The Kerala State Civil Supplies Corporation

Information Technology Usage Policy Version 1.0

February 2020

TABLE OF CONTENTS

PREFACE

The Kerala State Civil Supplies Corporation Ltd (popularly known as Supplyco) proudly submits the English & Malayalam version 1.0 of its IT USAGE POLICY as it is inevitable for the current scenario. It highlights the prominent aspects of our IT policy impeccable. It is drafted in lucid manner as such to learn its contents even by common people. The purpose of this policy is to outline the acceptable use of ICT infrastructure, web portal, email and software of the Supplyco. These rules and guidelines are in place to protect the employees and Supplyco, inappropriate use, exposes Supplyco to risks including

virus attacks, loss of confidential data, compromise of network systems and services and legal issue. Besides, IT POLICY clearly depicts the security measures to be taken while handling IT and ICT and precautions to prevent malicious programs. MIS Division has taken earnest efforts to compile the facts properly and adequately. MIS Division hope a positive response from all employees of Supplyco and users.

Sd/-

Manager MIS

1. BACK GROUND

The purpose of this policy is to outline the acceptable use of ICT infrastructure, web portal and softwares of the Supplyco. These rules/guidelines are in place to protect the employee and Supplyco. Inappropriate use, exposes Supplyco to risks including virus attacks, loss of confidential data, compromise of network systems and services, and legal issues.

Information security is no longer a technical issue but a business enabler. The challenge is to adapt it to the business objectives by developing a comprehensive information communication technology security strategy encompassing governance, risk management and compliance. It is a top-down process that begins with support and commitment from the management. Supplyco has agreed to adopt a culture of IT usage policy in its business activities. It has mandated the use of IT usage policy as the guiding standard for this adoption.

Information security is everybody's responsibility. Supplyco seek the involvement, participation and support of every employee and affiliate who deals with Supply co's Information Systems.

All Employees MUST acknowledge and sign this acceptable usage policy before gaining access to Supply co's Information Systems.

Locally Defined and External Conditions of Use — Individual units within the Supplyco may define "conditions of use" for information resources under their control. These statements must be consistent with this overall policy but may provide additional detail, guidelines restrictions, and/or enforcement mechanisms. Where such conditions of use exist, the individual units are responsible for publicizing and enforcing both the conditions of use and this policy. Where use of external networks is involved, policies governing such use also are applicable and must be followed.

2. POLICY OBJECTIVE:

This policy establishes the need for Supplyco to clearly define what behaviors and actions are permitted on their systems, and what is unacceptable. The objective of this policy is to ensure that personnel (staff, customers, vendors, contractors, and others) connected with the Supplyco information system are aware of their security responsibilities and that suitable controls are in place to mitigate risks arising out of human element. Increased protection of information and Information communication Technology Resources to assure the usability and availability of those resources to all Employees of "The Kerala State Civil Supplies Corporation Ltd. ("SUPPLYCO") is the primary intent of this Policy. The Policy also addresses privacy and usage guidelines for those who access "SUPPLYCO's Information Communication Technology Resources.

3. PURPOSE OF IT USAGEPOLICY:

"SUPPLYCO" recognizes the vital role information technology plays in effecting Company business as well as the importance of protecting information in all forms. As more information is being used and shared in digital format by SUPPLYCO's IT resources to authorized employees , the need for an increased effort to protect the information and the technology resources that support it , is felt by "SUPPLYCO" and hence this Policy.

Since a limited amount of personal use of these facilities is permitted by "SUPPLYCO" to employees, including Data resources, computers, printers, Laptop, e-mail and Internet access etc.., therefore, it is essential that these facilities are used responsibly by employees, as any abuse has the potential to disrupt company business and interfere with the work and/or rights of other employees.

Inappropriate use of information technology could expose the organization to potential embarrassment and possible litigation. The organization is committed to ensuring that this

valuable resource is not brought into disrepute in the workplace through inappropriate use. It is therefore expected of all employees to exercise responsible and ethical behavior while using “SUPPLYCO’s Information Technology facilities.

Standardization of specification of IT equipment is a strategy for minimizing IT costs within an organization by keeping hardware and software as consistent as possible. It will reduce the number of tools for management and also ensure interoperability and enhance up time.

As computers age, components begin to fail and it becomes increasingly difficult to find compatible parts for repairs or upgrades. Older machines will not support current operating systems and application softwares. Also, the amount of time required to support older hardware will be more.

To address the above issues, the following ‘policy guidelines’ are formulated .
This Policy aims to promote the following goals:

1. To ensure the integrity, reliability, availability, and superior performance of IT Systems.

2. Effectively manage the risk of security exposure within the organization.

3. Communicate the responsibilities for the protection of IT applications and systems of the Organization.

4. Reduce the opportunity for errors to be entered into an electronic system that support procedure and processes of the Organization.

5. Intensify the responsibilities of persons and steps to be taken in the event of an information asset misuse, loss of data or unauthorized disclosure.

6. Promote training and increase the awareness of information security to all employees.

7. To ensure that use of IT Systems is consistent with the principles and values that govern use of other Government facilities and services.

8. To ensure that IT Systems are used for their intended purposes.

9. To establish processes for addressing policy violations.

10. Guideline for condemnation and disposal of ITR resources.

Employees will follow the guidelines and policies to enable reasonable and appropriate usage of information systems, and to perform their jobs in accordance with all applicable laws, regulations and policies.

4. SCOPE

This policy applies to everyone who, in India, has access to SUPPLYCO's Information System/Resources and it shall be the responsibility of all Outlet/Depot/Regional Managers in the Outlets/Depots/Regional offices and MIS Division/Network Administrator at

the Head office to ensure that this policy is clearly communicated, understood and followed by all users.

This Policy also applies to all regular employees, contracted staff, daily wage staff and vendors/suppliers providing services to Supplyco that bring them into contact with SUPPLYCO's Information Technology Resources. The HR / Admin Supplyco and the respective Managers, Head of the section who contracts for these services shall be responsible to provide the contractor/vendor/supplier with a copy of this Policy before any access is given to them.

