Regulations for Information Technology (IT)

Resolution No. 29.5 of the 29th Board of Governors Meeting held on 12/11/2025

November 2025

Regulations for Information Technology (IT)

Policy

Presidency University believes in and shall continue to promote the extensive use of Information Technology [IT] in all its academic and administrative operations across, its Campuses. To ensure the effective use and application of IT, Presidency University shall equip all its Departments and Centres, across campuses, with the necessary hardware and software infrastructure and resources.The IT systems implemented shall include built-in mechanisms to ensure data security, protection, and disaster recovery in the event of any system failure or data loss. The academic community and the students of the University shall be made fully conversant with the IT facilities and their operational guidelines, including the required safeguards to be followed. The Policy on IT of the University is amplified in terms of its Objects, Scope, and Procedures in its Regulation for Information Technology (IT).

Regulation for IT

This Regulation for Information Technology shall be applicable to all the Campuses of the University. Although the University has adopted the principles and practices of effective use of State of the Art Information Technology in its operations for the past several years, this Regulation is intended to formalize the various aspects of IT Management at the Institution and shall be effective immediately.

Object and Scope

The Policy on Information Technology of the University aims to digitalize and reasonably automate all its process of academic and administrative functionalities. The principal objective of the Regulation is to have transparent systems and procedures in the usage of IT in the conduct of the University activities, including but not limited to Hardware Selection, Procurement and Installation, Software Procurement, Development and Licensing, IT Service Management including but not limited to Preventive and Breakdown Maintenance, Network and Information Security and Risk Management, Electronic Communication Systems and E-Waste Management.

Department of Information Technology Organisation

a) The administration and management of the IT Infrastructure and it usage at the University shall be vested with a dedicated department — Department of Information Technology (DIT) - headed by the Director for IT and supported by Managers, Engineers, Software Developers and Technicians as maybe approved by the Director and considered in the Manpower Budget of the University.

b) There shall be dedicated teams of DIT Technical Staff to undertake and be responsible for specific functional roles of the DIT

c) There shall be teams of DIT Staff posted at different Campuses of the University to coordinate, perform and discharge the duties and responsibilities of the DIT.

d) The DIT shall be responsible for all activities related to installation and servicing of the IT Facilities at the University.

e) Subject to mandated financial and administrative approvals, the DIT shall have exclusive powers to determine and decide on any IT-related proposals, whether for procurement, development, applications or replacement.

f) The DIT shall design/introduce its own protocols, procedures and guidelines including Own End User Code of Conduct for effective implementation of the IT Policy of the University

Procedural Aspects of Information Technology Compliances

The IT Compliances refers to various functional roles and responsibilities of the DIT. The functional roles and the procedural responsibilities for its conduct shall be as detailed hereunder:

1. Hardware Selection, Procurement and Installation

a) The DIT, with reference to the data processing needs of the University, from time to time, shall determine the design, specifications and storage requirements for the different types of Servers - database servers, file servers, mail servers, print servers, web servers, game servers, and application servers — it must possess and shall promptly maintain and upgrade the same as and when required. The Servers shall be installed in an exclusive location with absolute security control with restricted entry and fool-proof Password-protection.

b) Selection and purchase of Computer Hardware including but not limited to Standalone Desktops, Laptops, Pads/Tablets and such other Computer Devices shall adhere to the standard specifications as may be pre-approved by the DIT.

c) No purchase of Computer Hardware by any Department, Centre, Faculty or Staff for use at the University, shall be authorized/approved unless such requirement is prior- reviewed and endorsed by the DIT, in terms of its need and -technical specifications.

d) Any installation of Computer Hardware at the University including its configuration with required Software updates and Server connectivity, shall be handled only by the DIT, through its authorized technical staff.

e) The DIT shall maintain a Campus-wise inventory documentation (Asset Record) for all Computer Hardware purchased and installed at the University and also for the individual Laptops/Pads or other IT-related Assets, issued to Faculty /Staff.

