INFORMATION TECHNOLOGY POLICY & PROCEDURE VERSION 1.0

The Jute Corporation of India Limited
15N, Nellie Sengupta Sarani
7th Floor
Kolkata – 700 087

SL No	Policy No	Version	Created By	Revised By	Approved By	Effective Date
1	JCI/IT/2020/01	1.0	Addl. Mgr. (IT)	AM (IT & Tech)	CMD	10/11/2020

Table of Content

1. Introduction

JCI is committed to leverage Information Technology as the vital enabler in improving the customer-satisfaction, organizational efficiency, productivity, decision-making, transparency and cost effectiveness, and thus adding value to the business of Jute.

Towards this, JCI -

- Follow best practices in Business Processes through IT by in-house efforts / outsourcing thus ensuring the quality of product and services at least cost.
- Follow scientific and structured methodology in the software development processes with total user-involvement, and thus delivering integrated and quality products to the satisfaction of internal and external customers
- Install, maintain and upgrade suitable cost-effective IT hardware, software and other IT infrastructure and ensure high levels of data and information security
- Strive to spread IT-culture amongst employees based on organizational need, role and responsibilities of the personnel and facilitate the objective of becoming a best business organization in our segment.
- Enrich the skill-set and knowledge base of all related personnel at regular intervals to make employees knowledge-employees
- Periodically monitor the IT investments made and achievements accrued to review their cost effectiveness.

2. Purpose

Information security policies provide a framework for best practices that can be followed by all employees. It also turns staff into participants in the company's efforts to secure its information assets. The Purpose of this policy is to outline the acceptable use of IT/Computer resources at JCI.

The policy should-

- Protect people & information
- Set the rules for expected behaviour by users
- Authorize security personnel to monitor, probe and investigate
- Define and authorize the consequences of violation
- Define the company consensus baseline stance on security
- Help minimize risk
- Help track compliance with regulations and legislation

A policy defines the organization's attitude to information, and announces internally and externally that information is an asset, the property of the organization and is to be protected from unauthorized access, modification, disclosure and destruction.

3. Scope

This policy applies to employees, contractors, consultants, trainees and other workers at JCI, including all affiliated with third parties. This policy applies to all equipment that is owned or leased by JCI.

This policy applies to all who access JCI Information Technology Infrastructure. The policy also applies to all computer and data communication systems owned by or administered by The Jute Corporation of India Limited.

JCI is committed to the appropriate use of Information Technology and its Services in support, productive, administrative, and service functions. This policy defines the acceptable behaviour expected of users and intending users of the facilities.

4. Term Definitions

#	Term	Definition	#	Term	Definition
1	IT	Information technology	2	Data	Digital form of information
3	JCI, Company	The Jute Corporation of India Limited	4	User	Personnel who use Information technology resources
5	HoD	Head of the Department	6	Biometric data	Biometric data can include fingerprints, voiceprints, facial shape, or scan of hand or face geometry
7	E-mail	Electronic mail	8	Spam	irrelevant or unsolicited messages sent over the Internet, typically to a large number of users, for the purposes of advertising, phishing, spreading malware, etc.
9	Junk Mail	Unwanted or unsolicited advertising or promotional material received through the post or sent as email.	10	SOP	Standard Operation Procedure

5. General Policy Principles

5.1. The JCI IT facilities are provided to assist employees and other authorized users.

5.2. All users must accept full responsibility for using the JCI's IT facilities in an honest, ethical and legal manner and with regard to the privacy, rights and sensitivities of other people.

5.3. IT Services provides comprehensive documentation and user guides on the IT infrastructure services and support as when required.

5.4. Authorised users only may use the facilities and a user may only use those IT facilities to which they are authorised / assigned / allotted.

5.5. Where access to a facility is protected by an authentication method, e.g. a password, a user must not make this available to any other person. Users who do so will be held responsible for all activities originating from that account. A user must not use an account set up for another user nor make any attempts to find out the password of a facility they are not entitled to use.

5.6. The above does not apply where a user provides access to their account to an authorized support person of the IT department for maintenance purposes.

5.7. JCI discourages the storing of passwords (Diary, notebook, etc) due to the security risks this poses.

5.8. Each user, while using their account, is responsible for all activities which originate from their account; is responsible for all information sent from, intentionally requested, solicited or viewed from their account; publicly accessible information placed on a computer using their account.