These policies cover the usage of all of the Company's Information system and communication resources, whether they are owned or leased by the company or are under the company's possession, custody, or control, including but not limited to:

- All computer-related equipment, including desktop personal computers(PCs),

  Lap tops, terminals, workstations, PDAs, wireless computing devices, telecomm equipment, networks, databases, printers, servers ,security systems ,and shared computers, and all networks and hardware to which this equipment is connected.

- All electronic communications equipment, including telephones ,radio

  communicators, voice-mail, e-mail, fax machines, PDAs, wired or wireless communications devices and services, Internet and intranet and other on-line services.

- All software including in-house developed, purchased or licensed business

  Software applications, SUPPLYCO -written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on SUPPLYCO –owned equipment.

- All intellectual property and other data stored on SUPPLYCO's Information Technology equipment.

- These policies also apply to all users ,whether on Company property or otherwise, connected from remote connections via any networked connection, or using Company information system

5. **Definitions:**

In this Policy, a reference to the following word(s) shall have the following meanings assigned to it.

As used in this policy information resources are data and all computer and communication devices and other technologies which access, store or transmit information in the Organization. “Information” includes information in the Organization.

5.1 INFORMATION CLASSIFICATION:

Information shall be classified appropriately as applicable i n t h e Organization into the following categories:

a. Top Secret:

It shall be applied to information unauthorized disclosure of which could be expected to cause exceptionally grave damage to the organizational interest. This category is reserved for organization's closest secrets and to be used only in certain situations, e.g. .Data availability of commodity in the warehouse, passwords to protected systems, confidential records and so on.

b. Secret:

This is applied to information unauthorized disclosure of which could be expected to cause serious damage to the Organizational interest. This classification should be used for

highly important information and is the highest classification normally used. e.g. Data on stock position of outlets, procurement quantity and vendor procurement price details, products etc, Information related to critical infrastructure such as configuration details of servers in data centers, etc.

c. Confidentiality:

This shall be applied to information unauthorized disclosure of which could be expected to cause damage to the security of the organization or could be prejudicial to the interest of the organization or could affect the organization in its functioning. limited access to a very small set of persons; material whose disclosure would cause severe damage to the affected party, e.g. board/executive/minister level management changes, financial details, strategic decisions etc.

d. Restricted:

This shall be applied to information which is essentially meant for official use only and which would not be published or communicated to anyone except for official purpose. The information under this category may be available to the employees of the organization . Access for defined users, roles or user groups, according to specific rules; material whose disclosure would cause serious damage to the organization , e.g. HR data,. including security policies, official circulars and the like.

e. Unclassified/public:

Information available on the web or provided for public consumption .Information in this category requires no protection against disclosure but may need protection against unauthorized modification and other security or integrity threats. e.g. Information published on organizational websites and so on. The information or electronic files that may be classified into these categories will be specific to respective division or organizations and proceedings issued accordingly.

5.2 **INFORMATION TECHNOLOGY RESOURCES (ITRESOURCES)**:

Information Technology Resources for purposes of this Policy include, but are not limited to, "SUPPLYCO owned or those used under license or contract or those devices not owned by "SUPPLYCO" but intentionally connected to "SUPPLYCO" -owned Information Technology Resources such as computers, Servers, Portable devices such as laptops, PDAs, Tablets and Mobiles, Dongles etc, that have been provided by the Organization, personally owned devices connected to organizational resources, printers, scanners, security devices ,network devices, modems, fax machines online and offline storage , media and related equipment, software, and data files, Database, that are owned, managed, or maintained for organization, video conferencing rooms, VC data, and Internet, network management and monitoring equipments.etc.

5.3 **USER**:

Anyone who makes any use of any IT resources connected to IT infrastructure of SUPPLYCO (hardware, software, networking, Data files etc) from any location, including but not limited to, all employees, temporary employees, probationers, contractors, vendors and suppliers.

5.4 **SYSTEMS AUTHORITY:**

MIS DIVISION functioning under "SUPPLYCO"(Government of Kerala owned organization) is the legal owner or operator of all IT resources.

5.5 MANAGER (MIS) is the INFORMATION SECURITYOFFICER(ISO):

The ISO assumes overall responsibility for ensuring the implementation, enhancement, monitoring, and enforcement of the IT Usage Policies and guidelines for the organization. The ISO is responsible for providing direction and leadership through;

Investigation of all alleged information violations by following procedures and refer the investigation to other investigatory entities wherever necessary, including law enforcement agencies;

Monitor use of IT resources only for intended official purposes as defined by policies.

5.6 NETWORK/SYSTEM ADMINISTRATOR:

A person designated by the Systems Authority to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system, training and are authorized to determine who is permitted access to particular IT resources. In addition to their current responsibilities are responsible for

5.6.1 Administering security tools, reviewing security practices, identifying and analyzing security threads and solutions and responding appropriately to security violations.

5.6.2 Administration of all user – Ids and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges and reporting requirements. (Note: Where a formal Security Administration function does not

exist, the organization or officers responsible for the security administration functions described above will adhere to this policy. When such an individual or individuals exist, the individual or individuals will work closely with ISO).

5.7 SYSTEM SUPPORT OFFICERS (SSO):

These are the technical support persons of Supplyco designated by Manager(MIS), whom are providing all technical support and any technical issues arise at depot/outlet and regional office level. In addition to their current responsibilities are responsible for

5.7.1 Checking and updating antivirus software. Ensure the proper working of antivirus software and its DB updation status.

5.7.2 Providing support for all software's of Supplyco.

5.7.3 Any other task assigned by Manager MIS.

5.8 NETWORK OPERATIONS CENTER(NOC):

Centralized Network Operation Control Center, ensures network are available 24 hours a day, 7 days a week.

5.9 HELPDESK

All locations within Kerala where SUPPLYCO operates by itself, all help and support pertaining to the system/user/network shall be provided by the SSO's or where the SSO's are not available, by the central IT helpdesk(MIS DIVISION). In case any user finds any problem with the ICT systems or need any help, they can send in their request to IT Administrator at Head office via e-mail to techsupport@supplycomail.com.In the event of emergencies IT

Administrator can be contacted via telephone at 0484-2207935/0484-2206791, however all phone calls must be followed by an e-mail later.

