Mahatma Gandhi University
Priyadarsini Hills P. O.
Kottayam, Kerala - 686560

(Re-accredited by NAAC with A Grade)

IT /e-governance Policies & Guidelines

IT /e-governance Policies & Guidelines

Introduction

Scope

Applies to:

This Policy applies to everyone who accesses University Information Technology Resources, whether affiliated with the University or not, whether on campus or from remote locations, including but not limited to Students (UG, PG, Research), Employees (Permanent/ Temporary/ Contractual), Faculty, Administrative Staff (Non-Technical / Technical), Higher Authorities and Officers, Guests, and volunteers. By accessing any of the University's Information Technology Resources (ITRs), the user agrees to comply with this Policy.

RACI (Responsible, Accountable, Consulted, and Informed) Matrix

Policy	IT Committee	IT Cell	Users
IT Policy	RAC	RA	I

Terms and Definitions

- University: The Mahatma Gandhi University, Kottayam
- IT Committee: The body that governs all IT related operations in the University
- ITR: Information Technology Resources
- IT Cell: Implementing agency of the IT Committee
- Users: University Students, research scholars, Teaching and non-teaching Staff
- University Information/Data: This includes information disclosed by University, any means (hardcopy, softcopy or verbal) which includes Accounting information, Student information, University records, Exam informations, Software, programme codes, Service information, Procedures or operation related information, purchase informations, stock information, certificates informations, fees information, marketing and sales information, property rights and patent information, branding guidelines, logos and trademarks.

Change, Review and Update

This policy shall be reviewed once every year unless the IT Committee considers an earlier review necessary to ensure that the policy remains current. Changes of this policy shall be performed by the IT Cell and approved by the IT Committee. A change log shall be kept current and be updated as soon as any change has been made

Information Technology Resources (ITRs):

- Information Technology Resources (ITRs) includes, but are not limited to, the University-owned data transmission lines, LANs WANs, wireless networks, servers, Network Switches, internet connections, terminals, applications, and Desktops, Mini PCs, printers, communication devices.
- ITRs include those owned by the University and those used by the University under license or contract, including but not limited to Data recorded on all types of electronic media, papers, computer hardware, Hardiscs and external storage mediums, software,telephone systems.
- ITRs also includes, but is not limited to, Desktops, laptops, mobile phone, tablets, servers, wireless networks, data storage devices, cloud spaces and other devices not owned by the University but intentionally connected to the University-owned Information Technology Resources.

Need for an IT Policy

The University understands the importance of the role played by information technology in achieving the University's vision and missions. The University is also aware of how information Technology is involved in administrative and academic activities. As more information is used and shared in a digital format by students, faculty and staff, both within and outside the University, an increased effort must be made to protect the information and the technology resources that support it. Increased protection of our information and ITRs to assure the usability and availability of those Resources is the primary purpose of this Policy. The Policy also addresses privacy and usage of those who access University Information Technology Resources (ITR).

The University's Right to Access Files

All information stored on or transmitted through the University's ITRs, including but not limited to servers, computers, mobile devices, telephone systems and cloud-hosted services and storage is subject to the rules of University. This also includes rights to access data/information as and when required including the Policy on Access to Accounts and Information. The University also holds rights to access, preserve and review all information stored on or transmitted through the University's ITRs

Policies

General

- IT Policies shall be executed in such a manner that it supports academic freedom
- All members of the University community are expected to be honest, fair, timely and ethical in their dealings with ITRs

