VIVEKANANDA GLOBAL UNIVERSITY, JAIPUR

(Established by Act11/2012 of Rajasthan Govt. Covered u/s 2(f) of UGCAct,1956)

NAAC ACCREDITED A+ UNIVERSITY

IT Policies & Guidelines

Sector-36, NRI Road, Jagatpura, Jaipur-303012(Raj.) Website: www.vgu.ac.in •E-mail: info@vgu.ac.in
Ph.: 0141-2851000 Toll Free No.: 1800-3-131415 PAN No: AAATB5678H GSTIN: 08AAATB5678H1ZI

STANDARD OPERATING PROCEDURE

SOP No 3: INFORMATION TECHNOLOGY

"If you don't innovate fast, disrupt your industry, disrupt yourself, you'll be left behind."

John Chambers, CEO of Cisco

While conducting the **Orientation Training** of new joinee, the salient features of this SOP especially the users responsibilities towards IT operations must be included in the briefing.

Head IT must also keep issuing **IT Advisories** from time-to-time to highlight the omnipresence of privacy threats and ever-growing importance of cyber security.

For Vivekananda Global University, Jaipur

Registrar

SOP: INFORMATION TECHNOLOGY

Introduction

1. Vivekananda Global University (hereafter referred to as VGU), established in 2012, is a leading private university of Rajasthan. It is located at Jagatpura, Jaipur and is sponsored by Bagaria Education Trust. The main campus has 7 buildings to include Academic Block, Technology Block, Administrative Block, Singar-I Boys Hostel, Singar-II Boys Hostel, Gargi-I Girls Hostel, and Gargi-II Girls Hostel. The VGU campus has about 1.01 lakh sq m of built-up area and 1.19 lakh sq m of open area. Besides approximately 7500+ full time students and a staff complement of just over 500, a large number of visitors come to the University premises daily.

2. VGU not only believes in but have also promoted extensive use of Information Technology in all its facets of academic and administrative operations across the entire campus. For effective usage and application of IT, VGU has all its Departments and Centres adequately equipped with appropriate Hardware and Software. The University has as far as possible integrated its entire IT process under TCS iON cloud-based Enterprise Resource Planning (ERP) System. The IT Systems introduced so far, and in future too will have in-built procedures for the security and protection of data and for its recovery in case of any disaster. The academic community and the students of the University shall be made fully conversant with the IT facilitations and its operational guidelines including the required safeguards to be followed.

Aim

3. The aim of this SOP is to digitalize the VGU and reasonably automate all its processes of academic and administrative functionalities. The principal objective of the SOP is to have transparent systems and procedures in the usage of IT in the conduct of the University operations.

4. It has also outlined the acceptable use of University information technology resources, which include, but are not limited to equipment, software, networks, systems, data storage devices, media, facilities, and stationary and mobile devices used to access VGU information technology resources, whether the technology or devices are personally owned, leased, or otherwise provided by the University.

5. This SOP is also aimed to create a framework for assigning responsibilities and accountabilities of various functionaries involved in IT operations, maintenance and service activities.

Scope

6. This policy applies to all the members of VGU community, who use IT resources, as also the IT staff, vendors and consultants, who manage IT operations

For Vivekananda Global University, Jaipur

Registrar

at VGU. This includes development and maintenance of IT systems, networks, as well as IT facilities provided by individual centres, departments, and university laboratories.

VGU IT Policy Statement

7. The access to the University's information technology resources is a privilege that requires each authorized member to act responsibly and guard against inappropriate use and abuse. Therefore, both the VGU community as a whole and each individual user have an obligation to abide by the standards of acceptable use highlighted in the succeeding paragraphs.

8. The purpose of this policy is to effectively administer and run IT operations at VGU and establish a safe and secure university environment, so as to ensure that the university fulfills its legal and external sponsor obligations.

Guidelines for Fair Use of IT Infrastructure at VGU

9. Usage of VGU information technology infrastructure should always be legal, secure and civil.

(a) **Be Legal**.

(i) Obey Cyber Laws/IT Act 2000.

(ii) Don't illegally download, distribute or use copyrighted materials.

(iii) Don't use the VGU's network to run your business.

(b) **Be Secure**.

(i) Protect your identity. Your accounts are for your use only. Use strong passwords and keep them secret. Never give your password to anyone, no exceptions.