6 IT USAGEPOLICY

System users shall be responsible for the information assets (systems / infrastructure) provided to them to carry out their official responsibilities. They SHALL handle the information assets with due care and operate them in line with the Supply co's Acceptable usage policy.

The use of the SUPPLY CO’s information technology resources in connection with SUPPLYCO’s business and limited personal use is a privilege but not a right, extended to various users. The privilege carries with it the responsibility of using the Users of SUPPLYCO's Information Technology resources efficiently and responsibly.

By accessing SUPPLYCO’s Information Technology Resources, the user agrees to comply with this Policy. Users also agree to comply with the applicable laws and all governing contracts and licenses and to refrain from engaging in any activity that would subject SUPPLYCO to any liability. SUPPLYCO reserves the right to amend these policies and practices at any time without prior notice.

Any action that may expose SUPPLYCO to risks of unauthorized access to data, disclosure of information, legal liability, or other potential system failure is prohibited and may result in disciplinary action up to and including termination of employment and/or criminal prosecution.

Users of IT resources of SUPPLYCO are expected to abide by the following rules.

1. An individual in whose room/table the computer/Laptop/Tab is installed and is primarily used by him/her, is considered to be “primary” user. If a computer has multiple users, none of whom are considered the "primary" user, the divisional Head should make an arrangement and make a person responsible for compliance.
2. Employees of SUPPLYCO will follow guidelines and policies to enable reasonable and appropriate usage of information systems, and to perform their jobs in accordance with all applicable laws, regulations and policies and IT act of Government of India.
3. The user interface for information contained on Internet/Intranet systems should be classified as either confidential or not confidential, as defined by organizational confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: Organizational sensitive, secrets, Employees should take all necessary steps to prevent unauthorized access to this information.
4. Government as a policy encourages user community to go for open standard for interoperability.
5. Users while working at PC/laptop be careful not to spill water or food items on it. With clean hands only operate the PC/laptop. Regularly clean the system and its components (note:- Turn your PC off before cleaning it). Power off your system and UPS whenever it is not in use or user leaving the office.
6. Users are expected to take proper care of equipment, and are expected to report any malfunction to the staff on duty or to the in-charge of the facility. Users should not attempt to move, repair, re-configure, modify, or attach external devices to the systems.
7. Playing of Games using IT resources is strictly prohibited. Internet chat is also banned.
8. Display of offensive material (either on computer screens or through posters etc.) is strictly disallowed.

9. The facility should be used primarily for official purposes.

10. Political Use — Organizational information resources must not be used for partisan political activities where prohibited by state or other applicable laws, and may be used for other political activities only when in compliance with state and other laws and in compliance with applicable Organizational policies

11. Personal Use — Organizational information resources should not be used for activities unrelated to appropriate Organizational functions, except in a purely incidental manner.

12. Social Media—Employee is prohibited from media forums, including social networking websites, mailing lists, chat rooms and blogs by using Supplyco systems

13. Commercial Use — Supplyco information resources should not be used for commercial purposes, including advertisements, solicitations, promotions or other commercial messages, except as permitted under Supplyco policy.

14. Using the facility for illegal/commercial purposes is a direct violation of the policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages, and generation of threatening, harassing, abusive, obscene or fraudulent messages/images.

15. Information Belonging to Others—Users must not intentionally seek or provide information on, obtain copies of, or modify data , programs, passwords or other digital materialsbelongingtootherusers,withoutthespecificpermissionofthoseotherusers.

16. Internet Usage for personal device – Should not connect personal IT devices to interconnect on internet facility of supply co.

This Policy includes within its purview the following referred Policies

The General Information Technology Usage Policy

The Software Licensing Policy

The Internet and Intranet Usage Policy

The E-mail Usage Policy

Laptop policy

Data Backup Policy

Violations

6.1 GENERAL INFORMATION TECHNOLOGY USAGEPOLICY

6.1.1 Password Policy

- Individual password security is the responsibility of each user.

- Passwords are an essential component of SUPPLYCO‘s computer, Laptop and network security systems. To ensure that these systems perform effectively, the users must choose passwords that are difficult to guess. This means that passwords must not be related to your job or personal life. This also means passwords should not be a single word found in the dictionary or some other part of speech.

- Tomakeguessingmoredifficult,passwordsshouldalsobeatleastSixtoEight characters long. To ensure that a compromised password is not misused on a long-term basis, users are encouraged to change passwords every 90 days. Password history would be maintained for previous three passwords. This applies to the Systems Logon (windows password) and Mail passwords.

- All users are advised to adhere a password policy. Following points may be considered while creating a password.

  - The password should be difficult to break.
  - must be minimum of 8-12 characters in length
  - must include punctuation such as ! $ % & * , . ? + -=
  - must start and end with letters
  - must not include the characters # @ ' "`
  - Avoid using your own name, or names of your wife or children, or name of your Organization, or room No. or house No.etc.
  - passwords should be changed periodically and also when suspected that it is known to others.
  - Never use ‘Password’ as your password
  - Do not leave password blank and
  - Make it a point to change default passwords given by the software at the time of installation.

- Passwords must not be stored in readable form in batch files, automatic log-in

  scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them. Passwords must not be written down and left in a place where unauthorized persons might discover them.

- Immediatelyuponassignmentoftheinitialpasswordandinallcasesofpassword

  "reset" situations, the password must be immediately changed by the user to ensure confidentiality of all information.

- Under no circumstances, Users shall use another user's account or password without proper authorization.

- Undernocircumstances,theusermustsharehis/herpassword(s)withotheruser(s),

  unless the said user has obtained from the concerned section head/IT administrator the necessary approval in this regard. In cases where the password(s) is/are shared in accordance with the above, the user shall be responsible for changing the said password(s) immediately upon the completion of the task for which the password(s) was shared.

- When files, Data are shared through network, they should be protected with password and also with read only access rule.

