GALGOTIAS UNIVERSITY
Uttar Pradesh
CREATING KNOWLEDGE

4.3.2
IT Infrastructure
# Information Technology (IT) Policy

Galgotias University

Plot No. 2, Yamuna Expressway,
Opposite, Buddha International Circuit,
Sector 17A, Greater Noida,
Uttar Pradesh 203201, India

Information Technology (IT) Policy

(Galgotias University)

INDEX

1. Introduction

Galgotias University (GU) IT policy exists to maintain, secure, and ensure legal and appropriate use of information technology infrastructure established by the University on the campus. This policy establishes University-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 University. 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. Galgotias University took initiative in 2011 and established basic network infrastructure in the academic complex of the university.

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 university’s academic environment.

University has about 5500 network connections covering four buildings across the campus. Internet Unit is the department that has been given the responsibility of running the university’s intranet & internet services.

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

GU is getting its Internet bandwidth from Airtel. Total bandwidth availability from Airtel source is 1.5GB Mbps (leased line) and a backup line of Tata of 450 MB/s. This leased line provided by Precious Netcom Pvt. Ltd.

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, departments and individuals who are part of university community to understand how University 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
- University 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 university IT Policy applies to

1. The technology administered by the university centrally or by the individual departments
2. The information services provided by the university administration, or by the individual departments, or by individuals of the university community, or by authorized resident or non-resident visitors on their own hardware connected to the university network.
3. The resources administered by the central administrative departments such as Library, Computer Centers, Laboratories, Offices of the university recognized Associations/Unions, or hostels and guest houses, or residences wherever the network facility was provided by the university.

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 university IT policy.

Further, all the faculty, students, staff, departments, authorized visitors/visiting faculty and others who may be granted permission to use the University's information technology infrastructure, must comply with the Guidelines. The violation of this IT policy by any university member may result in disciplinary action against the offender by the university 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 University
- 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

   University's desktop software is licensed under a central license agreement form Microsoft. 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 8,000 University desktop computers/laptops. Core support includes:

   - 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 University networks including the campus' mobile network and importantly its connection, which interconnects each other.
7. Servers

   Management of the University'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. These servers host main University systems, departmental systems, web sites, and student and staff network file space.

8. Telecommunications

   IT Services are responsible for the management of the University's Telephone systems, which includes all cordless handsets, desk sets and mobile phones. Security Maintaining IT Security and virus protection and providing advice and guidance.

9. Developing and maintaining Standard and specialist software 'images' for staff desktops, open access areas and IT teaching lab. IT Services also maintains a University wide printer strategy including deployment of MFP & Scanner.

10. Day to day operation of existing systems

    a. Support: Maintaining a wide range of the Universities 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 University Integration Developing and managing the integration points between existing systems

