GL BAJAJ
Institute of Management & Research . PGDM Institute
FIND YOUR SPARK
Approved by AICTE, Ministry of HRD, Govt. of India

Information Technology (IT) Policy
(GLBIMR)

GL BAJAJ
Institute of Management & Research . PGDM Institute
FIND YOUR SPARK
Approved by AICTE, Ministry of HRD, Govt. of India

INDEX

S. No	IT Policies & Supportive Content
1	Introduction
2	IT Services Policy
3	Data backup Policy for faculty, staff and students
4	IT Hardware Installation Policy
5	Software Installation and Licensing Policy
6	IT Services helpdesk policy
7	Network (Intranet & Internet) Use Policy
8	Email Account Use Policy
9	Website Hosting Policy
10	Institute Database Use Policy
11	CCTV Surveillance Policy
12	Data Recovery in case of Disaster
13	Power Backup policy for IT hardware
14	Cyber Security and Data Privacy
15	Review and Revision Policy

1. Introduction

GLBIMR IT policy exists to maintain, secure, and ensure legal and appropriate use of information technology infrastructure established by the Institute on the campus. This policy establishes Institute-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability (CIA) of the information assets that are accessed, created, managed, and/or controlled by the Institute. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property.

Intranet & Internet services have become most important resources in educational institutions & research organizations. GLBIMR took initiative in 2018 and established basic network infrastructure in the academic complex of the Institute.

Over the last many years, not only active users of the network facilities have increased many folds but also the web-based applications have increased. This is a welcome change in the Institute's academic environment.

Internet Unit is running the Firewall security, DHCP, DNS, email, web and application servers and managing the network of the Institute.

GLBIMR is getting its Internet bandwidth from CJ Online. Total bandwidth availability from CJ Online source is 300 Mbps (leased line).

While creating these policies, every effort has been made to have a careful balance between security and the ability to conduct the rightful functions by the users. Further, due to the dynamic nature of the Information Technology, Information security in general and therefore policies that govern information security process are also dynamic in nature. They need to be reviewed on a regular basis and modified to reflect changing technology, changing requirements of the IT user community, and operating procedures. Purpose of IT policy is to set direction and provide information about acceptable actions and prohibited actions or policy violations.

Guidelines are created and provided to help organization and individuals who are part of Institute community to understand how Institute policy applies to some of the significant areas and to bring conformance with stated policies.

The current IT policy is sub-divided into following:

- IT Services Policy
- Data backup Policy for faculty, staff, students
- IT Hardware Installation Policy
- Software Installation and Licensing Policy

- IT Services helpdesk policy
- Network (Intranet & Internet) Use Policy
- E-mail Account Use Policy
- Website Hosting Policy
- Institute Database Use Policy
- CCTV Surveillance Policy
- Data Recovery in case of disaster
- Power Backup policy for IT hardware
- Cyber Security and Data Privacy
- Review and Revision policy

Further, the policy will be applicable at two levels:

1. End Users Groups (Faculty, Students, Senior administrators, Officers and other staff)
2. Network Administrators

It may be noted that Institute IT Policy applies to

1. The technology administered by the Institute centrally
2. The information services provided by the Institute administration, or by individuals of the Institute community, or by authorized resident or non-resident visitors on their own hardware connected to the Institute network.
3. The resources administered by the central administrative departments such as Library, Computer labs, Offices of the Institute wherever the network facility was provided by the Institute.
4. Computers owned by the individuals, or those owned by research projects of the faculty, when connected to campus network are subjected to the Do's and Don'ts detailed in the Institute IT policy.

Further, all the faculty, students, staff, authorized visitors/visiting faculty and others who may be granted permission to use the Institute's information technology infrastructure, must comply with the Guidelines. The violation of this IT policy by any Institute member may result in disciplinary action against the offender by the Institute authorities. If the matter involves illegal action, law enforcement agencies may become involved.

2. IT Services Policy

IT Services provides a wide range of computing and communication facilities for faculty, staff and students. IT Services has a clear user focus, which is aimed at "providing a high-quality service", includes

- Ensuring services meet user requirements
- Monitoring the performance of services
- Providing a cost-effective service
- Applying a flexible operation appropriate to the vision of the Institute
- Providing effective communication and keeping the users informed
- Achieving user satisfaction

The purpose of this policy is to set out the services provided by IT. The Services IT manages includes:

1. Desktop & Laptop computing and support
2. Central computer hardware and networks
3. IT Strategy and the introduction of new systems
4. Day to day operation of existing systems

A brief summary of the range of services offered by IT Services is set out below.