- Anyattempttocircumventsystemsecurity,guessothers'passwords,orinanyway

  gain unauthorized access to local or network resources is forbidden. Users may not use another person's computing account, attempt to forge an account identity, or use a false account or e-mail address.

- In cases where no prior approval had been obtained for sharing of password(s) with

  other user(s), such user shall be completely responsible for all consequences that shall follow in respect of breach of this Policy and SUPPLYCO shall initiate appropriate disciplinary proceedings against the said user.

- All PCs, laptops and workstations should be secured with a password- protected screen

  saver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended .

6.1.2 Security/ Access Control

- Users are forbidden from circumventing security measures.
- Before use of Information Systems, Employees shall authenticate themselves by providing a valid username and password/passphrase. At the end of the working session, they shall logoff the Information System. If a system is left attended, it should be locked to prevent unauthorized access and use.
- Information System passwords/passphrases will be kept secret and not shared with anyone else, including MIS staff. They shall be changed at least once every 90 days. Employees shall not modify or tamper with Information System hardware. Additionally they shall not install any software (executable code) without prior approval from IT Administration.
- Employees, unless authorized as part of their job duties, shall not engage in activities that may affect the integrity or availability of the network. Activities include, scanning of IP addresses, network reconnaissance, sniffing, hacking etc.
- Security applications that have been installed on Information Systems (e.g. anti-virus, personal firewalls etc.) shall not be disabled and shall remain operational at all times.
- All files that are uploaded from external sources (via CD, USB ,memory devices, external Hard disk, etc.) or downloaded from the Internet to Information Systems shall are scanned by anti-virus software before further use.
- Employees shall be responsible for the security of any corporate information stored on portable media in their possession. Protection of such portable media shall be by way of suitable encryption and/or strong passwords, or similar. Loss of such portable media (containing sensitive corporate data) shall be immediately reported to their line manager and to MIS division.

- Unauthorized access, use, transmission, damage, deletion, suppression, alteration or interference with organization's Information Systems are forbidden
- All "SUPPLYCO" computers ,laptop, mobile ,tab that are either permanently or

  temporarily connected to the internal computer networks must have a password-based access control system. Regardless of the network connections, all computers handling confidential information must also employ appropriate password-based access control systems.
- All in-bound connections to "SUPPLYCO" computers ,Laptop, mobile, tab from external

  networks must be protected with an approved password or login control system. Third part applications such as Remote Desktop, Team viewer and Any desk may only be used at SUPPLYCO's network after receiving the written approval of the Manager(MIS) and must be disconnected when not in use. If anyone violates this Policy and SUPPLYCO shall initiate appropriate disciplinary proceedings against the said user.
- Allaccesscontrolsystemsmustutilizeuser-IDs,passwordsandprivilegerestrictions

  unique to each user. Users are prohibited from logging into any "SUPPLYCO" system anonymously. To prevent unauthorized access all vendor-supplied default passwords must be changed before SUPPLYCO's use.
- Access to the server room is restricted and only recognized IT staff or someone with due authorization from ISO is permitted to enter the room.
- Users shall not make copies of system configuration files (e.g. Passwords, etc) for their own, unauthorized personal use or to provide to other users for unauthorized uses.
- Any computer (PC/Server/Laptop etc) that will be connected to the IT infrastructure,

  should have an IP address assigned by the Network Operations Center. Following a systematic approach, the range of IP addresses that will be allocated to each section is decided. So, any computer/Laptop/Tab connected to the network from that section will be allocated IP address only from that Address pool. Further, each network port in the

room from where that computer will be connected will have binding internally with that IP address so that no other person uses that IP address un authorize from any other location. An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same individual and will be connected to the same port. IP addresses are given to the computers but not to the ports.

- Computer accessories, Printer, Scanner etc. may be moved from one location to another with prior written intimation to the MIS division, as MIS division maintains a record of computer identification names and corresponding IP address. As and when any deviation (from the list maintained by MIS Division) is found for any computer system, network connection would be disabled and same will be informed to the user by email/ phone, if the user is identified. When the end user meets the compliance and informs MIS division in writing/by email, connection will be restored.

Wireless and Security

Where wireless LANs (WLANs) are used, they are used with sufficient authentication and transmission encryption measures in place, complemented by proper security Management processes and practices. Access points are located to minimize network tapping from publicly accessible area. The network default name, encryption keys and Simple Network Management Protocol(SNMP) community strings (and any insecure configuration) is changed at installation. SSID shall not reflect the name of any organization’s division, system name or product name. For non-public wireless access points, encryption keys are regularly changed and SSID broadcasting is disabled. It is better to engage a firewall or router is in place between the access point and the Supply co’s network to filter connections. Restricted firewall rules MUST be applied to allow only needed ports to pass from the wireless segment.

Network administrators regularly scan for “rouge” or “unauthorized” wireless access

points. Use multiple SSIDs with different configurations for different VLANs, client authentication methods, etc. For example, guest may use a different WIFI connections. Guest WIFI may have lower security and may only allow for connecting to the internet

Virtual Private Networks.

VPNs carrying classified data shall authenticate using two-factor authentication : • first one a one-time password authentication such as a token device or a public/private key system with a strong passphrase, Second username and password using external authentication server .VPNs disconnect automatically from Supplyco network after a pre-defined period of inactivity. The user shall be required to logon again to reconnect to the network. Supplyco should only permit one network connection at a time. All computers connected to a Supply co's networks via VPN are equipped with personal security software, latest security patches, anti-virus software and malicious code detection and repair software. This security software shall be activated at all time and with the latest virus signatures and malicious code definitions.

- Clock Synchronization.

  In order to comply with this policy user shall ensure that computers and network devices are synchronized with the local Supply co's NTP server if any

- SSO/Network Administrator has to ensure that Bios password has to be set for each system so that, the user cannot tamper with the system settings.
- It is advisable to disable USB port (Bios/disconnect from MB).
- The User will not attempt to override or break the security of the computers, networks,

  or machines/networks accessible there from. Services associated with the Net Access ID will not be used for illegal or improper purposes. This includes, but is not limited to, the unlicensed and illegal copying or distribution of software, and the generation of

threatening, harassing, abusive, obscene or fraudulent messages and also installing software.