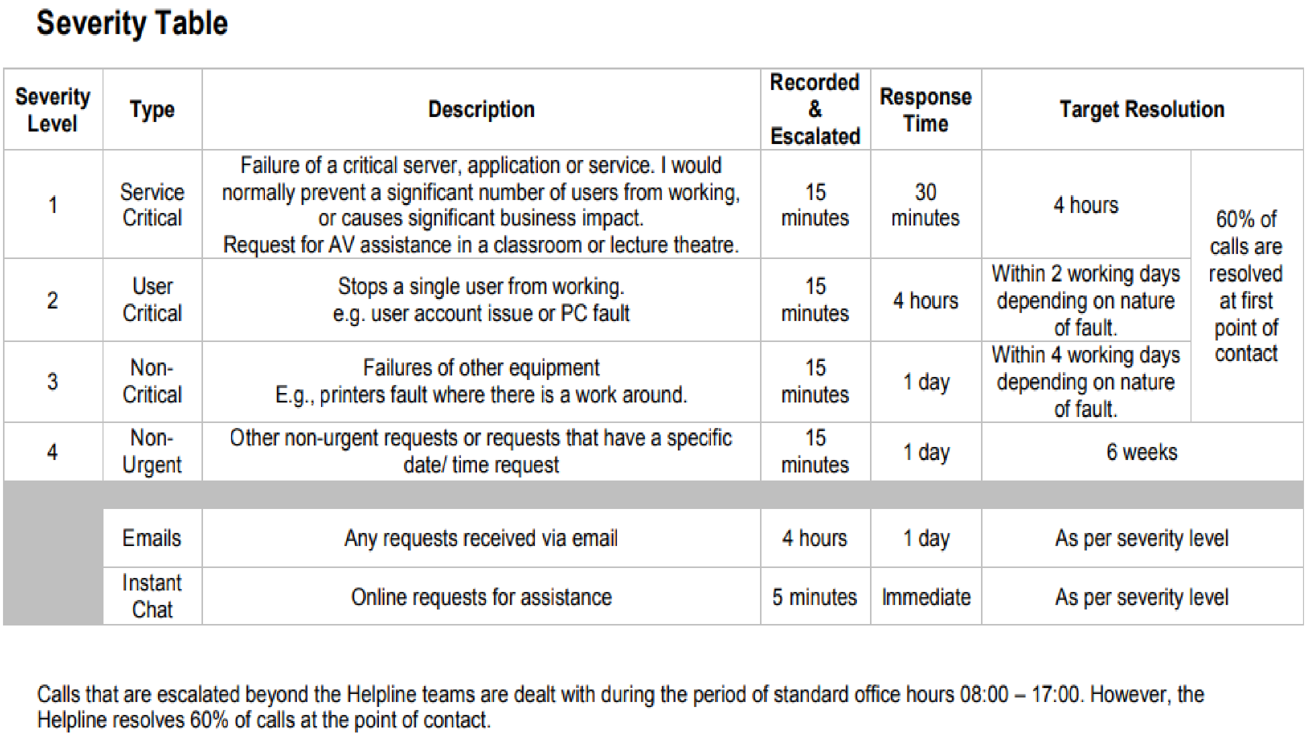
11. Operational Services

    a. IT Helpline & Problem Resolution
    b. New Username & Password: for Access the University 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 and partner Universities 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. When a problem arises, we will deal with it based on an initial assessment using severity table.



Severity Table

Severity Level	Type	Description	Recorded & Escalated	Response Time	Target Resolution	
1	Service Critical	Failure of a critical server, application or service. I would normally prevent a significant number of users from working, or causes significant business impact. Request for AV assistance in a classroom or lecture theatre.	15 minutes	30 minutes	4 hours	60% of calls are resolved at first point of contact
2	User Critical	Stops a single user from working. e.g. user account issue or PC fault	15 minutes	4 hours	Within 2 working days depending on nature of fault.	
3	Non-Critical	Failures of other equipment E.g., printers fault where there is a work around.	15 minutes	1 day	Within 4 working days depending on nature of fault.	
4	Non-Urgent	Other non-urgent requests or requests that have a specific date/ time request	15 minutes	1 day	6 weeks	
	Emails	Any requests received via email	4 hours	1 day	As per severity level	
	Instant Chat	Online requests for assistance	5 minutes	Immediate	As per severity level	

Calls that are escalated beyond the Helpline teams are dealt with during the period of standard office hours 08:00 – 17:00. However, the Helpline resolves 60% of calls at the point of contact.

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 E Mail- *itsupport@galgotiasuniversity.edu.in*

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 GU'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.

Technology Used

Duplicate disk-based technology is currently used to back up the data of all university level systems. The backup solutions reside in the secondary and tertiary backup data centers. The primary backup is done using cloud. At pre-defined time intervals as specified in a backup plan, a backup of the live data will be performed to our storage located in the primary data center. This data represents a point in time and is considered backup data.

For most non-critical systems, backup data and the live data constitute the two locations. Data deemed as mission critical may be replicated between locations using our Storage Area Network (SAN) technology. This guarantees that the data resides in at least two locations in a live production mode as well as at the second location as point-in-time backup data.

For mission-critical data that requires a higher level of protection, data is replicated to the tertiary backup data centers. The use of a replicated data solution is limited to select university mission critical systems, typically defined as Disaster Level Zero (DR0).

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 in datacenter using NAS - IOMEGA 16TB (4X4).

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. These records are maintained under both the department and school categories.

