Information Technology (IT) Policy

KIOCL Ltd

Contents

1. Introduction

1.1. Use of Information Technology (IT) in the day to day activities of Company has rapidly increased in recent years. Company has envisaged the use of IT to enable smooth function of its business. For the purpose of this policy, the term 'IT infrastructure' includes Desktop Computer, Laptop, portable and mobile devices, networks including Video conferencing devices, wireless networks, wired network, routers, switches, Internet connectivity, external storage devices and peripherals like printers and scanners and the software associated therewith.

1.2. Information Technology (IT) Policy is designed to guide the usage, manage and dissemination of Information and IT assets, as well as to ensure the continued delivery of services.

1.3. IT Policy shall help in optimizing the Information and IT facilities for the users, and to provide guideline to prevent the loss of data, security breaches or loss of Intellectual property, and events leading to disruption of business, loss of reputation and legal liability of the Company.

1.4. Misuse of IT Infrastructure can result in unwanted risk and liabilities for the Company. It is, therefore, expected that these resources are used primarily for official purposes and in a lawful and ethical way.

2. Scope and Applicability

The Information technology policy applies to all Company employees regardless of position and location. The policy shall be applicable to all external/ third party personnel (i.e. vendors, outsource employees, apprentice trainees, consultants, interns, contractors engaged by Company) who have access to Company's information.

This policy applies to all assets of IT Infrastructure (i.e. physical assets, information assets, Hardware and Software assets and services as an asset) at KIOCL.

3. Effective Date

This policy shall be known as KIOCL Information Technology (IT) Policy (the "IT Policy") and shall become effective from 05.03.2020.

4. Definitions of Key IT terms used

End Point Security: Securing end point devices such as Desktop and Laptop connected to an enterprise network.

End Point Devices: End point devices are Desktop, Laptop, Servers and Palmtop.

IAO: IT Asset Owner is the IT/Systems Department of respective location who shall manage the IT assets

Company: Company refers to KIOCL Limited.

5. Objective

The objective of the Information Technology (IT) policy is:

a. To establish a standardized IT Usage and Managing the IT asset by establishing comprehensive management process throughout the organization

b. To ensure electronic delivery of services to all stakeholders and business across all departments and functions to achieve the objective of transparency and efficiency.

c. To maintain confidentiality of data and to protect IT assets against unauthorized disclosure/usage.

d. To ensure integrity of data, availability and accessibility of IT Infrastructure as and when required.

6. Responsibility

a. It is the responsibility of the IT/Systems Dept. to monitor the state of IT systems and security.

b. Internal procedural changes if any shall be made with the approval of Competent Authority and same should be intimated to the users by IT/Systems Dept.

7. Account Privileges Policy

This user privilege policy is an internal IT policy and defines the privileges of various users on the Company network, who are allowed to have and specifically defines what groups of users have privileges to install computer programs on their own or other systems. This policy defines the users who have access to and control of sensitive or regulated data.

7.1. Policy Guidelines

There are three main categories of users on a computer and network. These categories include:

- **Restricted user** - Shall operate the computer and save documents but can't change system settings. Normally applies to contract employees, apprentice trainees and Guest user.

- **Standard user** –Shall use IT application and Infrastructure provided by IT/Systems department which are licensed and procured through IT/Systems department with the approval of Competent Authority and that does not affect Windows system files. Normally applies to regular employees of the Company.

- **System Administrators** - Have complete access to read and write any data on the system and add/remove/modify any programs or change system settings. Officers of IT department / Systems department of the Company will be the administrators. IT department / System department may authorise PC maintenance person to be disseminated as administrator.

8. Antivirus Policy

Defines anti-virus policy on every computer connected Company network defining the periodicity of virus updates, virus scan, detect, prevent, and remove malware.