- Accountability for the University Resources and infrastructure: All members of the University community have responsibility to protect University ITRs and are accountable for their access to and use
- Personal Use and Privacy: The University recognizes that students, teaching staff and non-teaching staff will be honest in their uses of Information Technology Resources (ITR) provided by the University. However:
    - The University owns the Information Technology Resources (ITR) and shared it with the students, teaching staff and non-teaching staff only for the purpose of accomplishing University's academic missions
    - All users are bound to follow legal and ethical restrictions
    - All Information Technology Resources owned and maintained by the University is for the benefit of the academic community and not for personal or business benefits/communications of individuals
- Section or Departments within the University can maintain additional IT policies that are specific to their operations, provided the same must be consulted, verified and approved by the University IT Committee and the Internal Quality Assurance cell
- The University IT Committee shall implement appropriate controls to ensure compliance with this policy by their users. IT Cell shall be the primary Implementing Agency and shall provide necessary support in this regard
- All ITRs users of the University shall not install any network/security device on the network without consultation with the IT Cell
- All ITRs users of the university (Students, teaching and non-teaching staffs) are expected to uphold the University's goodwill and reputation in any activities related to use of ITRs within and outside the University
- The privilege of using University's ITRs is limited to the University campus community and may not be transferred or extended by members of this community to people or groups outside the University without authorization from the higher authorities and IT Cell
- If a student, teaching or non teaching staff of the University encounter or observe any gap/security breach/issue in the University ITRs the same must be reported immediately to the IT Cell without trying to fix the issue on their own
- Usage of any digital medium (like but not limited to www, email, social media, forms, polls) using the University'sITRs for fundraising unauthorized by the IT Committee, even when conducted on behalf of non-profit organizations, is strictly prohibited
- Standards will be followed to develop, deploy and maintain softwares

- Any software application that the University need to purchase/develop should be performed only with the approval from the IT Committee and should follow the Software Development Policy defined in this document
- Any section(s)/Center(s)/individual(s)/any other user group within the University developing/purchasing applications directly through a third party vendor should provide a weekly status update to the IT Committee. The respective Section officer/HOD/Director will be responsible for providing the update to the IT Committee and accountable for the risks and issues involved. The respective Section officer/HOD/Director should assign a person (preferably technical) to monitor and track the development/engineering activity and this person will be the point-of-contact for the IT Committee during the tenure of the project. The IT Committee, at any point (During or after the tenure of the project) can instruct to submit any project related documents (which includes but not limited to Architecture diagrams, Workflows, Status reports, test reports, project expense reports, timeline) to the Section/Center/individual and the respective Section Officer/HOD/Director will be accountable for sharing this information with IT Committee within 7 days from the day of request. Also, to host application so developed, on the University Server (Cloud/in-house) approval must be granted by the IT Committee
- Any expansion plan on the University's existing network infrastructure (WAN & LAN) should be as per the direction from the IT Cell - Network team, and approval from IT Committee

University's ITR's use is a Privilege

- Any students, teaching and non-teaching staff using the University ITR's should consider the service as a privilege and not a right
- No person/section will deliberately or wilfully cause damage to ITR's or assist another in doing the same
- Unacceptable use/activity may result in suspension or cancellation of privileges as well as additional disciplinary action and/or legal action. The University IT Committee will be the final authority to decide whether a student's/teaching or non-teaching staff's privileges should be denied or revoked.

Internet access Policy

- Only University Students/Teachers and nonteaching staff will have access to Internet through the University network
- Internet access will be allowed only to registered users
- University Email ID will be used for user authentication to grant access to Internet over University network

- Users signing in to the network using guest ID (provided by IT Cell) or personal ID (approved be respective department/section) will be monitored by IT Cell and connection will be terminated without any notice if any malicious activity is detected

Websites access Policy

- The University will restrict access to certain categories of website and will manage this by classifying websites into three categories:
    - Sites that are available at all times
    - Sites blocked during normal work hours, which is defined as between 10.00AM to 4.30PM Monday to Saturday. These are categories of sites that are very unlikely to have a legitimate work usage and include:
        - Auction sites
        - Dating sites
        - Game sites
        - News Channels
        - Social Media
        - E-commerce sites except sites used for University's Purchase department(s)
        - Proxy site links
        - Television Channel links
    - Sites that contain pornographic and/or objectionable material will be completely blocked as far as is practicable
- The IT Committee will determine the sites to be blocked/opened upon recommendation from the IT Cell.
- Any user who has a requirement to access blocked sites may submit a request to the IT Cell and decision will be taken after discussing the request in the IT Committee
- In case of an urgency a written approval from Registrar would be required and the site will be opened only for a specific time for a specific IP/person/group
- IT Cell will be responsible for managing the internet restrictions throughout the University.
- The respective Departments and sections are required to ensure that their internet access is inline to the Website Policy

Information Technology Management and Audit

- The University shall perform Software, hardware and manual audits to manage the information technology operations. As a result of these audits actions will be taken or suggestions will be submitted for approval to IT Committee

- The activities will include (but not limited to) spam/virus detection and elimination; limitation of network volume or block access to specific file types or sites; or restriction of access to sites that present a security risk to the University's systems or experience high volumes of network traffic unrelated to the academic missions of the University.
- To implement certain tasks, if approval is required, the suggestion will be submitted to the IT Committee and action will be planned and implemented based on the confirmation.