Administrative staff records are maintained to record their web activities (done using the staff login). IT Team also maintains their access records of university portals such as RF campus, LMS, INPODS.

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.

Responsibilities

Technology resources and data owners are required to keep the Infrastructure Operations Security (IOS) organization advised as changes are necessary. Technology resources and data owners are responsible for data backup validation and testing recovery. IT Department will NOT be responsible for corrupt or incomplete data backups.

4. IT Hardware Installation Policy

The life of any desktop, laptop, or peripheral at Galgotias University 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 departments.

No academic or administrative staff member may obtain more than one computer (either desktop or laptop). Devices whose guarantee periods have expired, will be assessed and maintained as needed after obtaining the approval of the IT Manager.

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

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 university.

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 different colleges and departments, after being approved by the Manager of Information Technology.

The process of replacement and distribution of the devices should be documented.

1. Through repulsion slip.
2. Slip will be verified by the concern dean or HOD.
3. Old and defective material should be returned.

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 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.

Responsibility for ensuring software license compliance rests with the Head of Department.

The specific responsibilities are to:

- Maintain a register to provide proof of purchase of software.
- Maintaining a register of disposal of software through on-sale (for example software sold with a computer).
- Maintaining an inventory detailing where licensed software is installed. This must track redeployment of software within the department.

In the interests of ensuring compliance with licensing requirements, IT Department from time to time investigates a software compliance audit.

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

- Open-source software
- Virtual labs for conduction of practical
- LMS complier
- Licensed software
- Coursera for online certifications

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 Sunday 9:00 AM – 6:00 PM (excluding holidays)

Campus Support Request

- Get Support via ERP

  User can lodge the complaint using the option available in the university'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 itsupport@galgotiasuniversity.edu.in. 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 IT help desk at 0120-4806842.

- Visit Data center

  You can visit to datacenter to lodge the complaint manually.

7. Network (Intranet & Internet) Use Policy

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

The IT Manager is responsible for ensuring the security of information maintained on computer systems in accordance with government guidelines. All information maintained on Galgotias University computers is considered the property of GU. Access to GU 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 university’s computer system. 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 GU computers from viruses by using authorized virus protection software and scanning disks.
- Ensuring that software installed on GU computers is not copied illegally.
- Documenting sensitive or critical PC applications developed for departmental use and used to perform GU business.
- Maintaining the confidentiality of all records as required by applicable University 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 university’s intranet has been secured by using the Firewall – Cyberoam – CR2500ING-XP.

Cyberoam’s product range offers network security (Firewall and UTM appliances), Cyberoam 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 university – 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 university.

8. Email Account Use Policy

In an effort to increase the efficient distribution of critical information to all faculties, staff and students, and the University's administrators, it is recommended to utilize the university's e-mail services, for formal University 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 University communications are official notices from the University to faculty, staff, students and vice-versa. These communications may include administrative content, such as human resources information, policy messages, general University 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 university's email id and password. For obtaining the university'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 university's IT policy and may entail withdrawal of the facility. The illegal use includes, but is not limited to, the unlicensed and illegal copying or distribution of software, sending of unsolicited bulk e-mail messages and generation of threatening, harassing, abusive, obscene or fraudulent messages/images.
- 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 university IT security policy. It is ultimately each individual's responsibility to keep their e-mail account free from violations of university's email usage policy.

Any Spam mail received by the user into INBOX should be forwarded to

itsupport@galgotiasuniversity.edu.in

Any mail wrongly stamped as SPAM mail should be forwarded to

itsupport@galgotiasuniversity.edu.in

All the mails detected as spam mails go into SPAM_MAIL folder of the respective users' mail accounts. Users are requested to open these folders periodically to check any important mail wrongly stamped as SPAM mail and went into this folder. If so, user may forward that mail ID to itsupport@galgotiasuniversity.edu.in for necessary action to delete from the spam mail category. It is recommended to empty this folder as frequently as possible.

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 university's campus network, or by using the resources provided by the university to the individual for official use even from outside.