5.9. A user must:

5.9.1. Show restraint in the consumption of resources.

5.9.2. Respect intellectual property and the ownership of data and software.

5.9.3. Respect others rights to privacy and freedom from intimidation, harassment and annoyance.

5.9.4. Abide by the Company's policies regarding privacy

5.9.5. Abide by the Company's policies regarding antidiscrimination and harassment

5.10. No user shall:

5.10.1. Attempt to subvert the security of any of the Company's IT facilities.

5.10.2. Attempt to create or install any form of malicious software (for example worms, viruses, sniffers etc) which may affect computing or network equipment, software or data.

5.10.3. Attempt to interfere with the operation of any of the Company's IT facilities.

5.10.4. Attempt to subvert any restriction or accounting control of any of the Company's IT facilities

5.10.5. Attempt unauthorized access to any Company IT facilities.

5.10.6. The above may not apply to authorized support staff of / by the IT department in the performance of their duties.

5.11. The Company network and IT facilities, including email, application servers and other similar resources, may not be used for the creation or transmission of any material or data which could reasonably be deemed offensive, obscene or indecent.

5.12. Creation or transmission of defamatory material.

5.13. Transmission of material that infringes the copyright of another individual/organization.

5.14. Unauthorized transmission of material which is labelled confidential or commercial in confidence.

5.15. Transmission of any material that contravenes any relevant legislation.

5.16. Deliberate unauthorized access to facilities or services.

5.17. No user shall use the Company IT facilities for private gain or for financial gain to a third party.

6. Hardware/Software Policy

6.1. Purchasing Desktop/Laptop/Server/Networking Device/ Peripherals systems

6.1.1. JCI follows the laid-down norms for purchasing any type of good / service for any government / PSU organization, it includes Purchase through Gem, tender, spot purchase and other purchase mechanisms.

6.1.2. As per the Organization requirement the technical specification prepared by the IT Personnel /Committee for the required product.

6.1.3. Department Users can give their requirement through proper channels to the IT department and same may be verified by the technical team, based on the verification requirement report action can be taken for the same.

6.1.4. Purchase Order for any procurement (Product / Service) related to IT is to be issued from IT Department only and a copy is to be forwarded to other departments.

6.1.5. Open source or freeware software can be obtained without payment and usually downloaded directly from the internet. In the event that open source or freeware software is required, approval from IT HoD must be obtained prior to the download or use of such software. All open source or freeware must be compatible with the business's hardware and software systems.

6.1.6. Adoption of Open Source Software - Please refer to "Policy on Adoption of Open Source Software for Government of India" vide Ref. No. 1(3)/2014 – EG II by Department of Electronics & Information Technology, MoCIT.

6.1.7. In case, any variation of "Policy on Adoption of Open Source Software for Government of India", specific approval with suitable justification is to be placed before Competent Authority prior to issuing Purchase Order.

6.2. Policy for Use of Hardware/Software

As per HR/Admin policy new Hardware or software issue to Employee by IT/admin department however the customization of the new hardware or software done by IT department if any requirement occurred.

6.3. Software Licensing

6.3.1. All computer software copyrights and terms of all software licences will be followed by all employees of the business.

6.3.2. Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of IT HoD to ensure these terms are followed.

6.3.3. IT HoD is responsible for completing an IT audit or following the standards quality procedure (SOP) for all hardware, software to ensure that copyright and licence agreements are adhered to.

6.4. Software Installation

All software installation/updates is to be carried out by IT department personnel or the concern service provider. A software upgrade shall not be installed on a computer that does not already have a copy of the original version of the software loaded on it.

6.5. Software Usage

6.5.1. Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

6.5.2. All employees must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This will be the responsibility of

the IT department personnel or the concerned service provider as per the software/Hardware purchase/service policy.

6.5.3. Employees are strictly prohibited from installing any software in the system provided by JCI on his / her own. If any software is required to be installed, an intimation is mandatorily sent to the IT Administrator and any statutory compliance liability regarding licensing will not be upon JCI. If any software other than prior installed / intimated, is found to be installed in any of the system during audit, necessary action may be taken as may be deemed fit.