Non-University users or general public

University views the internet as a public right. However, the University will take measures to make sure that it's not misused.

- University networks and Internet services can be shared with the general public with very limited data transfer speed and for a short period of time
- The IT Committee will decide on the data transfer speed that can be offered to the general public. This can also change from person to person
- All guest users activity will be monitored by University network team and ITRs access will be denied and never revoked if any suspicious activity is identified
- No activity that is related to private financial gain, commercial, advertising or solicitation purposes are not entertained
- The University may collect personal information like Name, Phone number and email ID of non-university user(s) requesting/accessing University ITR's. The University ensures that such information is not used for financial gain.

Use of IT Devices Issued by the University

Any devices so includes, but is not limited to, Desktops, laptops, mobile phone, tablets, servers, wireless networks, data storage devices, cloud spaces and other electrical or electronic devices not only owned by the University but intentionally connected to the University-owned Information Technology Resources

- ITRs issued by the University to a user shall be primarily used for academic, research and any other University related purposes only and in a lawful and ethical way

Hardware Policy

University ITRs users needs to keep track of certain precautions while getting their computers or peripherals installed so that they may face minimum inconvenience due to interruption of services offered by the University due to hardware failures. Any device that the University owns as well as not owned but uses any of the University's ITR's service will be bound to follow the Hardware Policy of the University.

Primary User

- An individual who is the custodian of a University owned IT Asset or service will be considered as its Primary User
- If any ITRs that has multiple users, none of whom are or cannot be considered as "primary" user, the the respective section officer should make an arrangement and make a person responsible for compliance or the respective section officer will be considered as the “Primary” user

ID for ITR’s

- All ITR’s in the University campus will be managed and maintained by the IT Cell - Hardware wing
- There will be a naming convention for ITR’s and IT Cell will be managing this record
- A copy of IT asset register will be shared with the Purchase department, General Store and Audit section or any other section

Warranty & Annual Maintenance Contract

Any ITR’s purchased by any Section/Center/Project for the University should be preferably with a 3 year onsite comprehensive onsite warranty (including physical damage). The IT Cell will be taking necessary steps to take/renew an AMC (annual maintenance contract), after the existing warranty expires

Power Connection to Computers and Peripherals

All the computers and peripherals should be connected only to UPS points. All UPS points should ensure proper earthing and wiring. The Engineering department will be accountable for any issues caused to University ITR’s due to electrical interferences.

Network Connection

- All networking equipment connected to the university network must first be registered and approved by IT Cell of the University
- Any networked devices or services that degrade the quality of service on the network, will result in termination of network service to the respective device until the correction occurs
- Any activities, which interrupts the smooth operation of the University network, are prohibited. These include but are not limited to the propagation of computer worms, network sweeps, network probing, viruses, or Trojan horses
- Unauthorized Wireless Access Points (units that are not installed, maintained and managed by the University IT Cell) are prohibited in the University Campus

Cable

- While connecting University ITR’s like - but not limited to, Desktops, Laptops, printers, LAN Switches, the connecting network cable should be away from any electrical equipment, as they interfere with the network communication.
- Further, no other electrical/electronic equipment should be shared with the power supply from where the computer, Laptop and its peripherals are connected

Paper and Printing Resources

- Printer sharing facilities on the computer over the network should be installed only when it is absolutely required
- Unnecessary printing is wasteful in cost and conflicts with the University’s sustainability goals
- All students/teachers and non-teaching staff of the University community should practice thrifty and judicious printing. Try to ensure that editing take place online whenever possible rather than on a printed draft
- Information that can be shared effectively electronically should not be printed at all
- Anyone without proper authorization from the IT Cell found removing paper or toner cartridges from printers or copiers it will be considered a disciplinary matter

Shifting Computer from One Location to another

- Any ITR’s may be moved from one location to another within the university campus only after informing and getting approval from the IT Cell. The IT Cell will maintain record of ITR’s in each location and will have to modify these records when items are being shifted
- An ITR moved from one place to another may have changes in IP Address, Access privileges and ID. This will be managed by the IT Cell
- As and when any deviation (from the list maintained by IT Cell) is found for any ITRs, data connectivity, the respective device will be disabled by the IT Cell. And the respective Section officer and custodian of the ITR will be informed about the flaws either over Phone or email. Revoking the connectivity would require a written approval from the respective section officer and the end user should meet the compliance

Maintenance of Computer Systems provided by the University

For all the ITR’s purchased and distributed by the university, the IT Cell will attend the complaints related to any maintenance related problems.