9. Website Hosting Policy

Galgotias University Official Pages

Schools, departments, and Associations of Teachers/Employees/Students may have pages on Galgotias University Intranet Channel of the official Web page. Official Web pages must follow the University Website Creation Guidelines for Website hosting. As on date, the university's webmaster is responsible for maintaining the official web site of the university viz., http://www.galgotiasuniversity.edu.in only.

Affiliated Pages:

Faculty may host Web pages for "affiliated" professional organizations on department Web servers as long as adequate support and resources are available. Prior approval from the competent administrative authority must be obtained for hosting such pages. Individual units reserve the right to discontinue the service and will provide reasonable advance notice to that affiliated organization.

Web Pages for eLearning

This Policy relates to requirements for Web pages for eLearning authored as a result of Teaching/Learning process.

Faculty may have class materials (syllabi, course materials, resource materials, etc.) on the Web, linked through the appropriate department's pages.

10. University Database Use Policy

This Policy relates to the databases maintained by the university administration under the university’s E-Governance.

Data is a vital and important University resource for providing useful information. Its use must be protected even when the data may not be confidential. GU 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 university's approach to both the access and use of this university resource.

Database Ownership: Galgotias University is the data owner of all the University's institutional data generated in the university.

Custodians of Data: Individual Sections or departments generate portions of data that constitute University’s database. They may have custodianship responsibilities for portions of that data.

Data Administrators: Data administration activities outlined may be delegated to some of the officers in that department by the data Custodian.

ERP Components: For the purpose of E-Governance, ERP System of the university 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 schools, departments and administrative unit data users:

1. The university's data policies do not allow the distribution of data that is identifiable to a person outside the university.
2. Data from the University’s Database including data collected by departments or individual faculty and staff, is for internal university 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 university 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 University Registrar.
5. Requests for information from any courts, attorneys, etc. are handled by the Registrar Office of the University and departments should never respond to requests. All requests from law enforcement agencies are to be forwarded to the Office of the University 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 university or its departments.
7. All reports for UGC, MHRD and other government agencies will be prepared/compiled and submitted by the Registrar of the University.
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 department or 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/ departments.
    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 university member or outside members will result in disciplinary action against the offender by the university 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; SAN/NAS Storage; 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 university with the primary purpose of reducing the threat of crime generally, protecting universities 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.

Covert recording

Covert cameras may be used under the following circumstances on the written authorization or request of the senior officer, Registrar and where it has been assessed by the Head of Security and Facilities Services and the Data Protection Officer

- That informing the individual(s) concerned that recording was taking place would seriously prejudice the objective of making the recording; and
- That there is reasonable cause to suspect that unauthorized or illegal activity is taking place or is about to take place.

Any such covert processing will only be carried out for a limited and reasonable period of time consistent with the objectives of making the recording and will only relate to the specific suspected unauthorized activity.

The decision to adopt covert recording will be fully documented and will set out how the decision to use covert recording was reached and by whom.

The Security Control Room

Images captured by the system will be monitored and recorded in the Security Control Room, "the control room", twenty-four hours a day throughout the whole year. Monitors are not visible from outside the control room.

No unauthorized access to the Control Room will be permitted at any time. Access will be strictly limited to the duty controllers, authorized members of senior management, police officers and any other person with statutory powers of entry.

Staff, students and visitors may be granted access to the Control Room on a case-by-case basis and only then on written authorization from the Registrar. In an emergency and where it is not reasonably practicable to secure prior authorization, access may be granted to persons with a legitimate reason to enter the Control Room.

Before allowing access to the Control Room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorization. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organization they represent, the person who granted authorization and the times of entry to and exit from the center. A similar log will be kept of the staff on duty in the Security Control Room and any visitors granted emergency access.

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 university 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 third parties

Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:

- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.

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.

A person whose image has been recorded and retained and who wishes access to the data must apply in writing to the Head Security Officer. Subject Access Request Forms are obtainable from the Security Office, between the hours of 1020 and 1400 and 1430 to 1800 Monday to Friday, except when university is officially closed or from the Head Security Officer, the Records Office during the same hours.