(ii) Don't use other people's accounts. Don't attempt to gain unauthorized access to data and resources.

(iii) Run up-to-date anti-virus software. Apply the latest security patches to all your software and devices.

(c) **Be Civil**.

(i) Respect other's use of IT resources. Don't alter or damage others' data or software.

For Vivekananda Global University, Jaipur

Registrar

(ii) Take care of VGU's computers or networks.

(iii) If you come across an open account on a kiosk or in a computer lab, close it.

Definitions

10. **Access Rights**. The permissions granted to a user to read, write, or erase files in information systems.

11. **Assistive Technologies**. Assistive Technology includes but is not limited to any item, piece of equipment, or product system, whether acquired commercially, modified, or customized, that is used to increase, maintain, or improve functional capabilities of individuals with disabilities.

12. **Audit**. Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies, and operational procedures.

13. **Audit Log**. A chronological record of information system activities, including records of system accesses and operations performed in a given period.

14. **Authentication**. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

15. **Authorization**. The process of verifying that a requested action or service is approved for a specific entity.

16. **Availability**. The expectation that information is accessible by the University community when needed.

17. **Confidentiality**. The state of keeping information and/or materials private, with only authorized individuals, processes, and systems having access to view, use, or share.

18. **Deprovisioning**. The process of removing access rights of all employees and external parties to information and information processing facilities upon termination of, or change to, their employment, contract, or agreement.

19. **Equally Effective**. Equally effective means that, to the maximum extent possible, individuals with disabilities receive the same benefits or services as their nondisabled peers. Access is considered equally effective under this Policy where it communicates the same information and provides equivalent functions in as timely a fashion as does the web page or resource and affords persons with disabilities equal opportunity to achieve the same result, to gain the same benefit, or to reach the same level of achievement, in the most integrated setting appropriate to the person's needs. Providing equally effective access does not require that the alternate means provides the identical result or level of achievement for persons with and without disabilities.

For Vivekananda Global University, Jaipur

Registrar

20. **Guidelines**. Advice on the ways to comply with policy, written for non-technical users who have multiple options for secure information handling processes.

21. **Information Owner**. An organizational official with statutory, management, or operational authority for specified information who is responsible for establishing the procedures governing its generation, collection, processing, dissemination, and disposal. He is responsible for the appropriate use of data and its protection and retains that responsibility even when the information is shared.

22. **Integrity**. The expectation that the University's information will be protected from intentional, unauthorized, or accidental changes.

23. **Monitoring**. Continual checking, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected.

24. **Privileged Accounts**. A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

25. **Procedures**. Step by step instructions and implementation details for personnel to perform specific tasks in ways that ensure that the associated preventive, detective, and/or response mechanisms work as planned.

26. **Provisioning**. Defines the accounts and access rights that are authorized to users or automatically granted for users by the user's role.

27. **Restricted Data**. Restricted Data is the most sensitive information and requires the highest level of protection.

28. **System Owner**. Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

29. **System Account/System Service Account**. A user account created by an operating system and used for the operating system's defined purposes.

30. **Technology Standards**. A formal document that establishes uniform engineering and technical configuration parameters and associated values, methods, practices, or processes that ensure management can secure University assets and comply with University policy and regulatory requirements.

31. **University Business and Academic Activities**. University business and academic activities refer to those activities that students, employees, faculty or visitors must access in order to effectively participate in a program, service, or activity offered by the university.

32. **University Business**. Work performed as part of an employee's job responsibilities, daily work, and duties performed on behalf of the University by faculty, staff, student workers, guests, and other persons whose conduct, in the performance of work for the University, is under the direct control of the University, whether or not they are paid by the University. This includes any email, calendar events, files, or other

For Vivekananda Global University, Jaipur

electronic business data, created, stored, processed, and transmitted that is related to work performed for VGU.

33. **University Website**. Any website hosted by or for university units, organizations, faculty, students or staff that provides content related to university business or academic activities.