Software Licensing and Updating Policy

- Any Desktop/Laptop/Mobile devices purchases made by the individual departments/projects should ensure that the systems have all licensed software (like but not limited to operating system, antivirus and necessary application software) installed

- The University’s IT policy does not allow any pirated/unauthorized software usage or installation on the university owned ITR or any ITRs connected to the University network
- Purchase of new Software or renewal of software licence will be only based on study and recommendations by the IT Cell and must be approved by the IT Committee
- Individual users should make sure that respective computer systems have their OS updated in respective of their service packs/patches, through the Internet. If the user is not able to be aware of how to do this activity the same must be reported to the IT Cell. IT Cell will provide guidance for the users
- University will always encourage its community to work on open source software/applications like Linux, Open office etc wherever possible there by promoting Open Source application usage
- All ITRs in the university should be protected with end-to-end protection or Antivirus as applicable. These protection apps should be active and updated as necessary
- IT Cell will maintain a record that can be subjected for review by IT Committee, to provide proof of purchase of software and renewal of licences
- All Students/teaching and non-teaching staff should ensure and be aware of their own responsibilities in regard to ensuring they only use software in compliance with licence conditions

Anti-virus

- Updated licenced anti-virus software is mandatory for all Desktops and Laptops operating on University’s network irrespective of whether its University’s ITR or user’s.
- Users and IT Cell team should ensure that the anti-virus installed on desktops, laptops and servers are updated as as wen the software prompts for an update
- Only desktops, laptops and servers where a significant negative impact would result from operating anti-virus software, or servers running an Operating System with low likelihood of virus infection such as Solaris or VMS, may be considered for exemption from this procedure. However, this should be verified and approved by the IT Cell. The custodian of the respective device will be responsible for any vulnerability caused by their device in the University’s server or network

Server Administration Policy

- The University will maintain servers in an ethical manner and ensure to:
    - to maintain intellectual property rights of the owners of material on the server

    - that the material on these servers are not subject to unauthorised access/modification/delete

- Full access to servers are not permitted for students/teaching an non-teaching staff except team (or individual) designated by the IT Cell and approved by the IT Committee
- For exceptional reasons if access to servers needs to be opened for an Individual/team, they must get a formal approval from the Registrar
- The authorized server administrators may need to inspect databases in the course of their administration duties, this does not entitle disclosure of any personal or confidential information
- The University may,disclose anything stored on its Servers, only if its approved by the IT Committee
- The authorized server administrator should ensure that all the servers are synchronize their times and log timestamps
- The authorized server administrator should keep a record of Sections/Departments/ Users within the University running email servers
- Departments or organisations within the University running Web servers should:
    - Register the existence of the web server with IT Cell
    - Admin access should be provided to the member designated by the IT Cell to periodically monitor the server

Data Centre

A data centre refers to a secure facility which houses computer systems and associated computer hardware, such as telecommunications and data storage systems. A data center is designed to handle high volumes of data and traffic with minimum latency.

University shall maintain Enterprise, Cloud and Edge Data Center based on the requirements

Enterprise: A fully University-owned data center used to process internal data and host mission-critical applications

Cloud: Using third-party cloud services (like AWS, Google, Azure etc), and setting up a virtual data center in the cloud

Edge Data Center: An individual server PC or a smaller data center that is as close to the end user as possible

Cloud Computing Policy

This policy applies to all users accessing and using 3rd party services capable of storing or transmitting protected or sensitive electronic data that are owned by the University.

The purpose of this policy is to ensure that the University data is not inappropriately stored or shared using public cloud and file sharing services. Cloud and file sharing, for this purpose, is defined as the utilization of servers or information technology hosting on a third party provider.