The Head Security Officer will then arrange for a copy of the data to be made and given to the applicant. The applicant must not ask another member of staff to show them the data, or ask anyone else for a copy of the data. All communications must go through the university Head Security Officer. A response will be provided promptly and in any event within forty days of receiving the required fee and information.

The Data Protection Act gives the Head Security Officer the right to refuse a request for a copy of the data particularly where such access could prejudice the prevention or detection of crime or the apprehension or prosecution of offenders.

All such requests will be referred to the Security Control room Supervisor or by the Head Security Officer.

If it is decided that a data subject access request is to be refused, the reasons will be fully documented and the data subject informed in writing, stating the reasons.

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.

Complaints

It is recognized that members of University and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the Security Control Room supervisor. If having exhausted the steps set out, the complaint remains unresolved; the complainant may invoke Universities Centralized Complaints Procedure by obtaining and completing a University Complaints Form and a copy of the procedure. Complaints forms may be obtained from the Security Office, and the Registrar's Office. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Head Security Officer; these rights do not alter the existing rights of members of University or others under any relevant grievance or disciplinary procedures.

Compliance monitoring

The contact point for members of University or members of the public wishing to enquire about the system will be the Security Office which will be available during the hours of 1020 and 1400 and 1430 to 1800 Monday to Friday, except when University is officially closed. 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 University 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 University 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 university 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 University, 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.

Roles and Responsibilities

- Information Assurance (IA)
    - Maintains and publishes UNIVERSITY disaster recovery planning templates and processes.
    - Units or research projects that maintain information technology systems (system or business owner)
    - Identify mission critical systems.
    - Maintain adequate infrastructure resiliency and data backup and restoration processes for mission critical data and the IT systems assigned to them.
    - Develop, implement, document, maintain, and test disaster recovery plans.
    - Update the status of their DR planning to IA every two years.
- Unit IT Leader and/or Security Unit Liaison
    - Coordinate unit activities to satisfactorily implement or complete above unit responsibilities.
    - Work with unit IT to review unit DR plans at least annually or whenever significant system architecture or personnel changes occur.
    - Brief unit leadership on status of DR efforts and resources needs.
    - University Unit or Executive Leadership (Deans, Directors, University Office of Research)

We ensure that sufficient financial, personnel, and other resources are available as needed for the successful creation and ongoing maintenance of unit DR plans.

Definitions

Mission Critical: Mission critical IT systems and applications provide essential IT functions and access to data and whose unavailability will have an immediate and significant detrimental effect on the University and campus units if the system fails or is interrupted. A system or application may be designated mission critical if it meets one or more of the following conditions:

- Risk to human and research.
- Significant impact on the University’s research, learning and teaching, and administrative working.
- Significant legal, regulatory or financial costs.
- Serious impediment to a campus unit carrying out its critical business functions within the first 48 hours following an event (48 hours Recovery Time Objective – RTO).

- Loss of access to data with defined availability requirements.
- Loss of particular systems or applications may be originally assessed as not mission-critical, but may become more critical after an extended period of unavailability.

Critical Business Functions: Critical operational and/or business support functions that cannot be interrupted or unavailable for more than a mandated or predetermined timeframe without significantly jeopardizing UNIVERSITY operations.

Recovery Time Objective (RTO): The duration of time within which a business process must be restored and a stated service level achieved following a disruption in order to avoid unacceptable consequences associated with a break in service.

Recovery Point Objective (RPO): The maximum tolerable period in which data might be lost from an IT system or service due to a major incident. RTO and RPO timeframes for each criticality level are listed in Table 1 below.

Disaster Recovery Planning: The process, 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.

Business Continuity Planning: Business continuity planning, as opposed to disaster recovery planning, is the process of developing detailed plans, processes, and strategies that will enable an organization to respond to an event in such a manner that critical business functions can continue within planned levels of disruption and fully recover as quickly as possible.

Standard

The following are the core components required of all information technology disaster plans:

Critical Systems: All units and research programs that maintain critical information technology systems will develop, implement, and regularly test (exercise) disaster recovery plans for those systems;

Disaster Recovery Plan Template: Disaster recovery plans should follow the general content and guidelines.