8.1. Policy Guidelines

The Company uses a single anti-virus product for anti-virus protection. The following minimum requirements shall remain in force.

a) The anti-virus product shall be operated in real time on all end point devices such as Servers, Desktop, Laptop and Palmtop. The Bitdefender Endpoint Security is installed on all end point devices.

b) The anti-virus library definitions shall be updated at least once per hour.

c) Malware scans shall be done a minimum of once per day on all end point devices.

d) One should not stop anti-virus definition updates and anti-virus scans except by system administrators.

9. Application Implementation Policy

This policy is used to assess the security impact of new applications. When new applications are developed to provide new functionality to users, the impact of the new functionality must be assessed in order to keep the network stable.

9.1. Policy Guidelines

Once the data and application requirements are established, the computer security personnel, users, and application developers shall work together to provide required and reasonable access capability to systems and data both during development and final project implementation. Under no circumstances should the overall security of the network be seriously compromised for the benefit of any project.

Any changes and modification done on the developed application, the same shall be documented and logged.

The security assessment shall be conducted periodically for all applications and logged.

10. IT Asset Management Policy

Asset Management aims to achieve and maintain appropriate protection of Company's information assets. This involves:

a) Identification and categorization of all information assets

b) Maintenance of the asset inventory

c) Identification of the owners and custodians of the information assets

d) Identification of responsibilities of owners and custodians

e) Protection of information assets through appropriate access control

10.1. Policy Guidelines

a) All tangible and Intangible IT assets used are owned by the Company.

b) All IT assets issued by the company shall normally be used only for transacting official work of the company in a lawful and ethical way.

c) Use of resources provided by the Company implies the user's agreement to be governed by this policy.

d) IT/Systems department shall document & log the IT asset inventory and update the same on regular basis.

e) IT/Systems department shall be the IT Asset Owner (IAO) of all IT Assets and each user is the custodians of the IT assets used by them.

f) The responsibility for ensuring appropriate controls to safeguard the asset lies with the IAO.

g) Asset inventory shall be maintained and periodically audited. The asset inventory shall, at a minimum include information on type of asset, location, custodian/ user ,date of installation and its expiry.

h) All IT assets shall be handled as per the documented IT asset inventory.

i) The IAO may, at any time, upgrade information based on end of life of IT assets.

j) Access to any IT asset shall be defined by the IAO with the approval of concerned directors.

10.2. Security and Proprietary Information:

a) All active desktop computers and laptops shall be secured with a password-protected which should be set with automatic activation at 10 minutes or less, or log-off when the system is unattended.

b) User shall report any loss of data or accessories to the concerned authority of IT / Systems department of their respective location.

c) User shall obtain authorization from the concerned authority of IT/Systems Department before taking any Company issued desktop/Laptop outside the premises of their organization.

d) Users shall properly shut down the systems before leaving the office.

e) If users suspect that their computer has been infected with a virus (e.g. it might have become erratic or slow in response), it should be reported to IT / Systems department of their respective location for corrective action.

11. User Privilege Policy

KIOCL allows access to IT assets to full and part time employees, temporary employees such as interns, consultants and contract workers. Company reserves the right to withdraw such privileges based on the requirement.

11.1. Policy Guidelines

The following table maps the basic user privileges at the sole discretion of KIOCL management and expiration of those privileges.

Classification	Privileges	Expiry
Regular Full-Time Employee (General)	• Desktop PC, Laptop, Palmtop and associated IT infrastructure with applicable software. • Email id and Web browsing • Access to intranet applications. • VPN access to intranet application.	Till the date of separation of employee from Company.
Part-Time Employee	• Desktop PC, Laptop and associated IT infrastructure with applicable software. • Web browsing (including intranet)	Till the date of completion of tenure.
Intern / Contract worker	• Desktop PC, Laptop and associated IT infrastructure with applicable software. • Web browsing (including intranet)	Till the date of completion / termination of contract.
Consultant	• Web browsing (including intranet)	Till the date of completion / termination of contract.

The above privileges represent the allowable limit but subject to approval from Competent Authority depending on the need and circumstances. The IT/Systems department shall provide any additional privileges, with the prior approval of the Competent Authority.