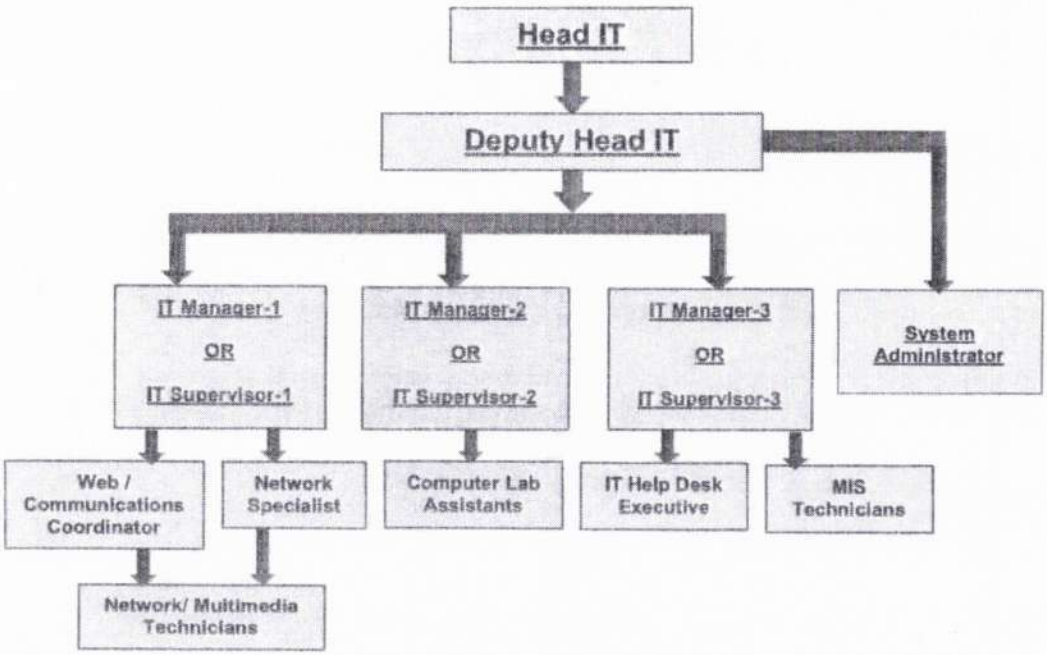
34. **User**. An individual, group, or organization granted access to organizational information in order to perform assigned duties.

35. **User Account**. The collection of specific access privileges for authorized users to gain access to information systems.

36. **Web Accessibility**. The practice of making web content accessible by applying specific principles for web design and programming that enable assistive technologies to function properly.

Organizational Structure and Reporting Channels

37. **Organizational Structure**. The Organizational Structure of the IT Cell will define the reporting channel and the escalation matrix of complaint reporting and resolution.



38. **IT Cell**. The administration and management of the IT Infrastructure and its usage at the University shall be vested with a dedicated department viz. IT Cell - headed by the Head IT and supported by Deputy Head IT, Managers, Engineers, Software Developers and Technicians as maybe approved by the Dy Director and considered in the Manpower Budget of the University.

For Vivekananda Global University, Jaipur

Registrar

39. There shall be dedicated teams of IT Cell Technical Staff at different blocks to undertake and be responsible for specific functional roles of the IT Cell. The IT Cell shall provide technical assistance for all activities related to installation, maintenance and oversight of the VGU's computer network, software, and hardware inventory, telecommunication network, and any technology initiatives within the VGU campus.

40. Subject to financial and administrative approvals, the IT Cell shall have exclusive powers to determine and decide on any IT related proposals, whether for procurement, development, applications or replacement. However, the IT Cell would encourage all departments and employees to be our partners in planning for future computing environments for the VGU. The IT Cell 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.

Roles and Responsibilities

41. **Management and Responsibilities**.

(a) It is essential that adequate resources are made available for managing the IT operations by ensuring proper maintenance and upkeep of the VGU's IT infrastructure and resources.

(b) It is important that all personnel involved in implementing this policy are competent, trained and aware of their responsibilities.

42. **IT Cell**. The IT Cell determines and conceptually plans the best ways for technology to meet the goals of the VGU. The IT Cell will install, maintain, and upgrade systems as necessary. The IT Cell will be responsible for researching and developing new ways to accomplish tasks in a productive timely manner. All computing devices and applications added to the VGU servers have an impact on the overall network. The IT Cell's ability to properly support new devices and applications often require additional resources that may take time to acquire and install. The IT Cell will balance the load of services across resources, as necessary. The security of the VGU's computer system is a major priority of the IT Cell. By including the IT Cell in preliminary discussions, University can start preparations to support and keep projects flowing smoothly. The IT Cell is responsible for the following functions: -

(a) PBX's & Voice Mail Systems.

(b) Internet Access & E-mail.

(c) Computer/Laptop Hardware.