1. Desktop computing and Support
2. IT Helpline the IT Services Helpline provides a first point of contact to IT Services for most users. Helpline Advisers provide help with a wide range of standard queries and ensure that problems are dealt with. The Helpline also deals with requests for new IT equipment and manages the communications to all staff about service availability for all systems.
3. Standard Hardware IT Services advise and recommend the choice of IT equipment. This includes purchases made with external/research funding. IT Services also co-ordinates ordering of all IT equipment and software to ensure cost-effective investment in IT.
4. License Software

   Institute's desktop software is licensed under a central license agreement from Microsoft apart from the opensource software. Other software, which has been properly evaluated, is available from a recommended software list. Requests for software can be made through IT Services Helpline.

5. Desktop/laptop support (including Audio Visual)

   Support for around 282 Institute computers/laptops. Core supportincludes:

   - Installation of relevant software
   - The setup of network connections, access to email, network file space and Internet
   - Fault diagnosis
   - Application of fixes on software and hardware
   - Central Computer Hardware and networks

6. Networks Manages the Institute networks including the campus' mobile network and importantly its connection, which interconnects each other.
7. Servers
   Management of the Institute's core servers housed in specially equipped data centers with secure, temperature-controlled environments. Key activities include server back-ups, upgrades, patches, and service enhancements.
8. Developing and maintaining Standard and specialist software 'images' for staff desktops, open access areas and IT teaching lab. IT Services also maintains a Institute wide printer strategy including deployment of MFP & Scanner.
9. Day to day operation of existing systems
   a. Support: Maintaining a wide range of the Institute's existing systems to diagnose and fix problems, which arise as well as applying and testing supplier upgrades and patches.
   b. Enhancement: Working with the users and suppliers to specify, develop and test changes to existing systems as these arise.
   c. Identity Management: Supporting and maintaining identity and access to systems by delivering a single view of a user's identity across the Institute Integration Developing and managing the integration points between existing systems
10. Operational Services
    a. IT Helpline & Problem Resolution
    b. New Username & Password: for Access the Institute internet and network
    c. New or replacement standard PC
    d. Specialist computer Hardware
    e. Mobile phone or mobile computing device
    f. Specialist computer Software
    g. Desktop software

h. Network access and Wi-Fi connectivity
i. Personal Storage
j. Email Services – Students & staff

Services Provided - First line support to staff, students, external customers is available 24 hours a day all year round.

End-User responsibilities - Provide adequate information in order that a ticket can be logged relating to the nature of the query.

IT Team monitors all open incidents and escalate unresolved incidents to individuals and groups who can help to resolve the problem.

User Feedback and Complaints

Feedback

If end-user would like to leave feedback or are not satisfied with our services, please let us know as soon as possible, so that we can do our best to put things right. All feedback is reviewed by management to monitor user satisfaction and ensure our continual service improvement. Please use our Grievance and Redressal in ERP.

3. Data backup Policy for faculty, staff and students

Scope of Procedure and Rationale

The main goal of the data protection strategy is to protect GLBIMR's data by having it backed up to an alternate location away from where the primary data resides. Electronic backups are a requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, sabotage, ransomware, data entry errors, or system operations errors.

Service Availability

Backup services are available as a standalone option. Backup services are bundled with storage services. The bundled storage/backup services is primarily done using cloud and a secondary storage/backup is available.

The backup service is used for Student records including their admission records, academic details, student login records. The backup of the web activities is also maintained (which are being done using student login). Employee records including their employment details, qualifications, salary records, attendance (presence, absence, leaves (used, remaining), in and out timings).

Faculty records includes their qualification, faculty development programs attended/organized, research work (ongoing/published), e-learning material developed by them.

Administrative staff records are maintained to record their web activities (done using the staff login). IT Team also maintains their access records of Institute portals such as ERP and LMS.

The records of all the academic and non-academic activities which include the details of organizing committee, participants, advertising, pictures, videos, financial details is also maintained.

