without approvals from IT Department
  - Any Tampering or Devices will be charged or subjected to legal action for company data loss. The Charges for physical damage/Data loss will be deducted from concerned persons, Eg: Either company will procure new one and deduct from user's salary or user must purchase new device and submit to company.
  - Commonly Using Devices should be kept off after usages and avoid storing confidential Data's, if shared then delete it after sessions end.

Bring Your Own Devices

- Need to get prior approval form IT department
- Asset Decommission
  - Only IT Department can check and update the decommission report to management

IT Software Policy

- Getting Software
  - The firm's IT Department must approve all applications before any applications are installed.
  - Request for new software should raise from Department head and Organizations GM
  - Users are unauthorized to use any unapproved software even if its freeware
- Vendor and purchase
  - Vendor management are carried by Procurement Division where, the list of vendors and its support should maintain in IT Department
- Use of Software
  - The Software are strictly for company usages only, any misuse, intrude or tampering found will be subjected to actions or legal policies
  - Organization did not permit the unauthorized copying of licensed computer software.
  - Organization shall adhere to its contractual responsibilities and shall comply with all copyright laws and expects all Users of Organization to do the same. Users who violate this policy may be subject to discipline according to standard Organizational procedures. An individual engaged in the unauthorized copying or use of software may also face civil suit, criminal charges, and/or penalties and fines. Subject to the facts and circumstances of each case, such individuals shall be solely responsible for their defense and any resulting liability.

- Software's are allocated to User/Department/Location basis. Sharing access or usages without proper Approval will subject to actions
- Users are not allowed to change settings configured by IT Department without approvals

- Website Policy
  - Websites contents should be approved from Divisional heads before making changes or updates
  - Its annexure is in Social media policy
- Maintenance Policy
  - Major Maintenance schedule will be provided from IT department, usual it will carry on ofttimes
  - Minor patches are updated regularly depends on its priority and operational off-peak time
- Documentations (functional and Technical)
  - All functional and technical flow should be documented and recorded with changes
- Change Policy
  - It should carry out through Quality Assurance and Management approvals
- BYOS - Bring Your own software, Use of Third-party software
  - Only Organization approved Software's are allowed for users, which are preinstalled by IT
  - If any other software needs to use, then approvals needed from IT Department

IT Backup Policy

- Critical Applications
- Backup Routines
  - Critical Data Base Backups on End of Business Days
  - Enhancement Backups on
  - Configuration Backups on Monthly and up on configuration Changes
  - VM backup on Monthly and before and after Configuration changes
  - All users Backup will be on users one drive
- Backup Rotations
  - Keep all Backup one copy locally, one copy SAN Storages and if possible one in Azure Cloud
  - Minimum 3 Previous Backups versions and one monthly based backup

Social Media Usages Policy

- IT Policy for using Company Social media and credentials
- Usages of company social media and its credentials are subject to Company policy
- Users cannot use, change, misuse or manipulate its content or data for his personal or any other benefits
- Usages, Downloads or uploads of images, data, content, and details should be legal and it should process through guidelines with approval from management, before uploading

- Be respectful, post only appropriate and respectful content, Comments, replies should be processed out with prior approvals subjected to its importance
- Sharing of credentials, data's or any details are against IT policy, if needed it should be done with proper management approval
- Company is not responsible for any legal actions against violation of this policy and the users are responsible
- Users should know the rules, regulations, security protocols, copyright, guidelines, legal and regulatory challenges before using
- Creating parallel company Profiles, sharing illegal activities, competitor Profiles or sharing credentials with any other media are strictly against the policy
- Users should not comment, share, or post any negatives against the company and should not involve in any activities that affect Company Reputations
- Users are not permitted to use personal SIM, Mobile, any other personal devices other than company allowed devices, its includes the verification methods
- Users cannot delete or changes content or ID without proper approval from management
- Users are not permitted to use or share his/her personal accounts or emails and it cannot keep on company allowed devices or for company usages
- Upon changing account information's, verification or passwords users should update his/her HOD and Management through updated password list and its expiry dates
- Payment or Transactions should only be processed only with HOD and management approvals and should keep a record of Invoices, renewals, and expiry dates
- Social media ID and profiles which are created while employing or part of Organizational time is absolutely owned by company account and cannot be treated or use as personal ID or profiles
- Any above types of violations are treated as Violation of IT Policy, and it will be taken to legal actions

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	Update Information	Author/ Reviewer
V 1.0	August 2022	Reflect the new roles and responsibilities to align with the org chart and authority matrix.	IE Office
V1.1	Oct 2022	Reporting line have been clearly identified	Head of IT