- Users are strictly prohibited from establishing internet connections, using dongles, modems or other such apparatus, from within any supply co's premises.
- Users who have been given mobile/portable laptop or any other device and duly

  authorized for such remote access, which connects to supply co's systems on a real-time basis, can do so through the Internet with proper written request to Manage MIS/ Network Administrator before accessing the services.
- UnlessthepriorapprovaloftheManagerMIS/NetworkAdministratorhasbeen

  obtained, users shall not establish Internet or other external network connections that could allow non-authorized users to gain access to supply co's systems and information. These connections include the establishment of multi-computer file systems, Cloud storages, Internet web pages & FTP servers.
- Users must not test, or attempt to compromise computer or communication system

  security measures unless specifically approved in advance and in writing by the Manager MIS/Network Administrator. Incidents involving unapproved system cracking (hacking), password cracking (guessing), file decryption, software copying, software installation, computer configuration changing or similar unauthorized attempts to compromise security measures will be considered serious violations of SUPPLYCO policy and also initiate disciplinary proceedings against such user. Likewise, short-cuts bypassing system security measures is absolutely prohibited.

- Use encryption of information in compliance with Acceptable Encryption Use policy.
- Employeesmustuseextremecautionwhenopeninge-mailattachmentsreceivedfrom

  unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code, Ransom ware etc.

- Rebuilding the Computer System - When the Service engineers or SSO reform at the computer systems and re-install OS and other application software, care should be taken to give the same hostname, IP address, network Mask, gateway as it was having earlier. Further, after installing the OS all the patches/latest service pack should also be properly installed. In case of anti-virus software, service engineers/SSO should make sure that its latest engine and pattern files are also downloaded from the net. Further, before reformatting the hard disk, dump of only the data files should be taken for restoring it back after proper re-installation. Under no circumstances, software files from the infected hard disk dump should be used to write it back on the formatted hard disk.
- Preservation of Network Equipment and Accessories - Routers, Switches, Fiber optic cabling, UTP cabling, connecting inlets to the network, Racks, UPS, and their batteries

that are installed at different locations .Tampering of these items by the user comes under violation of policy and will be treated as misconduct, misdemeanor, or indiscipline as appropriate . Tampering includes, but not limited to,

- removal of network inlet box.
- removal of UTP cable from the room.
- opening the rack and changing the connections of the ports either at jack panel level or switch level
- taking away the UPS or batteries from the UPS room.
- disturbing the existing network infrastructure as a part of renovation of the location
- Tampering of the database by the Supplyco or individual user comes under violation of policy.

- disturbing the existing data items or software components deliberately with ulterior motives even by authorized individuals/Supply co's,
- Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
- Trying to break security of the Database servers.
- Modifying/deleting the data items or software components by using illegal access methods.

6.1.3 Changes to Systems/Network

- No user must physically connect or disconnect any equipment, including SUPPLYCO owned computers and printers etc to or from any SUPPLYCO network. With the exception of emergency situations, all changes to SUPPLYCO information technology systems and networks must be documented, and approved in advance by the ISO/Network Administrator.
- Only persons who have been authorized by the ISO can make emergency changes to any SUPPLYCO computer system or network.

6.1.4 Managing System Privileges

- Requests for new user-IDs and changes in privileges must be made to the MIS division

Supplyco in Mail. Users must clearly state why the changes in privileges are necessary.

- In response to feedback from the Human Resources Supplyco, the MIS division will revoke any privileges no longer needed by users. After receiving information from HR/Admin Supplyco ,all system accessprivilegeswillbeterminatedwithin24hours when a user leaves SUPPLYCO.

- SUPPLYCO management reserves the right to revoke the system privileges of any user at any time. Conduct that interferes with the normal and proper operation of SUPPLYCO information systems, which adversely affects the ability of others to use these information systems, or which is harmful or offensive to others will not be permitted.

6.2 SOFTWARE LICENSING POLICY

For all software including purchased, in-house developed or licensed business software applications, SUPPLYCO-written applications, employee or vendor/supplier-written applications, computer operating systems, firmware, and any other software residing on SUPPLYCO -owned equipment, all users must comply with the software licensing policy and must not use/install/download any software for their individual use or even for business purpose without prior approval of the ISO/Network Administrator at Head office. In case any such software is found on any SUPPLYCO system which is not allocated to the individual user, it shall be the responsibility of the user to inform the same to the MIS Division, in cases the same is not installed by the said user otherwise SUPPLYCO shall initiate appropriate disciplinary proceedings against the said user.

All necessary software's are pre-installed on all SUPPLYCO systems for day-to-day office needs. Request for any additional needs to be addressed to the Manager MIS/Network Administrator for approval. Employees shall not violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, the copying or distribution of "pirated" or other software products that are not appropriately licensed for use by Supplyco

Use of SUPPLYCO network resources to illegally distribute or duplicate unauthorized copyrighted or licensed material is prohibited. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

6.3 INTERNET AND INTRANET USAGEPOLICY.

System users will conduct due diligence when accessing the web and browsing the web shall strictly follow Supply co's principles and guidelines on accessing the internet. Supplyco shall consider whether usage of forums, social networks, etc is permitted or not.. ICT assets are protected against web-based threats by implementing measures that will prevent downloading software programs, active content and non- business related websites.

Internet Access may only be allowed with the approval of the ISO/Network Administrator .Access to the internet and its resources is provided for the purposes of conducting business on behalf of SUPPLYCO. Reasonable personal use of the Internet is permitted, according to constraints and conditions set out by the Firewall. A staff /officer in SUPPLYCO utilizing a SUPPLYCO IP address while connecting to the Internet or sending mail, shall do so only for purposes determined by the concerned sections.

The MIS division reserves the right to block access to any Internet resource without any prior notice, in case anyone required access to restricted site, the same may be dealt as special case provided the same is identified as use strictly for official purpose and

conducting SUPPLYCO business. The approval for the same needs to be obtained by the Supplyco Head from the Manager MIS.