(d) Program Software.

(e) Copiers/Fax/Scanners - All peripherals.

(f) Video & Audio Equipment.

For Vivekananda Global University, Jaipur

Registrar

(g) Maintenance of network security and performance; establishment of workable directory structure, network security, and disk space allocation, etc.

(h) Set-up of user accounts according to set established policies, procedures, and limitations.

(i) Tracking of all problems or issues through work orders.

(j) Planning new phone lines and data ports when needed.

(k) Performing network maintenance, changes, and upgrades.

(l) Enhancing network by assessing new software and hardware products that would increase network performance and expand network services.

(m) Directing the performance of regularly scheduled systems management and maintenance procedures designed to ensure the integrity of all programs by running backup procedures and diagnostic software routines.

(n) Implementing disaster recovery plans; running system backups and disaster recovery operations.

(o) Developing procedural documentation or policies, as needed.

(p) Providing technical advice and training to VGU operations staff in the operation, maintenance, and support of computer hardware and software system.

(q) Train and update the IT staff with respect to security systems.

(r) Prepare reports and make recommendations to ensure the optimum efficiency of equipment and systems in accordance with departmental needs.

(s) Maintain stock of expendable and non-expendable computer equipment, materials, system, application, and supplies sufficient to ensure continuous and uninterrupted operation of systems; communicate with Head Procurement and vendors regarding purchases.

(t) Maintain professional and technical knowledge by conducting research; attending seminars, education workshops, classes and conferences; reviewing professional publications; establishing agencies and related organizations.

43. **Head IT**. The Head IT is responsible for all the IT operations across the VGU's properties. He will ensure that requisite support/training and resources are made available to the IT Managers to implement the IT Policy, including assembling and maintaining a suitably qualified supervisory team. He will also keep himself abreast with emerging IT technologies, and recommend upgradation whenever needed. He has the authority to hire or discharge subordinates. The duties and responsibilities of Head IT are enumerated at **Appendix A**.

44. **Deputy Head IT**. He is responsible and accountable for the total maintenance and upkeep of the VGU's IT infrastructure and resources. He will supervise all IT

For Vivekananda Global University, Jaipur

Registrar

Managers/Supervisors, plan and assign work assignments, organise training sessions/workshops for IT Cell staff, ensure cyber security, inspect completed assignments, and requisition supplies. The duties and responsibilities of the Deputy Head IT are enumerated at **Appendix B**.

45. **IT Managers/Supervisors**. The duties and responsibilities of IT Managers/ Supervisors are enumerated at **Appendix C**.

46. **IT Technicians**. The duties and responsibilities of IT Technicians are enumerated at **Appendix D**.

47. **IT Help Desk Executive**.

(a) The IT Help Desk is the nerve centre of the IT Cell. The desk is manned throughout the office hours from 08:30 AM to 05:30 PM on all the working days. Since the help desk is the hub of information dissemination in IT management, the IT Help Desk Executive is a critical person in IT operations. ***IT Help Desk Executive will record all the complaints reported to him/her, and not use his/her discretion whether to docket it or not.***

(b) The duties and responsibilities of IT Help Desk Executive are enumerated at **Appendix E**.

48. **Staff**. All staff must be knowledgeable of, and adhere to the IT SOP.

49. **Students**. Students must follow the various IT protocols, maintain proper cyber hygiene, look after the IT resources entrusted to them by the University, and co-operate with requests from the IT Maintenance Teams, especially while undertaking the various maintenance and repair works.

50. **Visitors**.

(a) Visitors are required to follow VGU's IT SOP and follow directions from their host/sponsoring section or the IT Maintenance Team, particularly when the repairs are in progress, and there is a breakdown in the network connectivity.

(b) It is the responsibility of the host/sponsoring agency to ensure all visitors are informed of and comply with the VGU's IT SOP of not interfering with the repair work of the IT Maintenance Teams, as also not to use the IT resources till such time it is fully repaired.

IT Policy: General

51. **User Responsibilities**.

(a) **Privacy**. Because the primary use of the VGU's communications and business systems is to further the institutional mission, members of the VGU

For Vivekananda Global University

Registrar

community should not have the expectation of privacy in their use of electronic systems, whether work-related or personal. By their nature, electronic systems may not be secure from unauthorized access, viewing, or infringement. Although the VGU employs technologies to secure its electronic resources and does not monitor the content on a routine basis, as a rule confidentiality of electronic data cannot be assumed and the University reserves the right to examine all files and content without notification.