12. Email Policy

E-mail systems are designed to improve services to customers, enhance internal communications and reduce paperwork. E-mail system has different risks than paper-based communications. This Policy is aimed at ensuring strict and appropriate controls for secure E-mail communications within and/or outside Company.

12.1. Policy Guidelines

a) E-mail ID is provided to employees who are required to communicate through E-mail for direct or indirect benefit of the Company.

b) Information created, sent, or received via Company's E-mail system including E-mail messages and electronic files, is the property of the Company.

c) Company reserves the right to:

- Decide E-mail ids to users
- Access, read, review, monitor, copy, intercept, block or auto forward E-mails and files on its system.

d) Management shall have access to all email messages whenever required to present to law enforcement agencies or third party without consent of the email user.

e) E-mails and electronic messages shall be protected from un-authorized access, alteration and denial of service.

f) Users shall abide by copyright laws, ethics rules, and other applicable laws while using Company E-mail system.

g) Users shall exercise sound judgment when distributing messages.

h) Client-related messages shall be guarded and protected.

i) User shall not use e-mail facility for un-authorized use. Unauthorized use of email system shall include but not limited to:

   i. Transmitting and/ or distributing E-mail containing derogatory, inflammatory, insulting, abusive, pornography or libellous information about any other employee, client, associate or any other person whatsoever.

   ii. Conducting any business (whether personal or professional) via Company E-mail system other than legitimate business of the Company.

   iii. Overloading unnecessarily or frivolously the E-mail system (e.g. chain mail, spamming, executable graphics and/or programs and junk mail which is not allowed.).

   iv. Enclosing information that is harmful to employees, business and reputation of the Company

   v. Accessing other's emails without the consent of the user by illegal methods

j) E-mail attachments with extensions like “exe”, “scr”,”vbs” & “vir” etc. shall be blocked for security reasons.

k) Use of E-mail system to solicit for commercial or personal benefit without appropriate authorization shall be prohibited.

l) E-mails sent outside KIOCL shall have an appropriate disclaimer attached as defined in clause No. 31.

m) Mailbox not accessed for specified period shall be deactivated. Mailbox of retired employees shall be removed with the consent of respective HoD.

n) Users shall report email security incidents to the respective IT/Systems Departments.

o) Wherever possible, for Inter departmental correspondence, email communication should be used instead of sending hardcopy of IOC's or IOC can be scanned and sent by email to avoid printing.

p) Violation of Email Policy shall invite disciplinary action.

q) The email ids are provided in the following pattern

- CMD and Directors are provided based on designation
- HOD's are provided based on department
- All other users are provided based on names.

13. Internet Usage Policy

Internet Usage Policy applies to all users who have been provided the Internet access. Use of the Internet is permitted and encouraged for official use only.

13.1. Policy Guidelines

a) Users shall use the Internet facility responsibly and productively. Internet access shall be limited to Company-related activities only.

b) All Internet data that is composed, transmitted and/or received by Computer systems is considered to be belongings of the Company and is recognized as part of its official data.

c) The Company reserves the right to monitor the Internet traffic, data and history of logs of individual users.

d) Users shall not undertake any activity through any website or applications to bypass filtering of the network or perform any other unlawful acts which may harm the network's performance or security

e) IT/Systems department may block content over the Internet which is in contravention of the relevant provisions of the IT Act 2000 (amended IT Act 2008) and other applicable laws or which may pose a security threat to the network. (Section 69A of IT Act 2000)

f) All sites and downloads may be monitored and/or blocked by the Company if they are deemed to be harmful and/or not productive to business

g) Unacceptable use of the internet by KIOCL employees includes, but not limited to:

i. Access to sites that contain obscene, hateful, pornographic, unlawful, violent or otherwise illegal material

ii. Sending or posting discriminatory, harassing, or threatening messages or images on the Internet or via email service

iii. Using computers to perpetrate any form of fraud, and/or software, film or music piracy

iv. Downloading, copying of pirated software and other unauthorised electronic files.

v. Sharing confidential material, trade secrets, or proprietary information of Company and its related business data outside of the Company

vi. Hacking into unauthorized websites

vii. Sending or posting information that is defamatory to Company, its products/services, colleagues and/or customers

viii. Introducing malicious software onto the network and/or jeopardizing the security of electronic communications systems

ix. Passing off personal views as representing those of Company

x. If an employee is unsure about what constitutes acceptable Internet usage, then he/she should inform the System Administrator.