Limited and occasional use of Information Systems to carry out Internet browsing, electronic posting or publishing is acceptable, provided that:

a. It is carried out in a professional and responsible manner;

b. It does not otherwise violate Supply co's policy or is detrimental to Supply co's best interests;

c It does not interfere with an employee's regular work duties.

Electronic posting or publishing by Employees on the Internet, public mailing lists, newsgroups, discussion groups, forums, blogs, etc. using Supply co's credentials (e.g. official email address, official designation/ address) MUST contain a disclaimer stating that the opinions expressed are strictly their own personal opinions/beliefs and not necessarily those of Supplyco. Supply co's trademarks, logos, branding and any other Supply co's intellectual property SHALL NOT be used in connection with any personal electronic posts or publishing. This provision does not affect officially authorized postings on behalf of Supplyco.

Employees MUST NOT make any discriminatory, disparaging, defamatory or harassing comments regarding Supplyco or its Employees in their electronic postings or publishing.

Employees, as per their employment contract, MUST NOT reveal any proprietary information, trade secrets, procurement details or any other material classified by Supplyco as Internal, Restricted or Confidential in their electronic postings or publishing.

Similarly, to protect Supply co's IT systems from imported viruses, downloading or exchanging screensavers, games, entertainment software or other inappropriate files (for example, video or audio materials for personal use), playing games against opponents or gambling over the internet is not permitted. Soft wares, software patches or updates may only

be downloaded, subject to approval and ensuring strict adherence to the vendor's security and usage guidelines.

Furthermore, users may not conduct any form of "hacking" or use malicious code to penetrate or attempt to penetrate other computers or to deliberately release viruses or other harmful programs within either the SUPPLYCO network or the internet or bypass security features.

Any connection from the SUPPLYCO network to an external network (wired or wireless) should be done or permitted only after the third party network / account has been approved by the Network Administrator or the ISO in the organization. Such clearances may be given after it is ascertained that the network / account has acceptable security controls, appropriate security measures and procedures (firewalls, filters etc) are in place. The integrity of the SUPPLYCO network should be preserved .The Network Administrator or System Administrator will need to regularly review audit trails and system logs of external network connections for abuses and anomalies.

Moreover, the Internet connection shall not be used for,

- Recreational downloads and peer to peer connections for recreational purposes are banned.
- Transferring copyrighted materials to or from the systems without express consent of the owner is a violation of international law. In addition, use of the internet for commercial gain or profit is not allowed. If done so, it will be sole responsibility of the user.
- Installation of unlicensed software on IT resources or on individual machines connected to the SUPPLYCO Network, is strictly prohibited.
- for hacking in to the computer system of the SUPPLYCO NETWORK or any other organization.

- for unauthorized copying or theft of electronic files.
- for passing on sensitive information of the Government, Supplyco without authorization.
- for sending of chain letters, religious images or messages or the like which may also lead to denial of service.
- for circulating letters, appeals or any content that is likely to create ill-will, hatred, violence or damage the image of the SUPPLYCO.
- for posting non-official related messages, groups on the Internet.
- for introduction of malicious programs into the network or server such as Viruses, Worms, Trojan, email bombs, Ransom ware and the like.
- for any form of harassment via email.
- for violation of any Government/Supplyco policy protected by copyright act, trade secret, patent or other intellectual property.
- for exporting software, technical information, confidential business data technical document, software codes, data, encryption software or technology of the organization.
- for revealing the user name and password to others or allowing the use of the account by others.
- for transmitting or viewing any material that is pornographic in nature or contributes to sexual harassment.
- for port scanning or sniffing (i.e., monitoring network traffic) except for those authorized to do so as part of their job.
- Blogging by officers and employees, whether using SUPPLYCO systems or personal

  systems, is subject to terms and restrictions .Blogging from SUPPLY CO systems is subject to monitoring by the organization. Employees shall not engage in any Blogging that may harm or tarnish the image of the organization. Employees should represent

themselves while Blogging and shall not represent themselves as a representative of the organization.

6.4 EMAIL USAGEPOLICY

Employee use e-mail with due diligence and include necessary classification labeling depending upon the content/attachments according to IT usage Policy. Appropriate measures are taken that e-mail is protected against potential threats as viruses, Trojans, spam mails, forgery and social engineering. Staff is aware that e-mails used to exchange confidential information SHOULD only be sent to named recipients and not to a group or distribution list.

Staff is aware that the use of automatic forwarding of e-mails is dependent upon the sensitivity

Emails carrying information classified SHALL NOT be automatically forwarded outside to the Supply co's systems.

Employees SHOULD NOT open email attachments received from unknown senders, as they may contain viruses, email bomb, malicious codes etc. Any email with an executable attachment SHOULD NOT be opened.

Employees SHALL NOT uses corporate email/messaging to distribute material that:

a. Is illegal or violates the morals and values of the Government of Kerala , Government of India;

b. May offend an individual or a group of individuals;

c. Typically qualifies as unsolicited email, chain emails, other scamming techniques.

All authorized officials/Outlets/Depots/Regional offices of SUPPLYCO are provided with an E-mail account, which is either individual to the specific user or generic Email ID and the same is protected with a password which is provided to the E-mail user. The use of E-mail should be restricted only for the business purpose; however personal mail can also be exchanged to a limited quantum provided that such exchange does not amount to breach of

this IT usage policy or otherwise materially affects SUPPLYCO's operations. In case any individual is found using e-mail service, which is objectionable by any means, the access can be terminated by MIS DIVISION without any prior information, however the same may be re-instated with the approval from the Managing Director and ISO.

Official email ids shall be provided to all Officials/Offices of SUPPLYCO on request and as per procedure laid down in this regard .Every employee shall use, as far as possible, the official email id for all SUPPLYCO business..Every employee shall be responsible for all communications received by him/her official email id. Such communication may not necessarily be followed by paper communication. However if the recipient desires he or she may request for authenticated copy of the mail to be sent. The authentication copy may be in the form of a paper copy duly signed or by means of a digitally signed electronic communication.