(b) **Intellectual Freedom**.

(i) It is the policy of VGU to allow access for its community to local, national, and international sources of information and to provide an atmosphere that encourages the free exchange of ideas and sharing of information. Nevertheless, the University reserves the right to limit or restrict the use of its information technology resources based on applicable law, institutional policies and priorities, and financial considerations.

(ii) Violations include but are not limited to certain categories of speech viz. defamation, obscenity, and incitement to lawlessness, which are not protected by the Constitution. The VGU reserves the right, at its sole discretion, to decline to post, to remove posted content, or to restrict University web sites or computer accounts which contain or are used for personal expressions of a non-academic nature.

52. **Use IT Resources Authorized to You**.

(a) **Scaling of IT Equipment Based on Academic Appointment/Rank**. The details of IT Equipment scaled to the various Faculty Members, as per their academic appointment/rank, are enumerated below: -

S/No.	Academic Appointment/Rank	IT Equipment		
		Desktop/Laptop	Printer	Intercom
(i)	Dean	Yes	Yes (Small)	Yes
(ii)	Associate Dean	Yes	No	No
(iii)	HOD	Yes	Common Big Printer/Copier/ Scanner in the Faculty Room	Yes
(iv)	Professor	No		No
(v)	Associate Professor	No		No
(vi)	Assistant Professor	No		No
Each group of ten faculty members in a Department (excluding Deans, Associate Deans, and HODs) will be allocated one desktop computer. If the number of faculty members exceeds ten, the number of desktops will be increased proportionately.				

(b) Each user may use only those information technology resources for which he or she has authorization. Violations include but are not limited to: -

For Vivekananda Global University, Jaipur

Registrar

(i) Failing to take reasonable and necessary measure to safeguard the operating integrity of systems and their accessibility by others;

(ii) Sharing passwords or log-in IDs. Users are responsible for any activity conducted with their computer accounts;

(iii) Using resources without specific authorization;

(iv) Using another individual's electronic identity;

(v) Accessing files, data, or processes without authorization.

53. **Use IT Resources Only For Intended Purpose**. Information technology resources must be used only for their intended purpose(s) relating to University business. Violations include but are not limited to: -

(a) Misusing software to hide personal identity, or to interfere with other systems or users;

(b) Misrepresenting a user's identity in any electronic communication;

(c) Using electronic resources for deceiving, harassing, or stalking other individuals.

(d) Sending threats, "hoax" messages, chain letters, or phishing;

(e) Sending mass emails to the VGU community without following proper procedures;

(f) Intercepting, monitoring, or retrieving without authorization any network or other electronic communication;

(g) Using University computing or network resources for private advertising or other private commercial purposes;

(h) Circumventing, disabling, or attempting to circumvent or disable security mechanisms without authorization;

(i) Using privileged access to University systems and resources for other than official duties directly related to job responsibilities, with the exception of incidental private use;

(j) Making University systems and resources available to those not affiliated with the University;

(k) Using former system and access privileges without authorization after association with the University has ended or using system and access privileges to a former organization's resources without authorization after the transfer to the new organization.

For Vivekananda Global University, Jaipur

Registrar

54. **Safeguarding Access and Integrity of IT Resources**. The access to and integrity of IT resources must be protected. Violations include but are not limited to: -

(a) Using third party, cloud and non-cloud, systems not authorized or approved by Head IT to transmit, process, or store the University data classified as Critical or Restricted;

(b) Creating or propagating malware, spyware, computer viruses, worms, Trojan Horses, or any other malicious code;

(c) Preventing others from accessing an authorized service;

(d) Developing or using programs that may cause problems or disrupt services for other users;

(e) Degrading or attempting to degrade performance or deny service or to waste or unfairly monopolize computing resources policies;

(f) Corrupting or misusing information;

(g) Altering or destroying information without authorization.

55. **Compliance of Laws and Policies**. Applicable Central, State, and local laws and University policies must be followed. Violations include but are not limited to: -

(a) **Laws**.

(i) Failure to respect the copyrights and intellectual property rights of others;

(ii) Making more copies of licensed software than the license allows;

(iii) Downloading, using, or distributing illegally obtained media (e.g., software, music, movies, images, etc.);

(iv) Uploading, downloading, distributing, or possessing electronic content explicitly prohibited by Centre, State, or local law (i.e., child pornography).