14. Monitoring and Privacy:

The IT /Systems department, for security related reasons or for compliance with applicable laws, may access, review, copy or delete any kind of electronic communication or files stored on Company provided devices under intimation to the user. This includes data contained in files, e-mails, Internet history and any other digital formats.

15. Limited Personal Use of Network Policy

Limited personal use of computer and network resources is allowed, but priority is given to Company's business and user's personnel usage shall be with due approval from the head of Department.

15.1. Policy Guidelines

a) Users of the Company network may access the Internet or make phone calls for personal purposes, but Company is not responsible for the security and privacy of data or messages transmitted for such purposes.

b) Company does not guarantee availability, reliability or capacity of Internet or voice connection for personal usage.

c) Users may store a limited amount of personal data and documents not related to their work on their computers. If storage is overloaded, users may be asked to remove such personal data and documents. Company will neither take responsibility nor protects such personal data stored.

d) Users are cautioned that Internet surfing, watching videos or use of audio materials on a computer not connected to company's business during work time is likely to distract from efficient work.

16. Access to Social Media Sites from Company Network

The uptake and usage of Social media such as Facebook, Twitter, Instagram, WhatsApp etc, is gaining rapid popularity, use and utility of such media for official purpose remain ambiguous. Many apprehensions remain including, but not limited to issues related to authorisation to speak on behalf of department/agency, technologies and platform to be used for communication, scope of engagement, creating synergies between different channels of communication, compliance with existing legislations etc.

In order to encourage and enable government agencies to make use of this dynamic medium of interaction, a Framework and Guidelines for use of Social Media by government agencies in India has been formulated.

16.1. Policy Guidelines

a) User shall report any suspicious incident as soon as possible to the IT/Systems Department of respective location.

b) User shall always use high security settings on social networking sites.

c) User shall not post any material that is offensive, threatening, obscene, infringes copyright, defamatory, hateful, harassing, bullying, discriminatory, racist, sexist, or is otherwise unlawful.

d) User shall not disclose or use any confidential information obtained in their capacity as an employee/contractor of the organization.

e) User shall not make any comment or post any material that might otherwise cause damage to the organization's reputation.

17. Security Incident Management Process:

17.1. Policy Guidelines

a) A security incident is defined as any adverse event that can impact the availability, integrity, confidentiality and authority of Company data.

b) IT/Systems department reserves the right to deactivate/remove any device from the network if it is deemed as a threat and can lead to a compromise of a system under intimation to the competent authority of that location.

c) Any security incident noticed must immediately be brought to the notice of IT/Systems department.

18. Scrutiny/Release of logs

Notwithstanding anything in the above clause, the disclosure of logs relating to or contained in any IT Resource, to Law enforcement agencies and other organizations by the company as per applicable laws.

The Company shall neither accept nor act on the request from any other organization, save logs as provided in this clause, for scrutiny or release of logs.

19. Intellectual Property

Material accessible through the company's network and resources may be subject to protection under privacy, publicity, or other personal rights and intellectual property rights, including but not limited to, copyrights and laws protecting patents, trademarks, trade secrets or other proprietary information. Users shall not use the Company network and resources in any manner that would infringe, dilute, misappropriate, or otherwise violate any such rights.

20. Enforcement

It is mandatory for all users to adhere to the provisions of this policy.

21. Deactivation

21.1. In case of any threat to security of the Company systems or network from the resources being used by a user, the resources being used may be deactivated immediately by the Company.

21.2. Subsequent to such deactivation, the concerned user and the concerned authority shall be informed.

22. Portable device acceptable use Policy

In today's complex IT environment, use of Portable devices has increased intensely. Users need to ensure that confidential business information is not compromised and consider risks of working with Portable computing devices. This policy shall regulate the use of Portable devices in Company premises.