Guidelines

The purpose of these guidelines is to establish the rules for the backup of electronic information. These guidelines shall be followed by all individuals responsible for the installation and support of technology resources, individuals charged with technology resources security, and data owners.

4. IT Hardware Installation Policy

The life of any desktop, laptop, or peripheral at GLBIMR should be at least three years. Desktop computers, laptops, and peripherals should not be replaced until their minimum life has expired, unless the device encounters malfunctions which cannot be repaired. The Information Technology team is responsible for supervising the acquisition of desktop computers, laptops, and peripherals in the institute.

No academic or administrative staff member may obtain more than one computer. Devices whose guarantee periods have expired, will be assessed and maintained as needed after obtaining the approval of the System Administrator.

System Administrator assesses and prepares the reports and plans the replacement of devices annually, at the beginning of each academic year, in consultation with the Institute fraternity. Applications for replacements that are outside the ordinary replacement cycle are submitted to the System Administrator.

The replacement applications depend on the following criteria:

1. Expiry of guarantee period.
2. A new technology or a practical need that requires replacement.
3. New technologies or requirements for work.
4. Repeated malfunctions.
5. Budget availability.

The Manager, Information Technology evaluates and consults specialized sales agents to choose the best national/international brands and quality of model, price, and efficiency that are suitable for Institute.

The Manager, Information Technology supervises the purchase and distribution process for desktop computers, laptops, and peripherals.

All the desktop and laptop computers are equipped with a preloaded operating system in line with the needs of the institute, after being approved by the Manager of Information Technology.

E-waste management is done in accordance with the E- Waste (Management) Rules, 2016 (amendment, 2018) [Government of India], under which it is ensured by the authority that the electronic waste is delivered to authorized recyclers or dismantlers annually by BRP INFOTECH PVT. LTD. after complete documentation is done.

5 Software Installation and Licensing Policy

The purpose of this Policy is to underline the importance of compliance with software licensing provisions and to define specific responsibilities relating to this compliance.

The specific responsibilities are to:

- Maintain a register to provide proof of purchase of software.
- Maintaining an inventory detailing where licensed software is installed. This must track redeployment of software within the institute.

To ensure the continuous education of students, the Institute encourages the usage of

- Open-source software
- LMS complier
- Licensed software

6. IT Services helpdesk policy

IT Team provides a wide variety of technical support to students, faculty and staff to enhance learning through the use of technology.

Hours of Operation: IT support is available Monday to Saturday 9:00 AM – 5:00 PM (excluding holidays)

Campus Support Request

- Get Support via ERP

  User can lodge the complaint using the option available in the Institute's ERP system, by logging in using authorized ID and password, followed by the completed details of the issue/problem encountered. The complainant is advised to mention their correct contact information (especially mobile number).

- Get Support via Email

  User can email our helpdesk request to sumit.kumar@glbimr.org. Please include your name, email address (if different), phone number and a detailed description of the problem.

- Call Us

  If your email and Internet service is unavailable you can contact the reception help desk.

7. Network (Intranet & Internet) Use Policy

The Institute will take reasonable and appropriate steps to protect the information shared with it from unauthorized access or disclosure. The Institute strives to implement security measures that protect the loss, misuse, and alteration of data collected. The Institute maintains a computer security policy.

The System Administrator is responsible for ensuring the security of information maintained on computer systems in accordance with government guidelines. All information maintained on GLBIMR computers is considered the property of GLBIMR. Access to GLBIMR computer systems is restricted to authorized users only. Access to administrative applications is determined by the owners of the institutional data.

Authorized users are responsible for:

- Maintaining the security of their passwords.
- Ensuring that removable media containing sensitive or critical data are put into locking storage when not in use or maintained in areas that are locked when not in use;
- Backing up critical data maintained on their microcomputers' hard disks.
- Ensuring that only authorized software is loaded onto any Institute's computersystem. Authorized PC software packages are those developed, approved, or installed by the Office of Information Technology, or those obtained from reputable vendors who guarantee their products. The use of unauthorized PC software and programs (software obtained from unauthorized computer bulletin boards, friends, other employees, etc.) is strictly forbidden.
- Protecting GLBIMR computers from viruses by using authorized virus protection software and scanning disks.
- Ensuring that software installed on GLBIMR computers is not copied illegally.
- Documenting sensitive or critical PC applications developed for institute use andused to perform GLBIMR business.
- Maintaining the confidentiality of all records as required by applicable Institute policy, central and state law.
- Any workstation (terminal, personal computer, etc.) that is left unattended for longer than fifteen minutes is to be protected from unauthorized access by either.
- Using a screen saver with password protection to prevent access, or logging off from all computer systems. When using a password-protected screen saver, this password is to be known only to the individual who is responsible for that workstation.