(b) **Policies**.

(i) Accessing, storing, or transmitting information classified as Critical or Restricted (e.g., social security numbers, patient health information, driver's license numbers, credit card numbers) without a valid business or academic reason or transmitting such information without using appropriate security protocols (e.g., encryption);

(ii) Distributing data/information classified as Critical or Restricted, unless acting as an authoritative University source and an authorized University distributor of that data/information and the recipient is authorized to receive that data/information;

For Vivekananda Global University, Jaipur

Registrar

(iii) Transmitting unencrypted Critical or Restricted information over open public networks such as the internet or unencrypted email;

(iv) Using social media to communicate or store University data/information classified as Critical or Restricted;

(v) Using third party cloud storage or data sharing tools (i.e., iCloud, Carbonite, Dropbox) to store University information classified as Critical or Restricted without prior approval of Head IT.

56. University business should be conducted using University-provided information technology systems, resources, and services.

57. **Accessing Information and Records**.

(a) Recognizing that not all circumstances can be anticipated, access to information and records residing on University information technology resources will ordinarily be governed by the following: -

(i) **University Responsibilities**. The University's obligations in relation to information technology resources include ensuring compliance with applicable laws and University policies and procedures, protecting the integrity and operation of its resources, and preserving information as necessary to protect the interests of the University and to enable it to satisfy these obligations. Accordingly, the University may access VGU-related electronic information on any device on which it is stored or may be accessed, and may access a user's records and information stored on University information technology resources systems or equipment for the above-mentioned purposes. Such access must be for specific, articulable reasons, must be appropriately circumscribed, and is limited to authorized personnel. The University understands that some users may have personal information and/or records on University systems and it respects the privacy of all users as to such information insofar as possible in complying with its above-mentioned obligations.

(ii) **Employee Obligations - Standards of Employee Conduct for Accessing or Monitoring Records**. It is a violation of this policy for an employee to monitor information technology resources or record systems or access records beyond the standards established within this policy. It is also a violation of the policy if the University has granted access to the employee (to monitor or access records or systems) and the employee has accessed or monitored records or record systems for purposes other than the purposes for which the University has granted access.

(b) **Standards for Accessing or Monitoring Information and Records**.

For Vinh Long Global University, Vietnam

Registrar

(i) The University may access or monitor any/all information, records, record systems, and/or information technology resources in the following circumstances: -

(ai) As necessary or appropriate to avert reasonably anticipated or already apparent threats or hazards to University information, records, or information technology resources. An example includes scanning to detect computer viruses;

(aii) As and when required by law or to comply with legal or contractual obligations of the University;

(aiii) In connection with a legal proceeding in which the Office of Proctor is involved or an investigation conducted by or on behalf of the ICC, for which access is necessary or appropriate;

(aiv) When there is reasonable cause to believe that the employee has engaged in misconduct, has violated University policies or regulations, or may have used University resources improperly and that the information and records to be accessed or monitored are relevant to the misconduct or violation in question;

(av) When the University otherwise has a legitimate need to access the information, records, or information technology resources.

(ii) Reasonable efforts will be made to notify the individual of the need for access to information or records in which the individual has a substantial personal interest in information or records stored on or transmitted through the University's information technology resources or other electronic system unless prohibited by law, inconsistent with University policy, or inconsistent with the University carrying out its normal operations and/or aforementioned obligations.

(c) **Preserving and Protecting Records**. In circumstances, where the University determines that there may be a specific risk to the integrity or security of records, data, information, or information technology resources, the University may take measures to protect or preserve them. For instance, the University may take a "snapshot" of a computing account to preserve its status on a given date, copy the contents of a file folder, or restrict user access to information technology resources in whole or in part.

58. **Telecommuting and its Impact to Security and Privacy**.

(a) University policies, procedures, laws and regulations are applicable at all times. Individuals accessing University resources, systems, and information from alternate places of work (i.e. telecommuting from home, temporary office space, or while traveling) must adhere to all University policies, procedures, laws, and regulations.

For Vivekanand Global University, Jaipur

Registrar

(b) **Information Users Must**.

(i) Access University resources, systems, and information via approved secure channels that enforce the classification of the data and all regulatory requirements pertaining to the resources.

(ii) Use only University-approved software for conducting University business including but not limited to email, video conferencing, and collaboration software.