Email messages created in the conduct of SUPPLYCO business are official records and are the property of the SUPPLYCO. They have to be retained as evidence of business activities and to meet SUPPLYCO business requirements. All e-mail messages created or received by employees using the SUPPLYCO email systems may be accessed as part of a legal discovery process of Right to Information request.

Wherever email ids other than official email ids are used for conduct of official business, it shall be the responsibility of concerned employee to manage email messages by ensuring that email records are filed , retained and are accessible.

Email users should be aware that exchange of information with external sites may not be secured with high risks of spam, Trojans, malicious codes etc. Hence exchange of information should be limited to reliable sites. Users are prohibited to use their e- mail ids/mail

domain in public domain without prior authorization from ISO.

Information must not be transmitted internally or externally which is beyond the bounds of generally accepted standards, values and ethics. This includes, for example, material which could be considered offensive or discriminatory; pornographic or obscene, defamatory or any other material which is otherwise abusive or contains illegal content prohibited by law or

regulation of the country or which brings the organization into disrepute. Information is understood to include text, images and is understood to include printing information and sending information via email.

All material contained on the email system belongs to the SUPPLYCO and users should consider messages produced/received by them on SUPPLYCO account to be secure. Each employee using e-mail has a responsibility for the control and management of the email content. The confidentiality of email data should be maintained by the individual user.

Individual employees are responsible for creating, using, communicating and sharing e-mail messages in accordance with SUPPLYCO guidelines. They are also responsible for ensuring that e-mail records are kept as evidence of business activities and that these e-mail records are available to meet SUPPLYCO business and accountability requirements .This is especially relevant in case email ids other than official email ids are used for SUPPLYCO business. Individual employees are free to delete those mails which do not relate to SUPPLYCO business such as SPAM mails. Users should ensure that all the official emails are accessible to either their substitutes or their senior officer.

The head of the Supplyco or Divisional heads can share the official E-mail to their credible subordinate for official communication only.

Security regarding access to the email system is of paramount importance. User identities and personal passwords must not be shared with others. Users should be cautious of providing their email addresses to external parties, especially mailing lists.

E-mails can be a major source of viruses and, therefore, utmost care should be taken by individual user while accessing them and in case of doubt or a virus is suspected, the file or attachment must not be opened and the matter must be reported to the MIS-DIVISION immediately for inspection and action.

SUPPLYCO email users are required to use this communication tool in a responsible fashion and to observe the related guidelines. SUPPLYCO provides the email system for the purposes of conducting official business and it may not be used for personal gain or business activities

unrelated to SUPPLYCO's operations. Users must not use the system to promote an external cause without prior permission from the ISO.

It is forbidden to use electronic mail and other network communications facilities to harass, offend, or annoy other users of the network, including impeding their computing systems, software, or data. Chain letters are not allowed. Neither is any form of commercial advertising, or soliciting allowed. Spamming is strictly disallowed. 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). Any form of harassment via email whether through language, frequency, or size of messages., Unauthorized use, or forging, of email header information. 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. Creating or forwarding "chain letters" or other "pyramid" schemes of any type. Posting the same or similar non- business-related messages to large numbers of Usenet newsgroups spam.

Reasonable personal use of the email system is permitted. Personal use of the e-mail service must not interfere with SUPPLYCO's operations, involve cost implications for SUPPLYCO or take precedence over the user's job accountabilities.

Where it is considered that there has been a breach in the use of the email system, the service of the user will be terminated without any prior information.

6.5 LAPTOP POLICY

SUPPLYCO is issuing laptop computers to certain officers to facilitate their office works, while they are at travelling/home and associate communication. Officers shall exercise appropriate professional judgment and common sense when using SUPPLYCO's laptop computers, equipment and accessories.

All laptops, equipment and accessories are SUPPLYCO property and are provided to SUPPLYCO employees for a period of time as deemed appropriate by the organization. As a condition of their use of SUPPLYCO's laptop computers, users must comply with and agree to all of the following:

- Prior to being issued one of SUPPLY CO's laptops, User will sign the Laptop

Acceptance Form and agree to all outlined policies.

- User should NOT attempt to install software or hardware or change the system configuration including network settings.
- Users are expected to protect laptops, equipment and accessories from damage and theft.
- Each user is monetarily responsible for any hardware damage(including repair costs).
- User will not be held responsible for computer problems resulting from regular work-related use; however, associates will be held personally responsible for any problems caused by their negligence as deemed by SUPPLYCO.
- Users will provide access to any laptop computer or accessories they have been assigned upon SUPPLYCO's request.

General Laptop Rules

Employees SHALL ensure that laptops are kept under continual direct supervision when in use or kept secured when not in use. You are responsible for protecting your laptop from loss or theft and for protecting the information it contains. These rules are provided to assist in assuring that your laptop is secure at all times. All conceivable situations cannot be covered in this document. User must realize that common sense should be your guide when faced with unusual or unforeseen situations.

6.5.1 Power off your laptop whenever it is not in use. Do not carry the laptop in suspend or hibernation mode.

6.5.2 Personal use of the laptop, equipment and accessories is prohibited

6.5.3 Keep your laptop close to you and in sight. Otherwise, keep it locked away securely. It only takes a moment for a thief to walk away with your laptop.

6.5.4 Laptops are provided for official use by authorized employees. Supplyco laptops must not be loaned or be allowed to be used by others.

6.5.5 Laptops have anti-virus software installed, but laptops are vulnerable if the software is not kept up to date.

6.5.6 Laptops should not be connected to the Internet unless a suitable firewall package has been installed.

6.5.7 E-mail attachments are one of the main sources of virus – avoid opening any e-mail attachment unless they are expected from a legitimate source.

6.5.8 Report any security incidents (such as virus infections) to the IT Supplyco immediately in order to minimize the risk.

6.5.9 Report any security incidents (such as virus infections) to the IT Supplyco immediately in order to minimize the risk.