6.5.4. Where an employee is required to use the assigned system outside his/her head-quarter while on leave / duty, prior intimation is to be given to the IT / Administration Department and during that period, security of the system will lie upon that concerned employee.

6.5.5. Unauthorised software is prohibited from being used in the business. This includes the use of software owned by an employee and used within the business.

6.5.6. The unauthorised duplicating, acquiring or use of software copies is prohibited. Any employee who makes, acquires, or uses unauthorised copies of the software will be referred to IT HOD and appropriate disciplinary action can be taken for the same. The illegal duplication of software or other copyrighted works is not condoned within this business and IT HOD is authorised to undertake disciplinary action where such an event occurs.

6.5.7. Where there is a breach of this policy by an employee or Where an employee is aware of a breach of the use of software in accordance with this policy, they are obliged to notify IT HOD immediately.

7. Privacy Policy

JCI seeks to comply with the privacy requirements and confidentiality in the provision of all IT Services. Users must also be aware that, network and systems administrators, during the performance of their duties, need to observe the contents of certain data, on storage devices and in transit, to ensure proper functioning of the JCI IT facilities.

The Company's policy and statutory obligations relating to privacy will be upheld in all cases.

8. Security Policy

JCI recognizes the importance of information technology security and is committed to ensure all business activities performed with the employment of information technology are protected and maintained, and that sustainable procedures are in place to reflect "best practice" information technology security. Since we have neither using any external online web server for any JCI application purpose nor maintaining WAN network so the use of separate firewall or Unified Threat Management not in place in business however with technology upgradation and better security of data it will be proposed in near future.

Presently all the Information security levels are managed at the End-user level.

8.1. Physical Security:

8.1.1. For all servers and other network assets, the area must be secured with adequate ventilation and appropriate access through lock/biometric/network rack lock/cabling cover etc.

8.1.2. It will be the responsibility of JCI's IT HOD to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify IT HOD immediately.

8.1.3. All security and safety of all portable technology, such as laptop, tablet, mobile etc will be the responsibility of the employee who has been issued. Each employee is required to use such as locks, passwords, etc. and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

8.1.4. In the event of loss or damage, IT HOD/Management will assess the security measures undertaken to determine if the employee will be required to reimburse the business for the loss or damage.

8.1.5. All IT equipment such as laptop, notepads, iPads etc. when kept at the office desk is to be secured by such as keypad, lock etc. provided by admin department.

8.2. Password Policy

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of JCI's entire corporate network. The purpose of this policy is to establish a standard for creation of strong passwords, protection of those passwords and the frequency of change.

8.2.1. All system-level passwords (e.g., root, admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

8.2.2. All user-level passwords (e.g. email, web, desktops etc.) must be changed at least every six months. The recommended change interval is every three months.

8.2.3. User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.

8.2.4. Users are advised not to access official portals, email over public network / wifi hotspot in public places.

8.2.5. Passwords must not be inserted into email messages or other forms of electronic communication

8.2.6. General Password Construction Guidelines

8.2.6.1. Passwords are used for various purposes at JCI. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, and local router logins. Very few systems have support for one-time tokens (i.e. dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

8.2.6.2. Poor, weak passwords have the following characteristics:

8.2.6.2.1. The password contains less than eight characters

8.2.6.2.2. The password is a word found in a dictionary (English or foreign)

8.2.6.2.3. The password is a common usage word

8.2.6.3. Strong passwords have the following characteristics:

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

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

8.2.7. At the time development of any new portal/application, password policy must be enforced.

8.3. E-Mail Security Policy

JCI having cloud base Mail solution for their employee which can be access through internet service. Too keep it safe and secure there are some Standard practices always followed like:

8.3.1. The attachment(s) must be scanned before opening as well as confirming the sender that indeed an attachment has been sent. This will also reduce the risk of running a program that has been e-mailed out automatically (unknown to the originator) via some kind of malicious application that has made use of the mail account(s) and/or mailing system of the sender.

8.3.2. Do not use the company e-mail accounts for registration purposes of any kind service and do not use it while posting messages in web forums or newsgroups.

8.3.3. Do not use the company e-mail system for running own business, excessive personal mailing, sending large attachments, thus wasting valuable bandwidth.