Security Arrangements:

The Institute's intranet has been secured by using the Firewall – Sophos – XG430.

Sophos's product range offers network security (Firewall and UTM appliances), Sophos network security appliances include multiple features like Firewall – VPN (SSL VPN & IPsec), Gateway Anti-Virus, Anti-Spyware & Anti-Spam, Intrusion Prevention System (IPS), Content & Application Filtering, Web Application Firewall, Application Visibility & Control, Bandwidth Management, Multiple Link Management for Load Balancing and Gateway Failover, over a single platform.

To access the intranet facility, each member of the Institute – student, research scholar, faculty and staff has been provided with a unique login ID and password, this ensures the network security from the premises outside of the Institute.

8. Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculties, staff and students, and the Institute's administrators, it is recommended to utilize the Institute's e-mail services, for formal Institute communication and for academic & other official purposes.

E-mail for formal communications will facilitate the delivery of messages and documents to campus and extended communities or to distinct user groups and individuals. Formal Institute communications are official notices from the Institute to faculty, staff, students and vice-versa. These communications may include administrative content, such as human resources information, policy messages, general Institute messages, official announcements, etc.

To receive these notices, it is essential that the e-mail address be kept active by using it regularly. To use this facility faculty, staff, and students must log-in on Gmail based domain with their Institute's email id and password. For obtaining the Institute's user email id, user is to contact Registrar office/data center by submitting an application in a prescribed Performa.

Users may be aware that by using the email facility, the users are agreeing to abide by the following policies:

- The facility should be used primarily for academic and official purposes and to a limited extent for personal purposes.
- Using the facility for illegal/commercial purposes is a direct violation of the Institute's IT policy and may entail withdrawal of the facility. The illegal useincludes, 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.
- While sending large attachments to others, user should make sure that the recipient has email facility that allows him to receive such large attachments.
- User should keep the mail box used space within about 80% usage threshold, as 'mail box full' or 'mailbox all most full' situation will result in bouncing of the mails, especially when the incoming mail contains large attachments.
- User should not open any mail or attachment that is from unknown and suspicious source. Even if it is from known source, and if it contains any attachment that is of suspicious nature or looks dubious, user should get confirmation from the sender about its authenticity before opening it. This is very much essential from the point of security of the user's computer; as such messages may contain viruses that have

potential to damage the valuable information on your computer.

- Users should configure messaging software (Outlook Express/Netscape messaging client etc.,) on the computer that they use on permanent basis, so that periodically they can download the mails in the mailbox on to their computer thereby releasing the disk space on the server. It is user's responsibility to keep a backup of the incoming and outgoing mails of their account.
- User should not share his/her email account with others, as the individual account holder is personally held accountable, in case of any misuse of that email account.
- User should refrain from intercepting, or trying to break into others email accounts, as it is infringing the privacy of other users.
- While using the computers that are shared by other users as well, any email account that was accidentally left open by another user, should be promptly closed without peeping into its contents, by the user who has occupied that computer for its use.

Impersonating email account of others will be taken as a serious offence under the Institute IT security policy. It is ultimately each individual's responsibility to keep their e-mail account free from violations of Institute's email usage policy.

The above laid down policies are broadly applicable even to the email services that are provided by other sources such as Hotmail.com, Yahoo.com etc., as long as they are being used from the Institute's campus network, or by using the resources provided by theInstitute to the individual for official use even from outside.

9. Website Hosting Policy

GLBIMR Official Page

Institute and Associations of Teachers/Employees/Students may have pages on GLBIMR Intranet Channel of the official Web page. Official Web pages must follow the Institute Website Creation Guidelines for Website hosting. As on date, the Institute's webmaster is responsible for maintaining the official web site of the Institute viz., http://www.glbimr.org only.

10. Institute Database Use Policy

This Policy relates to the databases maintained by the Institute administration under the Institute's E-Governance.