University may store data on the university managed cloud Instance (like but not limited to AWS, Google, Azure) provided access to these instances/storage is protected and data is secured

The University will consider the following contract terms to ensure a minimum level of information security protection wherever data sharing is applicable:

- Data transmission and encryption requirements
- Authentication and authorization mechanisms
- Intrusion detection and prevention mechanisms
- Logging and log review requirements
- Security scan and audit requirements
- Security training and awareness requirements

AWS (Amazon Web Services)

The following recommendations should be considered while using AWS

Control	Recommended Implementation
Additional AWS accounts if any must be provisioned as a child of the University account	Request should be submitted and approved by the IT Committee to create new AWS account under the University or to create a new instances in the University account
Administrative access to cloud resources should be granted only to one designated person from the University (and a designated person from the vendor whose profile details should be shared with the University and approved by the IT Committee) .	This user should be approved by the IT Committee and monitored by IT Cell. For those who have an urgent requirement, requests must be forwarded to IT Cell and approval should be taken from the Registrar. The access should be removed immediately upon a users' departure. Also, the admin access groups should be audited on a weekly basis.

User accounts with access to root privileges must have MFA (multi factor authentication) enabled.	
All data volumes and storage accounts must be tagged with approved data sensitivity classification (e.g. “Sensitive”, “Non-sensitive”)	Tag S3 objects and EBS volumes with a key such as “Classification” and value of “Public”, “Internal”, or “Legally/Contractually Restricted”.
All resources must be labeled with approved Project, Owner, and Environment tags.	Assign a “Project” tag to each resource with the name of the associated project. Assign an “Owner” tag (MGU) to each resource with the email address of the responsible party (email of the university network administrator) . Assign an “Environment” tag to each resource with a value of “Dev”, “Test”, “Staging”, or “Production”.
Compute instances must have a monitoring or management agent installed.	Use a monitoring tool for management and automation of instances.
Compute instances must not have a public network interface unless requested	Do not assign a public IP address to compute instances unless requested.
Storage accounts and volumes must not be configured to allow public access unless requested.	Block public access to all or selected S3 buckets at the account level, only permitting public access when requested.
Activity logging must be turned on for all resources and services.	Do not disable the NUIT_Support Cloud Trail trail that is created in your AWS account.

VM firewalls and network security groups should have only authorized ports open. Certain ports are only authorized to receive traffic from approved networks.	Use EC2 Security Groups to allow network access on specific ports from specific IP ranges.
User, network, and compute instance access privileges should follow the least-privilege principle.	Do not use the Admin role to access the account unless necessary. Use federated roles or roles assigned to your compute instances with IAM managed policies that provide access to only the services and actions required.
Resource diagnostics with logs and metrics should be enabled for all resources.	Enable alarms to be alerted of application incidents.
Elastic IP addresses, storage volumes, and other instance-related resources not associated with a running instance should be released or deleted.	Periodically audit your EBS volumes and Elastic IP address and remove unattached, unneeded resources.

University Data Centre Access Policy

University currently owns a Tier 1 Data Center. The plan is to uplift the infracture to Tier 3 gradually and ensure that any component can be taken out of service without affecting production.

- Access to the University data centres will be granted only to the following Units:
    - Unit 1
        - People within the IT Cell whose role and responsibilities include operating and maintaining the data centre and its hardwares
        - This list will be maintained by the Manager, Network and Infrastructure, IT Cell
        - Member(s) may access the data centre in an emergency
    - Unit 2
        - People who require access to the data centres to maintain or service specific equipment(s) in the data centre
        - Access for these people will be under strict supervision of Manager, Network and Infrastructure or a person designated by the Manager, and will be intimated to the higher authority

        - In an emergency, member(s) will gain access by contacting the security department who will provide access and stay for the duration and will ensure that the data centre is secured after the event
    - Unit 3
        - People who are interested in the data centres may request a guided tour unders the supervision of Manager, Network and Infrastructure or a person designated by the Manager
        - Such access will require approval by Manager, Network and Infrastructure and intimated to the higher authority
        - Access is granted only when visits will not interrupt any operations of the data centre
- A register should be maintained to log check-in and check-out time for all the Unit's people to the Data Centre along with ID/biometric access. The Manager, Network and Infrastructure, should review this register periodically and should be submitted for inspection to higher authorities on demand.
- Any planned access (outside normal hours) must be pre-approved by the Manager, Network and Infrastructure in writing and should be intimated to the higher authority

Electronic Information Policy

From time to time, members of the University, including students, may use electronic means to collect data related to University's official business or any academic activities. Data collected or transferred through these means should be considered confidential. At no time University owned data/information should be disclosed in ways that could directly expose personal information of individuals or affect University's values.