Disaster Recovery Review/Plan Testing: Disaster recovery plans must be reviewed annually and updated whenever a significant change to system architecture, system dependencies or recovery personnel occurs, At a minimum, an annual tabletop exercise or equivalent should be conducted that simulates the abrupt and unscheduled loss of critical functions.

New System Evaluation: New applications or systems will be evaluated; systems determined to be critical require a disaster recovery plan to be documented and tested prior to go-live;

Risk Assessment: Environments designated as mission critical must have a performed at least every four years or in accordance with the regulatory requirements of the system. Disaster recovery plans need to include mitigation of potential negative impacts to the mission critical system.

Data Backup: Backups are the result of copying or archiving files for the purpose of restoring them to a specific point-in-time or in the event of data loss resulting from computer viruses, hardware failures, file corruption, accidental or intentional destruction, etc. Backups preserve data integrity in the event of data corruption or other loss of the primary copy.

Data Backup Requirements

Data backup and restoration should include a documented process for recovery, accounting for data dependencies or relationships where data from multiple systems must be in sync or share common data elements. The method and media for data backups should allow meeting RTO and RPO requirements for restoration.

In addition to system criticality requirements, data backups are:

- *Required*, for all mission critical systems and for any system or machine that creates, processes, maintains, or stores data classified as Restricted or High.
- *Recommended,* for Moderate data, and for data that cannot be recreated in a timeframe satisfactory to the owner.
- *Optional,* for all other systems or data.

System resiliency is a desirable objective, but is not a substitute for, and does not negate the necessity to perform, data backups and have a disaster recovery plan.

The following table should be used to determine disaster recovery and backup requirements for systems or machines that create, process, maintain, or store Restricted, High, or Moderate data and for mission critical systems irrespective of data classification. Where data can be classified into more than one of the categories listed below or RTO classification/criticality level), the classification with the most stringent data backup requirements must be met.

Data Classification	**Data Backup**	**Data Backup Encryption**	**Disaster Recovery Plan Requirements**
Restricted	Required	Required – At rest/in transit	Dependent on Recovery Time Classification
High	Required	Required – At rest/in transit	Dependent on Recovery Time Classification
Moderate	Required	Recommended	Dependent on Recovery Time Classification
Low	Recommended	Optional	Dependent on Recovery Time Classification

Violations and Sanctions

Violations of this policy by faculty may result in appropriate sanction or disciplinary action consistent with applicable University procedures. If dismissal or demotion of qualified faculty is proposed, the matter will be addressed in accordance with the procedures set forth in. In addition to disciplinary actions, individuals may be personally subject to criminal or civil prosecution and sanctions if they engage in unlawful behavior related to applicable federal and state laws.

Any department or unit found to have violated this Standard may be held accountable for the financial penalties, legal fees, and other remediation costs associated with a resulting information security incident and other regulatory non-compliance.

Implementation

Information Assurance is responsible for the implementation, maintenance and interpretation of this Standard.

13 Power Backup policy for IT hardware

Galgotias University is having its power back up (generators) unit rated 1500 KVA (three of 500 KVA) for enough back up energy around 10 hours for entire load. 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 40 KVA. It is operational 24x7. Power supply will be guaranteed and generators start automatically.

14 Cyber Securities and Data Privacy

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

IT Manager is responsible for ensuring the security of information maintained on computer systems in accordance with State Agency guidelines. All information maintained on Galgotias University computers is considered the property of GU. Access to GU 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 any UMGC computer system.
- Protecting GU computers from viruses by using authorized virus protection software and scanning disks;
- Ensuring that software installed on GU computers is not copied illegally;
- Documenting sensitive or critical PC applications developed for departmental use and used to perform GU business;
- Maintaining the confidentiality of all records as required by applicable University 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

GU has a provision for reviewing and revising this policy. For this the members of the GU 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 university’s policies
- Need of the university infrastructure

The committee members will include

- Vice-Chancellor
- CEO
- Registrar
- Chief Proctor
- Deans
- Manager, IT
- Head of Security
- Student representatives (five – 2 from Masters, 3 from Bachelors)

Authorized Signatory

Dr. Nitin Kumar Gaur
Registrar,
Galgotias University