Data is a vital and important Institute resource for providing useful information. Its use must be protected even when the data may not be confidential. GLBIMR has its own policies regarding the creation of database and access to information and a more generic policy on data access. Combined, these policies outline the Institute's approach to both the access and use of this Institute resource.

Database Ownership: GLBIMR is the data owner of all the Institute's institutional data generated in the Institute.

Custodians of Data: Individual Sections generate portions of data that constitute Institute's database. They may have custodianship responsibilities for portions ofthat data.

ERP/LMS Components: For the purpose of E-Governance, ERP/LMS System of the Institute may broadly be divided into seven categories. These are:

- Employee information management system
- Students' information management system
- Financial information management system
- Asset information management system
- Project information monitoring system
- Library information management system
- Document management and information retrieval system
- Examination management information system
- Attendance management information system
- Student admission management system
- Student placement management system
- Alumni information management system

General policy guidelines and parameters for data users:

1. The Institute's data policies do not allow the distribution of data that is identifiable to a person outside the Institute.
2. Data from the Institute's Database including data collected by individual faculty and staff, is for internal Institute purposes only.
3. One's role and function define the data resources that will be needed to carry out one's official responsibilities/rights. Through its data access policies, the Institute makes information and data available based on those responsibilities/rights.
4. Data directly identifying a person and his/her personal information may not be distributed in any form to outside persons or agencies, including all government agencies and surveys and other requests for data. All such requests are to be forwarded to the Office of the Institute Registrar.
5. Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the Institute should never respond to requests. All requests from law enforcement agencies are to be forwarded to the Office of the Institute Registrar for response.
6. At no time information, including that identified as 'Directory Information' be released to any outside entity for commercial, marketing, solicitation or other purposes. This includes organizations and companies which may be acting as agents for the Institute.
7. All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the Registrar of the Institute.
8. Database users who repackage data for others in their unit must inform the recipients of the above data access issues.
9. Tampering of the database by the individual user comes under violation of IT policy. Tampering includes, but not limited to:
    a. Modifying/deleting the data items or software components by using illegal access methods.
    b. Modifying/deleting the data items or software components deliberately with ulterior motives even by authorized individuals.
    c. Causing database or hardware or system software crash thereby destroying the whole of or part of database deliberately with ulterior motives by any individual.
    d. Trying to break security of the Database servers.

Such data tampering actions by Institute member or outside members will result in disciplinary action against the offender by the Institute authorities. If the matter involves illegal action, law enforcement agencies may become involved.

11. CCTV Surveillance Policy

The system comprises of fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; Public information signs.

Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.

Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV/IP Camera installation is in use.

Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

Purpose of the system

The system has been installed by Institute with the primary purpose of reducing the threat of crime generally, protecting institute premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.
- In the case of security staff to provide management information relating to employee compliance with contracts of employment

The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking.

Security Control Room Administration and Procedures

Details of the administrative procedures which apply to the Control Room will be set out in a Procedures Manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.

Images of identifiable living individuals are subject to the provisions of the Prevailing Data Protection Act; the Control Room Supervisor is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.

Staff

All staff working in the Security Control Room will be made aware of the sensitivity of handling CCTV/IP Camera images and recordings. The Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV/IP Camera.

Recording

Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time. Images will normally be retained for fifteen days from the date of recording, and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.

All hard drives and recorders shall remain the property of Institute until disposal and destruction.

Access to images

All access to images will be recorded in the Access Log as specified in the Procedures Manual. Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.

Access to images by a subject

CCTV/IP Camera digital images, if they show a recognizable person, are personal data and are covered by the Data Protection Act. Anyone who believes that they have been filmed by CCTV /IP Camera is entitled to ask for a copy of the data, subject to exemptions contained in the Act. They do not have the right of instant access.

Request to prevent processing

An individual has the right to request a prevention of processing where this is likely to cause

substantial and unwarranted damage or distress to that or another individual.

All such requests should be addressed in the first instance to the Security Control Room Supervisor or the Head Security Officer, who will provide a written response within 21 days of receiving the request setting out their decision on the request. A copy of the request and response will be retained.

Compliance monitoring

The contact point for members of Institute or members of the public wishing to enquire about the system will be the Control Room. Upon request enquirers will be provided with:

- A summary of this statement of policy
- An access request form if required or requested
- A subject access request form if required or requested
- A copy of the Institute central complaints procedures

All documented procedures will be kept under review and a report periodically made to the Estates Management Committee.