Electronic information is governed by the same laws and regulations of the University, as paper documents, including statutes protecting the privacy of student records, medical information, and other kinds of personal information etc.

Users/Sections/Departments who use cloud storage accounts for university work are responsible for ensuring that the University's information is not placed or stored in unapproved or inappropriate locations. If at all any such storage is required, an approval needs to be obtained from the IT Committee

Data protection policy

This policy ensures the University's obligation to ensure the protection of data

- Copying University's digital information information from one location to another for testing validating or for any other purposes requires documented authorization from the Registrar

- Non Disclosure Agreement (NDA) should be signed with third party services providers if they are involving in any activity that make use/transfer/have access to University ITR's or University Data

Information Retention and Disposal

- Users like but not limited to Students, Teaching and non-teaching staff are responsible for retaining their data and information that is of value to the University, whether for business processes, legal purposes, or historical value
- Retention of electronic records will be as per the University's Record Retention Policy
- All Students/teachers and non-teaching staff should refrain from unwarranted or excessive amounts of storage on central or departmental computing systems or any similar ITRs and servers

Official Email

- All students/teaching and non-teaching staff of the University with ready access to email are responsible for knowing the content of official correspondence sent to their University-provided email address
- Students, Teachers and non-teaching staff who have personal email accounts with services outside the University should use only their University-provided email accounts for communications regarding University matters. Using University email protects the privacy and security of University data; allows for verification of sending and receiving critical correspondence regarding academic and other matters; and facilitates responses to subpoenas and other situations that may require the retrieval, inspection, or production of documents including e-mail.
- All users who submit files via email should retain copies of the document until certain that the receiver has received a legible copy
- University account-holders who have their email copied or forwarded to an outside account must take care to avoid marking for their outside email provider any such copied or forwarded mail as spam
- University ITRs must not be used to transmit or receive malicious, harassing, or defamatory content
- Official email ID issued by the University to its Students/Teaching and non-teaching staffs should not be used for (but not limited to), creating and managing social media accounts, registering for free softwares/service, registering for trial version of software/service, e-commerce, communication outside the university unless its official, bill payments, registering for web enabled services without approval from the authority.

- Any email account(s) suspected to be misused will be suspended/terminated by the IT Cell and only be revoked after receiving approval from the authority
- Mass Mailings - mass electronic mailings are permitted only as authorized by the appropriate University offices

Transferring large files

- Transferring large movie or music files may overload the network and degrade services. Transferring large files can slow the network making it less responsive or even unavailable to users really in need.
- Transfer of large files needs to be done through a University shared storage. The same must be informed to the University IT Cell - Network Team

Password Policy

Passwords are used for various purposes at the University. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection and local switch logins. Since very few systems have support for one-time tokens, (i.e., dynamic passwords which are only used once), everyone should ensure selecting strong passwords and secure their accounts

- Do not use the same password for the University accounts as for non-University application access
- The "Remember Password" feature of applications/browsers should not be used
- Passwords should not be written down and stored them anywhere in your office/classroom/lab
- If an account or password is suspected to have been compromised, report the incident to the IT Cell
- If someone demands a password, refer them to this document or have him/her call the Network Administrator
- Don’ts:
  - Don't reveal a password in an email message.
  - Don't reveal a password to the boss.
  - Don't talk about a password in front of others.
  - Don't hint at the format of a password (e.g., "my family name")
  - Don't reveal a password on questionnaires or security forms.
  - Don't share a password with family members.
  - Don't reveal a password to co-workers/friends while on vacation.
  - Don’t reveal a password in chat

Use of the University’s Name and Logo

- No individual/department/companies/vendors/general public may use the Mahatma Gandhi University’s name, seal, logos, restricted images, or other identifiers that indicates Mahatma Gandhi University or University’s Department/Section, except to the extent such individual/section/department has been authorized by the Mahatma Gandhi University authorities
- Misuse of the University’s name or other marks by any unauthorized member of public or the University community will be considered as a serious offense