22.1. Policy Guidelines

a) Portable devices shall imply but not limited to

- Laptops/Palmtops
- Tablets/ I Pad
- USB/ Pen/ Flash Drive
- External Hard Disk
- Mobile Phones
- CD /DVD
- Dongle and Hotspot

b) Use of Portable devices by any employee shall be with approval of the Competent Authority.

c) Lost, stolen, or misplaced devices shall be immediately reported to the IT/Systems department and the concerned authority of the respective location.

d) Portable device users shall abide by the policy guidelines issued by the Company.

e) Portable devices shall be returned to IT/Systems Department on transfer or separation from the Company.

f) When installing software, user shall review the application permissions to ensure that unwanted information regarding the user is not shared with the application provider

g) All Portable devices shall be adequately protected against unauthorized access.

h) Users of Portable devices shall ensure that Company's business information is not compromised when using portable and communication devices like palmtops, Tablet, Laptops and Mobile phones either inside or outside office premises.

i) Users shall not allow USB device belonging to outsiders to be mounted on Company's IT devices.

j) In-charge of respective departments shall ensure that visitors to an organization shall not be allowed to carry any portable media without permission.

k) If it is necessary to allow the visitor to use a USB memory device for any reason, it shall be used only on designated systems meant for presentation purpose. Under no circumstances the USB device belonging to visitors shall be mounted on systems that are connected and belong to the Company Network.

l) In-charge of IT /Systems Department of the company shall ensure that process is in place to maintain records for procurement, issue, return, movement and destruction of the storage devices.

m) All obsolete USB devices shall be physically destroyed to avoid misuse

n) Self-certification for verification of USB devices by individuals at regular intervals of one year shall be carried out by issuing authority to ensure that devices issued to them are under their safe custody.

o) Access to Company's business information by remote users across public networks shall be granted after successful identification and authentication.

p) Use of personally owned portable devices shall be prohibited, unless authorized. Violation of this policy shall invite disciplinary action.

q) Users of portable devices shall ensure that they:

- Shall not connect to the office network from any public utility networks like cybercafé.
- Ensure the devices have latest antivirus software in consultation with IT /Systems department.
- Scan for malicious codes before connecting to office network and remove malicious code, if present, before connecting to Company network
- Shall not leave the mobile computing devices unattended.

23. Password Policy

The purpose of this policy is for creation of strong passwords, the protection of those passwords, and the frequency of change. Passwords are used for various purposes in the Company. Some of the regular uses of passwords in the Company include email accounts, screen saver protection, developer accounts, administrative accounts and local router/wifi logins.

The scope of this policy includes all end-users and personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system/service in the Company domain. These include personnel with their designated desktop systems. The scope also includes designers and developers of individual applications.

23.1. Policy Guidelines

a) Passwords must be changed on a regular interval according to the following schedule:

- All system-level passwords (e.g., root, application administration accounts etc.) must be changed every 90 days. All production system-level passwords must be part of the administered global password management database.

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 6 months.

b) User accounts that have system-level privileges must have a unique password from all other accounts held by that user.

c) All access codes including user ID passwords, network passwords, PINs etc. shall not be shared with anyone. These shall be treated as sensitive, confidential information.

d) The "Remember Password" feature of applications shall not be used.

e) Users shall refuse all offers by software to place a cookie on their computer excluding trusted sites such that they can automatically log on the next time that they visit a particular Internet site.

f) First time login to systems/services with administrator created passwords, should force changing of password by the user.

g) If the password is shared with support personnel for resolving problems relating to any service, it shall be changed immediately after the support session

h) Individual users are responsible for the protection of their passwords.

i) Users should change their passwords immediately if they suspect that it has been stolen or otherwise compromised. IT Dept to be contacted for guidelines and assistance.

j) Passwords must not be inserted into e-mail messages or other forms of electronic communication.

k) Users shall not share their account(s), passwords, security tokens (i.e. smartcard), Personal Identification Numbers (PIN), digital signatures certificate or similar information or devices which is used for identification and authorization purposes

l) All user-level and system-level passwords must use strong password that shall preferably have the following characteristics:

- Contain both upper- and lower-case characters (e.g., a-z, A-Z)

- Have digits and punctuation characters as well as letters e.g.,
  0-9,@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

- Passwords must contain at least 8 digits

- passphrase (Ohmy1stubbedmyt0e).

- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

23.1.1. Password for Application Development and System Administrator

Application developers must ensure their programs contain the following security precautions:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- For Password Change Control, both the old and new passwords are required to be given whenever a password change is required
- All designers/developers responsible for site/application development shall ensure the incorporation of this policy in the authentication modules, registration modules, password change modules or any other similar modules in their applications.
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

24. Printer Policy

The purpose of this policy is to implement a uniform and consistent approach to the allocation, access and usage of printers for business purposes. Printing documents and other material is an essential business function for maintaining records, reporting and other communications if required. To meet these business functions, Company is committed to providing printing devices that are fit for purpose and represent value for money. While printing is necessary in certain circumstances, it should be limited and carried out in an efficient manner

All employees are encouraged to consider using or storing electronic copies wherever possible instead of printing the documents. Personal usage of Company printers may be avoided.

24.1. Policy Guidelines

24.1.1. Access and Usage

In general, the following practices shall apply at all sites within scope:

Printers should be used only for Company business purposes. Only the necessary pages in the document are to be printed and also double-sided printing shall be done wherever possible.

A network printer will be made available to staff within close proximity to their work area.

Additional printers i.e. other than the network printers will be allocated to an individual or work group in exceptional circumstances, based on a business need substantiated and endorsed by the Head of Department and approved by the concerned Director.

A network printer should be used in preference to printers when producing a large number of copies.

Black-and-white printers should be used in preference to colour printers.

Confidential information which is printed should be collected from the printer immediately.

24.1.2. Colour Printers

The Colour printers shall be provided to the office of CMD and Directors. Colour printers shall be provided to the departments & projects, based on the requirement. The same shall be recommended by respective HoD's and approved by the competent authority.

The following practices shall apply:

a) Multi-function devices with colour copying/printing capability will be set to print in black-and-white only, with the ability to change the default setting for colour printing allocated to nominated personnel.

b) Documents, when deemed necessary, may be printed by the nominated staff in colour.

25. Purchasing IT Equipment & Failure Prevention Policy -

Procurement of any IT devices shall be done during the following conditions

a. When the device reaches the end of life
b. Based on the user's requirement
c. Failure of IT devices.

25.1. Policy Guidelines

25.1.1. IT Services for procurement

IT/Systems Department shall procure based on the requirement of users such as :

a) Desktop, Laptop and accessories.

b) Equipments for Printing, scanning, plotting and FAX

c) Web based application

d) Devices for Email services

e) Database services for internal users and critical external applications.

f) Critical external/internal application servers.

g) Network components like Firewall, switches, routers, cables etc

h) The software required to support the functions

i) Any servers or equipment that supports these services should adhere to this policy including connection equipment from the internet to these services.

25.1.2. Equipment Requirements

a) The hardware and software based on the requirement of the user

b) All critical services are required to utilize redundant technologies including:

- Dual power supplies on all servers providing critical services.
- RAID disk arrays to prevent one disk failure from interrupting services
- Uninterruptable power supplies that can provide power for a minimum of 1 hour to servers operating critical services in the event of a power outage.

c) Uninterruptable power supplies for all the IT infrastructure to address power outage or fluctuations issues.

26. Software Installation Policy

IT/Systems department with the approval of Competent Authority shall procure and install licensed software for the users as per the requirement.

Company recognizes its legal obligation to the holders of copyright on computer software. To fulfil the obligation, no user of Company shall make copies of computer software owned by Company unless written permission is obtained from Competent Authority. Copies made under license remain the property of the Company. Unless specifically allowed by the license agreement, no copies for personal use shall be made.