8.3.4. Do not respond to chain letters, or any other sort of spam using the company e-mail systems.

8.3.5. Never forward any company data to external e-mail accounts.

8.3.6. The proper use of the E-mail system should continuously be monitored and the users should be aware that they could be held liable for illegal activities, such as spamming, sending and receiving illegal content, etc. from their account.

8.3.7. Any kind of harassment via email should not be done.

8.3.8. Do not send any unsolicited email messages, including the sending of "Junk Mail" or other advertising material to individuals who did not specifically request such material.

8.3.9. Postings by an employee from JCI email address to newsgroups should contain a disclaimer stating that the opinions expressed in the message are strictly their own and not necessarily those of JCI, unless posting is in the course of business duties.

8.3.10. One should not transmit the information through email as defined by corporate confidentiality guidelines. Confidential information includes but are not limited to company private, corporate strategies, competitor sensitive, trade secrets, customer lists and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

8.3.11. Also take the proper backup of sent mails and clear it at regular interval to ensure proper functioning of the mailing solution with better utilization of the resources.

8.3.12. Where an employee forgets the password or is 'locked out' after multiple attempts, then Contact IT personnel who are authorised to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

8.4. Antivirus & Malicious Code Policy

Antivirus and malicious code protection software are made available at user PC/Desktop to secure the user data and transaction certain level. Too keep secure and unharmed by these malicious codes, users must follow some standards practice like:

8.4.1. Do NOT run any files without first scanning them, no matter what the file extension is, i.e. (.exe, .bat, .com, .doc, etc.)

8.4.2. Do NOT download any files and/or programs from unknown sources, if in doubt, contact the IT department personal.

8.4.3. Do NOT open attachments, even if they were sent by a friend or family member, verify first that indeed, he/she has sent the file, but nevertheless scan before open/run anything.

8.4.4. Do NOT run any programs that have found on diskettes/CD's around desk if not completely sure about the belongingness.

8.4.5. If downloading is allowed, limit it to the minimum, if need a specific application or something else, always contact the IT department for further information BEFORE download and installing something;

8.4.6. Scan (full system scan) the system at least once per week with Corporate standard /default Anti-Virus scanner software which is available with the IT department and loaded on user PC/System;

8.4.7. Update the antivirus signature files as often as possible, so to ensure that the latest malicious software patterns are detected.

8.4.8. If having any doubts regarding malicious software (viruses/Trojans/worms), contact the IT department immediately to prevent any potential devastating mishaps, due to inappropriate and erroneous handling of dangerous and harmful incidents.

8.4.9. Backup critical data and system configurations on a regular basis and store the data in a safe place.

9. The Network Policy

The Company operates a computer network, which is designed to facilitate communication within the HO and with other RO/RLD for employees and other authorized users.

9.1. Access to the JCI Network

Each employee can be access JCI network by their assigned Compute IT system with the authorised user name and password. User can be connected/access through wired or wireless. The hardware (MAC) address of the system will be recorded such that it may be entered into the department's DHCP system for security purpose.

9.2. Network Modification/Upgradation

All cabling modifications or additions to the IT network must be coordinated through JCI's IT department to ensure they comply with national, state and local codes as applicable to wiring methods, construction and installation of data and communications cabling systems, and equipment as per standard Guidelines.

Only JCI's IT department approved or nominated contractors are authorised to replace, repaired or modification can be permitted.

9.3. Internet Usage Policy

Internet shall be used only for business work. Internet facility shall be provided to JCI user and company reserves every right to monitor, examine, block or delete any/all incoming or outgoing Internet connections on the company's network. Other requisites on internet usage are as mentioned below:

9.3.1. Internet access shall be provided on "need to use" basis. Anyone who requires it shall be given access after appropriate authorization. Such access shall be reviewed periodically by the IT Personnel.

9.3.2. Corporate Mailing solution is available to all having corporate email Id. Use of personal Instant messenger and chat is prohibited. Users shall not carry out any objectionable, frivolous or illegal activity on the internet that shall damage the company's business or its image.

9.3.3. Users shall not attempt to subvert security measures on either the company's network resources or any other system connected to or accessible through internet.

9.3.4. Users shall not post to public discussion groups, chat rooms or other public forums representing the company on the Internet unless pre-authorized by company. Users shall not send on the internet, any information other than "JCI General business", the disclosure of which may in any case cause harm or loss to either the company's or its customers' reputation.