Allowing Access to Others

- If you the administer of a device like but not limited to server/router/switch/Shared Space or allow accounts or access privileges to others, whether user of the University community or people outside the University, on a device like but not limited to any networked device, system, server, router, you are responsible for protecting the University's property and good will from damages that can be caused by others to whom you might provided the access controls
- As the permission grantor you will be responsible for ensuring that no copyrighted material (including but not limited to any files, licences, learning materials, recordings, logos, circulations,software) is published on, or distributed from, that system without permission of the copyright holder

Use of University ITRs for personal gains or social media

- Students/Teaching and non-teaching staff of the University are prohibited from using University ITRs and digital resources for personal business purposes without consent from the authority
- University departments and groups that are authorized to conduct certain kinds of commerce should get approval from the authority and IT Cell. University holds the right to approve/reject any such applications without disclosing any reason
- User of University ITRs for ecommerce/online purchase is not entertained

Use of University ITRs for Campaigns or Surveys

- Appropriate authorization from authority and IT Cell must be obtained to conduct Web-based or e-mail surveys, whether among members of the campus community or of people outside the University using University ITRs
- The University will hold all right to pull out any such polls/campaigns/ advertisements/tage from University’s digital resource without any notice to the author/promoter/group of the campaign

Conflicts of Interest

A conflict of interest may arise in situations where the personal, academic or financial interests of a student/teaching or non-teaching staff is affected by the IT Policy or with the body maintaining the IT Policy

In such a situation:

- The respective person should inform (verbally and in writing) to their reporting officer
- The Reporting Officer will Inform the IT Cell. Action will be taken once the subject is discussed in the IT Committee.

Human Resource Security Standard

These standards needs to be ensured so that all users of the University ITRs are aware of, understand, and fulfill their responsibilities in regards to information security responsibilities and requirements for the University's ITR's that they access:

During their tenure with University:

1. Section/School Responsibilities: All Section/School should ensure that its users are aware of and fulfill their information security responsibilities as defined by the IT Policy
2. Security Awareness Training: Users can consult or seek help from the implementing agency - IT Cell, on security awareness education and training if required
3. Disciplinary Process: Users will be subjected to disciplinary actions if they are found not to comply with IT Policies

Termination

- IT Cell should be informed regarding a user's termination and no dues must be issued by the IT Cell after returning of assets
- All access to the University information resources which includes but not limited to network access, hardware access, email, data storage and software access should be revoked by the IT Cell upon full termination (day of termination) of employment/completion of course with the University
- All users should ensure that they share all University related information to their successor or reporting head

Public Information

Any data or information that is available to all members (student, teaching and non-teaching staff) of the University and that can be made available to the public. The University holds all the right to control the content and format of Public Information.

Software Development Policy

This Policy standardizes the software development procedures for all University-level centrally-managed web/desktop applications using best practices. Since these applications and services commonly deal with sensitive data, protecting this data is required. Standardizing the development approach and coding techniques for systems will ensure their maintainability, scalability, and security against cyber-attacks and accessibility.

RACI (Responsible, Accountable, Consulted, and Informed) Matrix

Policy	IT Committee	IT Cell	Users
Software Development	RAI	RAC	RA

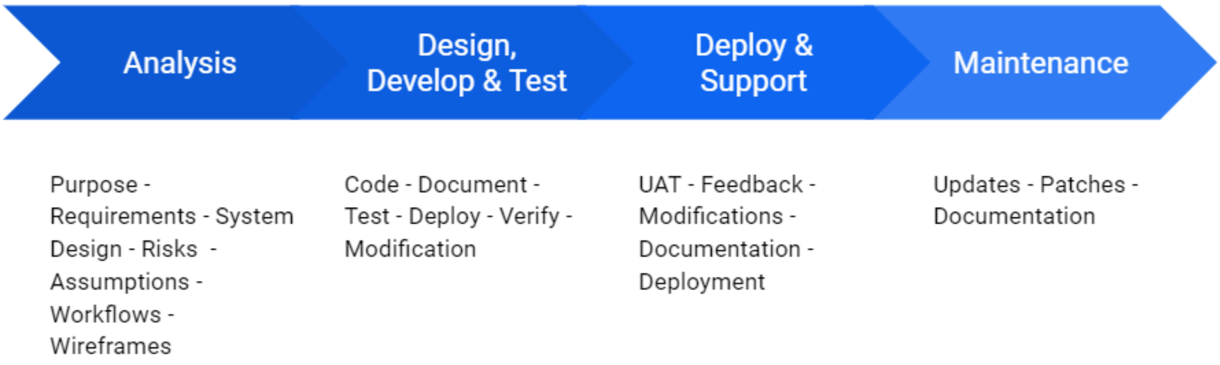
- The IT Cell will be responsible for developing, maintaining, and participating in a System Development Life Cycle ("SDLC") for University software projects
- All software developed in-house and through a third party service provider which runs on production systems must be developed according to the SDLC policy as defined in the SDLC Plan section in this document
- All software development projects, including maintenance projects, must follow these standards:
    - Software/feature requests should have a clear definition of purpose
    - Prepare Specifications/Requirements checklist:
        - Was thought given to the system administration
        - functionality?
        - Was thought given to error handling?
        - Does the specification clearly divide the project into phases?
        - Do all the phases have verifiable (and preferably undisputable) outcomes?
        - Does the document refer to any related documents as specifically as possible? (Document title, revision, page number)?
        - Is the maximum load (data and system usage) estimated?
        - Are the security requirements specified?
        - Are the operation and maintenance requirements specified
        - Are the education/training requirements specified?