f) Any mishandling, by unauthorized persons of the installed Computer Hardware, at any shall fall to the account of the Department/Centre within whose jurisdiction the said Hardware was installed and such an act of commission or omission shall be deemed an act misconduct by the Faculty/Staff concerned and the Head of the Department shall be held accountable for the fallout.

g) Notwithstanding anything stated above, except for approved BOYD-devices for Laptop [installed with Antivirus Software], no Desktop, on Storage Device, Printer 0r Network Routers shall be brought or used on Campus, without the prior written approval of the DIT

2. **Software Procurement, Development and Licensing**

a) No purchase of Computer Software, for any purpose whatsoever, by any Department, Centre, Faculty or Staff for use at the University shall be authorized / approved unless such requirement is prior-reviewed and endorsed by the DIT in terms of its technical specifications and compatibility.

b) All Software installations in the Systems of the University shall be done only by or under the supervision of the DIT and no other person, including faculty or staff, shall be permitted to directly any–download or independently install any Software.

c) Any in-house Software Development (using the In-house Systems) for use at the University, shall be undertaken only with the prior approval of the DIT and may be undertaken only by involving authorized technical staff of the DIT.

d) The DIT shall ensure that all its Computer installations carry and support only Licensed versions of Software for its Operating System, Antivirus Protection and/or other required applications. Usage of pirated / unauthorized versions of any Software on any Computer System of the University shall remain strictly prohibited under all circumstances.

e) The DIT shall maintain a proper record of the Software used and shall ensure that all Licensed Software installed are duly renewed and validated from time to time.

f) The DIT shall be responsible for periodic checking and updating of the Operating Systems as may be applicable and as provided by the Original System Manufacturers and no individual User shall be permitted to directly download any such updates. For any direct download of such updates.

3. IT Service Management including Preventive and Breakdown Maintenance

The Information Technology Services falling within the authority and responsibility of the DIT shall include all applications and uses of the IT Infrastructure of the University for its Academic, Administrative and other Functional Activities whether or not they are covered by the adopted ERP System, apart from the regular maintenance, upgrading and/or replacement of the IT infrastructure.

a) Any data, literature, brochure, circular, announcements, or such other information whether owned or outsourced, in whatever format, [other than the e-Governance- related pre- approved direct uploading by authorized End Users], shall be uploaded or incorporated in to the ERP System or in the Website/Social Media of the University only with the express approval, in the prescribed format, of the concerned designated Authority not below the rank of the Director, Vice Chancellor, or the Registrar for its authenticity and for non-infringement of IP Rights, where applicable and with additional approval of the Director IT.

b) The Service Team of the DIT shall prioritise the different types of service requirements for its execution and shall set maximum time limits for compliance of and/or resolution of the said service requests.

c) While prioritising the services, due consideration shall be given to the related functional significance/criticality and the impact of time-delay in the service execution. The Priority Classification will be Immediate, High, Medium or Low and shall be attended within the specified time limits for each of the said priorities.

d) In any case any service request (other than for uploading of Data etc.) shall remain unattended/unresolved beyond the immediately following 2 working hours, unless more time is otherwise necessitated, by reason of any valid exigencies and the same has been so informed to the End User, requesting for the service. Services of Immediate Priority shall be attended to even beyond normal working hours. The term 'End User' will mean, the Departments, Centres, Offices, Faculty, Staff and the Students of the University, as may be applicable.

e) Any Service Request shall be made in the prescribed format, either through the relevant ERP Platform,if available or by electronic mail to the System Administrator, from registered email address of the End User or by call recording Help Desk at the DIT, from Official Extension Phone Number of the End User. No Service

Request from Third-party or Unregistered extraneous emails shall be entertained. All Service Requests may be tracked, for its Status, through specially developed Tool.

f) Any Service Request by the End User concerned for uploading data etc.in the Website/social media, as specified in sub-clause (a) above shall be submitted to the Digital Administrator at least 48 hrs prior to the expected date of uploading. Digital team shall not be obliged to attend to any such request submitted at short notice.