The Following services are blocked by default and can be revoked as per the decision made by the management -

- Access to download executable files
- Access to sites related to sports, finance, news and jobs
- Entertainment software or games, or play games over the internet.
- Freeware / shareware / unlicensed software or tools without prior consent from authorized personnel.
- Users with internet access shall not upload Any software licensed to JCI, Data owned or licensed by JCI, Documents classified as JCI Proprietary, JCI Confidential or JCI Internal Use, without explicit authorization
- Images or videos unless there is an explicit business-related use for the material. Or display any kind of sexually explicit image or document on any company system. In addition, sexually explicit material shall not be accessed, attempted to be accessed, archived, stored, distributed, edited, or recorded using JCI's network or computing resources.

10. Data Policy

10.1. A user must not examine, disclose, copy, rename, delete or modify data without the express or implied permission of its owner. This includes data on storage devices and data in transit through a network.

10.2. A user must respect the privacy and confidentiality of data stored or transmitted on the Company's IT facilities. Any release of data to those not authorized to receive it is expressly forbidden.

10.3. Users storing data of a sensitive nature, such as information on individuals whether for administrative or services use must ensure that the privacy of such information is not compromised.

10.4. The Company has a legitimate right to capture and inspect any data stored or transmitted on the JCI's IT facilities (regardless of data ownership), when investigating system problems or potential security violations, and to maintain system security and integrity, and prevent,

detect or minimize unacceptable behaviour on that facility. Such data will not be released to persons within or outside of the Company, except who authorised to.

10.5. Access to any data will always be via network or systems administrators, or via persons nominated by the head of IT.

11. Equipment Policy

11.1. Users must take due care when using IT equipment and take reasonable steps to ensure that no damage is caused to IT equipment.

11.2. Users must not use IT equipment if they have reason to believe it is dangerous to themselves or others to do so.

11.3. Users must report any damage to IT equipment to IT personnel.

11.4. User has no authorization to use their own software or hardware to attach any device to Company IT facilities or connect any equipment to the Company network without the prior written approval of the head of IT department or delegated persons, that such connection meets Company security standards.

12. Biometric Device Policy

JCI maintain biometric system for attendance's record keeping purpose. Every JCI's Employee need to register biometric attendance system as per advised by JCI admin/HR department. An individual's biometric data (Finger print) will be stored for attendance purpose only and JCI will destroy biometric data when the initial purpose for obtaining or collecting such data has been fulfilled.

12.1. For better performance of the device user must keep their finger clean and use the full face of the finger scanner of the biometric.

12.2. For any help contact to the IT personnel.

12.3. JCI's policy is to protect and store biometric data in accordance with applicable standards and laws.

13. Data Backup policy

This policy defines the Data backup for IT system within the organization. These systems are typically servers/desktop/Laptop but are not necessarily limited to servers. Servers expected to be backed up include the application server, tally, mail server, Attendance server, data base server etc.

13.1. Data to be backed up include the following information:

13.1.1. User data stored on the hard drive.

13.1.2. System state data

13.1.3. The registry

13.2. Systems to be backed up include but are not limited to:

13.2.1. Application server

13.2.2. Database server

13.2.3. Biometric Server

14. Custom IT Software Application Policy

JCI has its own in-house developed software for purchase, Inventory and Parole management. It's been fully managed by the JCI's IT personnel.

Other standard procedure for using software, backup etc. are applicable as mention in this policy document will be applicable.

In future whenever any new requirement arises to develop a indigenous software / application, following documentation is to be followed –

- Software Requirement Specification (SRS)
- User Acceptance Testing (UAT)
- Third-party Testing (as per requirement)

14.1. Software Requirement Specification (SRS)

As per industry practice, following nine topics that must be addressed when designing and writing an SRS:

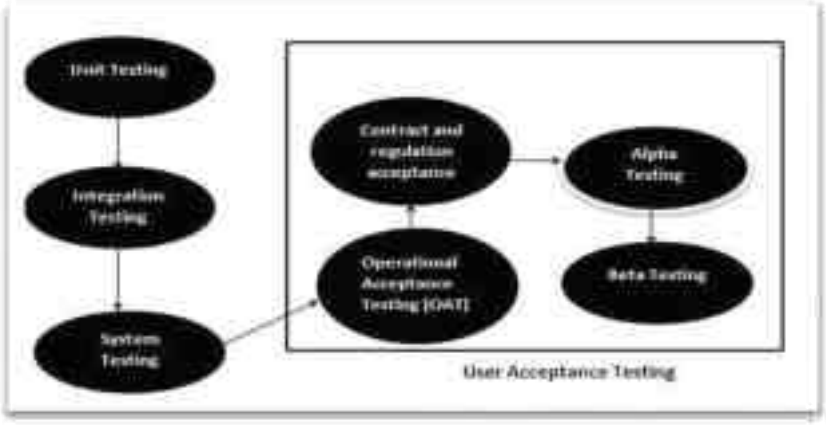
- Interfaces
- Functional Capabilities
- Performance Levels
- Data Structures / Elements
- Safety
- Reliability
- Security / Privacy
- Quality
- Constraints and Limitations

A sample of a basic SRS outline may be adapted from IEEE Standard 830-1998 (Superseded by IEEE/ISO/IEC 29148-2011).

14.2. User Acceptance Testing

User acceptance testing, a testing methodology where the clients/end users involved in testing the product to validate the product against their requirements.

The following diagram explains the fitment of user acceptance testing in the software development life cycle:



The acceptance test cases shall be executed against the test data or using an acceptance test script and then the results are compared with the expected ones.

14.2.1. Acceptance Criteria

Acceptance criteria will be defined on the basis of the following attributes:

- Functional Correctness and Completeness
- Data Integrity
- Data Conversion
- Usability
- Performance
- Timeliness
- Confidentiality and Availability
- Installability and Upgradability
- Scalability
- Documentation

14.2.2. Acceptance Test Report - Attributes

The Acceptance test Report should have the following attributes:

- Report Identifier
- Summary of Results
- Variations
- Recommendations
- Summary of To-DO List
- Approval Decision

14.3. Third-party Testing

After obtaining UAT Reports, third-party audit requirements – functional and security are to be fulfilled prior to launching of the software / application. Third-party audit can be conducted by Standardisation, Testing and Quality Certification (STQC) – MeitY or any Cert-IN empanelled auditors.

Designing and/or writing of SRS and obtaining of UAT Reports & Third-party audit reports will be the responsibility of Project In-charge / Nodal Officer.

N.B.: For security of custom developed web application and mobile application OWASP ASVS v4.0 and OWASP MASVS v1.2 are to be followed respectively.

15. Website policy

15.1. Website Register

The website register must record the following details:

- List of domain names registered to the business
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting

15.2. Website Content

- All content on the business website is to be accurate, appropriate and current. This will be the responsibility of IT HoD.
- All content on the website must follow JCI's Business requirement.
- The content of the website is to be reviewed by regularly basis by the Authorises Personnel.
- The following persons are authorised to make changes to the JCI's website:
  - ✓ Name1
  - ✓ Name2
  - ✓ Name3

15.3. Security Audit of the Website should be done once in every three years.

16. Cloud Service Adoption Policy

JCI will follow Guidelines issued by MeitY from time to time in this regard. For hiring of cloud services, list issued by MeitY for "MeitY empanelled Cloud Service Providers (CSP)".

Guidelines issued by MeitY should always be referred while procuring any Cloud Services for hosting of any application on Cloud Server –

- Guidelines for Enablement of Government Departments for Adoption of Cloud v2.1
- Guidelines for User Departments on Service Level Agreement for Procuring Cloud Services v1.0

17. Document Digitisation Policy

Policy and procedure for Documents digitisation have been detailed in "Policy & Procedure for Document Digitisation".

18. IT Emergency Management Policy

    In the event of any services like IT Hardware/software Failure, Virus/Trojan, website issue, physical damage, threat, fire or any interruption in IT services must bring notice to the IT personnel /IT HoD. IT Emergency Management Team will handle the situation.

19. Enforcement Policy

    This Policy applies to all of the IT services offered by JCI IT and services offered on third-party. This Privacy Policy doesn't apply to services that have separate policies that do not incorporate in this Policy.

    Any personnel who are related to JCI directly or indirectly if violated the norms of IT policy may be subject to disciplinary action.

20. Review Policy
    This policy will be reviewed in every 2 years.