        - Are the installation/migration requirements specified?
        - Has there been a peer-to-peer review (walkthrough)?
        - Has the application architect reviewed (walkthrough)?
        - Have the requirements/specifications been agreed by the user?
        - Have reporting requirements been clearly identified?
    - Simplicity of use: Application/features developed should be easy to use
    - Delivered on time and when needed
    - Reliability and Scalability
    - API enabled and Secure
    - Efficiency (fast enough for the purpose it was created)
    - Minimum development and running cost
    - Coding standards (like OWASP)
    - Development /Coding checklist
        - Does every input that comes from an untrusted source (i.e., typing into fields on a page, external systems) have associated error checking accounted for?
        - Are all forms of validation done on the server side? (only allow on the client side on an as needed basis)
        - Stored procedures used as the method for data validation/delivery
        - Number of temporary tables that would be needed
        - Any extra database reads/writes that would be required.
        - Does the code have the following:
            - Proper naming convention
            - Purpose is documented
            - Brief description
            - Original author and date are identified
            - Change control area showing date of change, reason, person who did it and associated project or ticket number
            - Sample execute
            - Unit test documented and repeatable

        - Sufficient commenting exists throughout the code to make it readable and understandable (i.e., maintainable) and the comments match the actual code.
    - Clear, accurate and detailed user manual documentation, technical documentation, test approach documentation and test reports
    - Go Live: Ensure the project team and primary user are aware and accept the implementation plan
    - Should have a Post Implementation period: Resources should be assigned to the project, typically with a lower percentage of time, and available to make adjustments if issues arise
- The SDLC Policy should address the areas of preliminary analysis or feasibility study, risk identification and mitigation, systems analysis, development, quality assurance and acceptance testing, implementation, maintenance and review
- There should be a separation between the production, development and test environments. This will ensure that security is maintained for the production system, while the development and test environments can maximize productivity with fewer security restrictions
- Development and test staff must not be permitted to have access to production systems. If at all access is required, the requested must be verified by the IT Cell and approved by the Registrar

SDLC Plan

This SDLC framework is a basic framework. The model is subjected to change as part of continuous process improvement.


Analysis

Purpose - Requirements - System Design - Risks - Assumptions - Workflows - Wireframes

Design, Develop & Test

Code - Document - Test - Deploy - Verify - Modification

Deploy & Support

UAT - Feedback - Modifications - Documentation - Deployment

Maintenance

Updates - Patches - Documentation

Noncompliance

- *University Students, teaching/non-teaching staff not complying with these policies may leave themselves and others at risk which could result in damaged or lost data, wrong data etc. Also any individual's noncompliant ITRs can affect other individuals,* *groups, departments, or even the entire university. Hence it is critical to bring all ITR's into compliance as soon as they are recognized not to be.*

- *If the IT Cell identifies a non-compliant resource, the team will notify the custodian and Section Head and will ask that it be brought into compliance. Such notification will be sent over emails*
- *The department/section/individual personally will be responsible for any noncompliance activity*
- *Noncompliance activities may result in suspension or cancellation of privileges as well as additional disciplinary action and/or legal action. The University IT Committee will be the final authority to decide whether a student's/teaching or non-teaching staff's privileges should be denied or revoked.*