g) Apart from attending to the general service requests from time to time the Service Team of the DIT shall schedule periodic preventive maintenance of the entire IT Infrastructure including standalone equipment/s (Desktops) at the University which will include checking and validation of essential support gadgets like UPS, Power Stabilizers, Printers etc. and software like Patch Updates, Anti-Virus, Anti-Spy, Anti-Spam etc. The Service Team while carrying out the scheduled Preventive Maintenance must ensure proper care and diligence for not disturbing or otherwise alienating any saved or unsaved files in the System.

h) All breakdown maintenance irrespective of the location or usage of the IT Equipment shall, unless not feasible for extraneous reasons, be attended to on Immediate Priority.

i) The Service Team of the DIT shall maintain a Log of Services rendered according to its classification as General, Preventive or Breakdown, duly recording the date, time, location, end user, problem identification and resolution, to be verified by the concerned Engineer/Manager and approved by the Director. Any observation by the Service Team for improper handling of the System or for unauthorized net browsing thereon shall be immediately reported to the Director DIT, who may initiate necessary warning/ disciplinary action against the End User concerned, post due process.

4. Network and Information Security and Risk Management

Ensuring Network and Information Security in the University Net Connectivity and to have strict guidelines for data protection and management of inherent risks involved in the usage of the System, shall be a significant responsibility of the DIT. In this regard the DIT as well as the End Users shall strictly adhere to the directions/guidelines specified herein.

A: Network Security

a) Any computer (PC/Server) that is connected to the University Network, shall have an IP address allocated to each End User from a pre-determined address pool and with specified range. Each Network Port at a particular location from where any computer is connected will be bound internally with that IP address so that no other person shall be able to use that IP address from any other location.

b) An IP address allocated for a particular computer system should not be used on any other computer even if that other computer belongs to the same End User and is connected to the same port.

c) IP address allocation shall be done only in alignment with the Dynamic Host Configuration Protocol (DHCP) and no manual IP allocation shall be permitted for any system unless specifically authorized , by the DIT, for valid reasons.

d) The DIT shall provide static IP addresses to the Servers, based on the location of the Server which shall be accessible across the Campus.

e) Any breach of IP Allocation Policy resulting in disconnection of the Network Port shall be deemed a serious misconduct by the concerned and shall be dealt with accordingly.

f) The Wide Area Network (WAN) of the University shall be protected by a Firewall and its connections will be guided through the gateway to ensure legitimate Network Traffic.

g) The University may extend Wi-Fi Facility to the End Users, on their pre-registered devices (Laptops/ Mobiles), to access the Local Area Network within the Campus for pre- authorized use and subject to the Code of Conduct as may be specified. All such access provided shall be controlled either by pre-allotted Password or through Firewall Technology Application.

Provided that any such facilitation of Wi-Fi shall be restricted to the devices supported by the DIT-approved Operating System with active Antivirus Software. Provided further that the DIT shall be empowered to monitor the usage of the devices and shall have the power to discontinue the Wi-Fi Facilitation if the device is found to be used for unauthorized purposes.

h) The University may extend Remote Desktop Application Facility to the End Users, specifically authorized for the use of such Facility, subject to such conditions as may be specified by the DIT, in this direction.

B: Information Security

a) The DIT, subject to prior arrangement, shall facilitate security of the Information Files generated on the Systems at critical Offices/Locations by creating real-time back up storage in separate Storage Devices (NAS Backup) to enable retrieval of data in the event of any exigency.

b) The Information Security of the Files in individual Desktops/ Laptops shall be the primary responsibility of the End User who shall adhere to the Advisory Guidelines that may be issued by the DIT, from time to time. The Guidelines shall include instructions for saving of files in specified Drives within the System or in accessible open source storages like Cloud, Google Drive etc. or in external Hard Dish Drives.

c) The DIT shall conduct training programmes and workshops for orienting and familiarizing the End Users, particularly for the new Faculty and Staff, with essential knowledge and operating guidelines about the usage of the Computer Systems allotted to them including the desirability of Password protection, safeguards against likely pop ups of malicious software etc.