6.5.10 Do not download, install or use unauthorized software programs. No personal programs are to be used.

6.5.11 Never store passwords with your laptop or in its carrying case.

6.5.12 Other forms of user authentication should be kept separate from your laptop at all times.

6.5.13 Sincethelaptop'skeyboardandtouchpadarepermanentlyattachedtotherestofthesyste m, make sure that your hands are clean before using them. Because hand lotion is a major contributing factor to dirt and dust, please make sure your hands are free from lotion before using the computer. It is costly to change a laptop keyboard and/or touchpad that has been damaged be excessive dirt.

6.5.14 Do not place drinks or food in close proximity to your laptop.

6.5.15 Extreme temperatures can damage a laptop. You should not leave a laptop in an unattended vehicle.

6.5.16 In order to squeeze as much life out of your laptop battery, once your laptop hits 100 percent, unplug it.

6.5.17 Avoid discharging your laptop completely after charging it. The best thing you can do is try to keep the battery level between 20 percent to 80percent.

6.5.18 Supplycowillnottolerateinappropriatematerialssuchaspornographic,racist, defamatory or harassing files, photographs, videos or e-mail messages that might cause offence or embarrassment. Never store, use, copy or circulate such material on the laptop

6.5.19 Theuserofthelaptopmustcomplywithrelevantlaws,regulationsandpolicies applying to the use of Laptops and information, e.g .Supply co policy, license, copyright, and privacy laws.

7 DATA BACKUPPOLICY

In order to prevent loss of information by destruction of the magnetic means in which it is stored, a periodic backup procedure is carried out. The responsibility for backing up the server data at Head office located in shared network storage is the Network/Database administrators. It must be borne in mind that not only are hard disks inclined to fail, but also magnetic tapes are quite prone to errors that destroy their contents, so we need to do the restoration testing time to time basis. The responsibility of the Data base restoration is carried out by Data base / Network administrator on predefined time.

- **General Rule**: As daily Full backup is happening for all critical business applications (i.e. Monday to Sunday).

- **Data Backup in Database Servers**: The Systems Management backs up all the information in the databases through an automated procedure in predefined time..

- **DataBackupinDesktopPCatOutlet/Depot**:Thistaskistheresponsibilityofthe

Officer in charge to whom the Outlet/Depot responsibility has been assigned. The responsible officer should check regular backups of their vital data. Virus infections often destroy data on an individual's computer. Without proper backups, recovery of destroyed files may be impossible .Preferably, at the time of OS installation itself, onecanhavethecomputer'sharddiskpartitionedintotwovolumestypicallyCand

D. OS and other software should be on C drive and user's data files on the D drive. In case of any virus problem, generally only C volume gets corrupted. In such an event formatting only one volume, will protect the data loss. However, it is not a fool proof solution. Apart from this, users should keep their valuable data either on CD or other storage devices such as pen drives or shared volume of other computer connected in network.

- Ifanyoutlet/officehasmorethanonecomputerthebackupdatashouldstoredin

  another computer also.SSO should facilitate and provide awareness to the OIC or the personnel in responsible. SSO also has to verify and ensure that all outlets or depot under his purview are performing regular back up on their data.

8 VIOLATIONS

The following activities are, in general, prohibited:

Employees SHALL NOT engages in any activity that is illegal, using Supply co's Information Systems.

The following activities are strictly prohibited, with no exceptions:

a. Using Information Systems to actively engage in procuring or transmitting material that SHALL be deemed as obscene, offensive to the state and/or co-Employees;

b. Making fraudulent offers of products, items, or services originating from any Supplyco account;

c. Circumventing the security systems implemented to protect Information Systems;

d. Providing Supply co's Internal, Restricted or Confidential information including, personal information of organization, Employees, its financial information, data ,reports strategic plans etc. to parties outside organization for personal gain.

e. Using of anonymous, faked or forged identities on Information Systems

Incident Response**:**

An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Reporting Violations — System users shall report violations of this policy to the ISO/Network admin, and also immediately report defects in system accounting, concerns with system security, or suspected unlawful or improper system activities.

All Employees SHALL report any observed incident immediately to the MIS division helpdesk or alternatively to their line ISO. Incidents may be reported by phone ("0484-2207935/0484-2206791") or by email ("techsupport@supplycomail.com").

Abuse of Computing Privileges — Users of Supplyco information resources must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the Supplyco. For example, abuse of the networks to which the Supplyco belongs or the computers at other sites connected to those networks will be treated as an abuse of Supplyco computing privileges

Suspension of Privileges — System/network administrators may temporarily suspend access to information resource if they believe it is necessary or appropriate to maintain the integrity of the information resources under their oversight

Cooperation Expected — Information resource users are expected to cooperate with any investigation of policy abuse. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions

Accessing Information & Systems– Inspecting and monitoring information and information resources may be required for the purposes of enforcing this policy, conducting Supplyco investigations, ensuring the safety of an individual or the Supplyco community, complying with law or ensuring proper operation of information resources. Only the Information Security Officer (or designate) may authorize this inspection and monitoring.

Access for Legal and organization Processes-Under some circumstances, the organization may be required by law to provide electronic or other records, or information related to those records or relating to use of information resources, ("information records") to third parties. Additionally, the organization may in its reasonable discretion review information records, e.g., for the proper functioning of the organization in connection with investigations, or to protect the safety of individuals or the organization. The organization may also permit reasonable access to data to third-party service providers in order to provide, maintain or improve services to the organization. Accordingly, users of organization information resources do not have a reasonable expectation of privacy when using the Supply co's information resources.

Violations of policy will be treated as misconduct, misdemeanor, or indiscipline as appropriate.

All network failures and excess utilization are to be reported to the NOC. Non-intrusive monitoring of wide network traffic on routine basis will be conducted by Network Administrator. If traffic patterns suggest that system or network security integrity or net work performance has been compromised, Network Administrator will analyze the net traffic offending actions or equipment are identified and protective restrictions are applied until the condition has been rectified or the problem has been resolved. In this process, if need be, a report will be sent to ISO, in case the offenses are of very serious nature.

The policy may change as and when it is considered appropriate and new policies or the changes in policy will take effect immediately after a brief announcement by any means, e-mail, printed notices, or through the news groups.

…….. End of the Document…….....