The effectiveness of the system in meeting its purposes will be kept under review and reports submitted as required to the Estates Management Committee.

12. Data Recovery in case of Disaster

Overview

In order to facilitate the recovery and restoration of Institute IT systems that support critical functioning of organization, units shall engage in disaster recovery planning efforts.

Disaster recovery planning is the ongoing process of developing, implementing, and testing disaster recovery management procedures and processes to ensure the efficient and effective resumption of critical functions in the event of an unscheduled interruption, irrespective of the source of the interruption.

Engaging in disaster recovery planning ensures that system dependencies have been identified and accounted for when developing the order of recovery, establishing recovery time, recovery point objectives, and documenting the roles of supporting personnel.

In addition, data backup is an integral component of disaster recovery planning. Data backup protects against the loss of data in the event of a physical disaster, database corruption, and error propagation in resilient systems, hardware or software failure, or other incident which may lead to the loss of data. The backup requirements found in this document will allow Institute business processes, teaching and learning activities and research projects to be resumed in a reasonable amount of time, based on criticality, with minimal loss of data.

Scope

This Disaster Recovery Standard applies to:

- Critical core IT infrastructure and other services which facilitate the transport, authentication and security of systems and data. Critical core infrastructure is defined as components which, when they experience degradation or failure, compromise all other services (e.g., data centers, identity and access management, network, firewall, DNS, Active Directory).

- Information technology systems that process or store mission critical data managed by, or on behalf of, the Institute, as determined by the unit that maintains the system; this specifically excludes desktop devices and workstations which do not require disaster recovery plans but may require data backup.
- The processes, policies and procedures related to preparing for recovery or continuation of technology infrastructure, systems and applications which are vital to an organization after a disaster or outage.

13 Power Backup policy for IT hardware

GLBIMR is having its power back up (generators) for enough back up energy. The generators turned on and all the protected electric loads seamlessly transferred to the backup power system.

For IT enabled essential applications are on UPS power supply. All academic blocks are having central UPS which are with redundancy. There is a separate UPS for Data Center. A substation is created which draw power from national grid and step down to 80 KVA. It is operational 24x7. Power supply will be guaranteed and generators start automatically.

14 Cyber Securities and Data Privacy

The Institute will take reasonable and appropriate steps to protect the information you share with us from unauthorized access or disclosure. The Institute strives to implement security measures that protect the loss, misuse, and alteration of data collected. The Institute maintains a computer security policy.

System Administrator is responsible for ensuring the security of information maintained on computer systems in accordance with State Agency guidelines. All information maintained on GLBIMR computers is considered the property of GLBIMR. Access to GLBIMR computer systems is restricted to authorized users only. Access to administrative applications is determined by the owners of the institutional data.

Authorized users of computing facilities are responsible for:

- Maintaining the security of their passwords;
- Ensuring that removable media containing sensitive or critical data are put into locking storage when not in use or maintained in areas that are locked when not in use;
- Backing up critical data maintained on their micro computers' hard disks;
- Ensuring that only authorized software is loaded onto all computer system.
- Protecting GLBIMR computers from viruses by using authorized virus protection software and scanning disks;
- Ensuring that software installed on GLBIMR computers is not copied illegally.
- Documenting sensitive or critical PC applications developed for institute use andused to perform GLBIMR business.
- Maintaining the confidentiality of all records as required by applicable Institute policy, federal, state and local law.
- Any workstation (terminal, personal computer, etc.) that is left unattended for longer than fifteen minutes is to be protected from unauthorized access by either:
- Using a screen saver with password protection to prevent access, or logging off from all computer systems. When using a password-protected screen saver, this password is to be known only to the individual who is responsible for that workstation.

15. Review and Revision Policy

GLBIMR has a provision for reviewing and revising this policy. For this the members of the GLBIMR fraternity mentioned below are the committee members who will meet annually at the beginning of each academic session for the aforesaid purpose. The committee members can make the changes based on:

- New and/or amended government laws/acts
- Addition or removal of the end-users
- Revised Institute's policies
- Need of the Institute infrastructure

The committee members will include

- Director
- Program Chairperson
- COE
- Registrar
- Program Office
- Manager, IT
- Student representatives

Authorized Signatory

Mr. Kuldeep Adhana
Registrar,
GLBIMR