C: Risk Management

a) All desktop computers shall be loaded with updated version of approved Anti-virus and Anti-Spy Software to protect the System and its files. Access to make any changes to Settings of the Computer shall be restricted to the authorized Technical Staff of the DIT.

b) The DIT in order to ensure a robust Disaster Recovery Management Process shall be solely responsible for the management of all the Servers including their timely upkeep and maintenance.

c) The DIT shall ensure practice of High Availability (HA) System that is continuously operational with Load Balancing and Replication Strategies to protect and provide uninterrupted services such as ERP, LMS and Internet to the University. This shall include daily check and documentation of down-time analysis by the IT team to improve the High Availability Factor.

d) The DIT shall ensure Disaster Recovery (DR) compliance by formulating specific policies and procedures to enable the recovery or continuation of vital infrastructure and systems following a natural or human-induced

disaster. This shall include implementation of NAS Backup Device, Replication Architecture, Maintenance of Critical Application Servers, at different locations and Synchronization of Data, across the locations.

5. Electronic Communication Systems

a) The DIT shall introduce and manage effective Electronic Communication System (Email) for the University, for its Faculty, Staff and Students to enable paperless official communication, both internal and external.

b) Every Department or Centre of the University in its Campuses shall have independent email access and every Faculty, Staff and Student of the University shall be provided with exclusive Email ID and login credentials either by designation or by name or by both as may be applicable.

c) Email ID may be allotted to other category of persons such as Guest/Adjunct Faculty, Alumni etc. for specific purposes, subject to administrative approval of the University.

d) The DIT shall control the allotment and removal of Email ID to the approved recipients while they remain associated with or discontinue from the University as the case may be.

e) This shall be done on real-time basis or as soon as such information is advised by the relevant administrative authority of the University, namely the Human Resources Department.

f) No access to any or the system-based facilities and services at the University shall be permitted, unless logged in through the officially allotted Email ID.

g) In addition to personal Email ID allotted to the approved recipients, there may be Group IDs for Faculty or Staff of individual Departments or Deanery or for the Students of particular Class/Section, as may be approved.

h) It shall be the responsibility of the Email ID recipients to protect their email account with strong password which shall remain strictly confidential and personal to the holder. The DIT, unless required under exceptional circumstances as may legitimately warrant and as approved by the Director, shall not directly access any Email account using the System information.

i) The Email Account allotted is intended only for official use of the recipient for recognized purposes and shall be liable for immediate deactivation without notice if it is found to be misused or used for any unauthorized /prohibited purposes.

6. IT E-Waste Management

a) The E-Wastes pertaining to Information Technology normally refers to all material parts of IT Infrastructure and shall include working, outdated, defective or broken items of Desktop Computers, Computer Monitors, Laptops, Circuit Boards, Hard Drives, Storage Devices, and Printing Devices etc.

b) DIT, in pursuance of Social Responsibility Mission of the University and in compliance of the Environment (Protection) Act 1986, shall promptly identify, segregate, store and dispose of all IT E-Wastes generated within the Campus, through approved E-Waste Contractors.

c) No IT E-Wastes generated shall remain stored for beyond 180 days and no part of the E- Waste shall be discarded, burned or buried within the Campus or in the University premises.

Other Regulatory Matters

a) This Regulation has been approved by the Vice Chancellor towards formalization of the IT Policies and Practices already recognized and being followed by the University and has been accordingly notified.

b) Any dispute or conflict with reference to interpretation and implementation of this Regulation shall be resolved by the Director IT in due consultation with technical and or legal experts, if and as may be, felt necessary. The decision of the Director IT in this regard shall be binding on all concerned.

c) No part of this Regulation shall be amended or modified without express consent of the Vice Chancellor of the University.

*****