In addition to any civil or criminal penalty imposed by the software manufacturer, user of Company in violation of this policy may be subject to disciplinary action.

The users shall not copy or install any software on their own IT devices.

26.1. Policy Guidelines

All requests for new software installations must be made to IT/Systems department through the Head of Department for approval from the Competent Authority.

The request may be denied if:

- An insufficient number of licenses is procured

- The software is known to interfere with other applications or the Company Network
- If the software is a freeware and is expected to contain malware.

27. Third Party Management Policy

The purpose of this policy is to ensure appropriate control over security exposures and risks on services provided by external or third parties.

27.1. Policy Guidelines

a) Selection / appointment of third party for outsourcing or external facility management work shall be in-accordance with Company Policy.

b) All outsourced contracts requiring third party access to critical business information and systems of Company's application shall sign confidentiality agreements / non-disclosure agreements (NDA) with KIOCL.

c) Inventory of all IT assets such as equipment, licenses, backups, documents etc. shall be clearly identified and maintained by IT /Systems department.

d) Service level agreement shall be signed with external or third parties for providing services.

e) Periodic service assessment and review of all outsourced services shall be done for each service.

f) All external or third parties and their representatives shall bring to the notice of the Company, any weakness or incidents relating to information security during their period of contract in the Company.

28. Training Policy

This policy defines the minimum training for users on devices, application software and network usage to make them aware of basic computer usage and threats to protect the data on their devices, application and network.

This policy is designed to protect the Company's resources on the network and increase employee efficiency by establishing a policy for user training. When users are trained about computer use and security threats, they work more efficiently and are better able to protect Company resources from unauthorized intrusion or data compromise. This policy will help prevent the loss of data and Company assets.

Company needs to ensure that IT Training needs to be provided to the users periodically.

28.1. Policy Guidelines

28.1.1. Training Categories

Training categories shall include but not be limited to the following areas:

- Basic awareness on usage of IT equipments and application
- IT Security and Cyber Security
- Web based training
- Application Software
- User specific software

21.1.2 Training Mode

Training shall be provided either on premise, out station or through web learning depending on the requirement as per the approval of Competent Authority.

29. Wireless Networking Policy

This Policy applies to all wireless infrastructure devices that connect to a Company network that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and Tab / I-Pad. This includes any form of wireless communication device capable of transmitting packet data.

Unauthorised access of Wi-Fi facility provided to Directors/CMD office without the approval is strictly prohibited.

29.1. Policy Guidelines

All wireless infrastructure devices that connect to a Company network,

a) Shall be installed, supported, and maintained by IT/Systems dept.

b) Shall be connected by authorised user only.

c) A user shall register the access device and obtain one-time approval from the competent authority before connecting the access device to the Company’s wireless network.

d) To ensure information security, it is recommended that users should not connect their devices to unsecured wireless networks.

e) Usage of personnel devices on the network is strictly prohibited unless authorised.

f) Maintain a hardware address (MAC address) and IP Address which can be registered and tracked.

30. Website Maintenance Policy

This Policy applies to all users of the Company website.

This includes the updating of data, uploading of data such as documents, contents, photos and videos.

30.1. Policy Guidelines

a) All content on the website should have proper approval or authorisation before it is published and should be reviewed on regular basis.

b) Guidelines issued by Government/Government agencies regarding security, contents, design, style, etc. of the website from time to time should be followed.

c) All information published on the website should meet prescribed statutory requirements to bring more transparency about the working of the Company.

d) The Contents uploaded on the website will be responsibility of the respective nominated officers of the department and the same shall be regularly updated.

31. Email Disclaimer

This e-mail is for the sole use of the intended recipient(s) and may contain confidential and privileged information. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies and the original message. Any unauthorized review, use, disclosure, dissemination, forwarding, printing or copying of this email is strictly prohibited and appropriate legal action will be taken.

32. Review:

Future changes in this policy, as deemed necessary, shall be made by IT department with the approval of the competent authority.

-000-