(iii) Use only University-approved devices for conducting University business including but not limited to laptops, computers.

(iv) Keep University and personal data or email from being co-mingled.

(v) Ensure all personal devices used to access the Internet (modems, Wi-Fi, etc.) are up-to-date with regard to operating systems, application software versions, and antivirus protection.

(vi) Adhere to the following practices to protect University information:

(ai) Utilize multifactor authentication,
(aii) Clean desk/clear screen,
(aiii) Log off/lock all devices when unattended or not in use,
(aiv) Secure University equipment in a locked drawer or room when not in use.

(vii) Be alert for fraud, suspicious email, phishing, and scams that will attempt to take advantage of the situation.

(viii) Ensure printed information and other media are protected from theft and accidental disclosure and are disposed of in a manner that enforces the classification of the data (e.g. shredded).

(ix) Backup and save University work product only to secured network drives.

(ai) Encrypt data classified as Restricted or Critical that is to be transmitted.

(aii) Report loss or theft of a Mobile Computing Devices, Removable Media or media immediately to the IT Help Desk and Proctor, as per VGU Policy on Incident Management.

Procedural Aspects of Information Technology Compliances

For Vivekananda Global University

Registrar

59. The IT Compliances refers to various functional roles and responsibilities of the IT Cell. The functional roles and the procedural responsibilities for its conduct shall be as detailed in the succeeding paragraphs.

60. **Hardware Selection, Procurement and Installations.**

(a) The IT Cell with reference to the data processing needs of the University from time to time shall determine the design, specifications and storage requirements of the Cloud Server to cater for the needs of different types of servers viz. database servers, file servers, mail servers, print servers, web servers, game servers, and application servers. Depending upon the IT resources and IT load, IT Cell must acquire Cloud Server of appropriate size and rental, as also promptly maintain and upgrade the same, whenever the need arises.

(b) Selection and purchase of Computer Hardware including standalone Desktops, Laptops, Pads/Tablets and such other Computer Gadgets shall adhere to the standard specifications as may be pre-approved by the IT Cell.

(c) No purchase of Computer Hardware by any Department, Centre, Faculty or Staff for use at the University shall be authorised/approved unless such requirement is prior reviewed and endorsed by the IT Cell for its need, compatibility and its technical specifications.

(d) Any installation of Computer Hardware at the University including its configuration with requisite software updates and server connectivity shall be handled only by the IT Cell, by its authorised technical staff.

(e) The IT Cell shall maintain a block/building-wise inventory documentation (Asset Record) for all Computer Hardware purchased and installed at the University and also for the individual Laptops/Pads issued to Faculty/Staff.

(f) Any mishandling of the installed Computer Hardware by unauthorised persons shall be accountable by the Department/Centre concerned and will be a deemed misconduct by the Faculty/Staff concerned.

61. **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 authorised/approved unless such requirement is prior reviewed and endorsed by the IT Cell for its technical specifications and compatibility.

(b) All software installations in the systems of the University shall be done only by the IT Cell and no other person including Faculty or Staff shall be permitted for any direct download or independent installation of Software.

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

(d) The IT Cell shall ensure that all its computer installations carry and support only Licensed Software for its operating system, antivirus protection and the required applications. Usage of pirated/unauthorised versions of any

For Vivekananda Global University

Registrar

software on any Computer System of the University shall remain strictly prohibited under all circumstances.

(e) The IT Cell 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 IT Cell 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 for any direct download of such updates.

62. **Prohibited Hardware and Software**.

(a) The IT Cell will monitor the software and hardware installations within the VGU's systems, the following are prohibited hardware and software: -

(i) Hardware or software that makes any portion of the network unstable.

(ii) Hardware or software that is used for illegal purposes.

(iii) Hardware or software, which have licensing issues, which legally prohibit its use.

(iv) Hardware or software may also be prohibited due to its tendency to destabilize or compromise the security of core network services.

(b) In all cases, any hardware or software that makes any portion of the network unstable will be immediately removed from the network and the system will be restored to its standard configurations.

63. **Portable Devices**.

(a) The users of portable devices are responsible for such devices and will be held accountable for the care of such devices. The term "portable device" includes but is not limited to the following: -

(i) Laptops.
(ii) External Hard Disk Drives.
(iii) USB Data Devices.
(iv) Portable Music Players.
(v) Storage Media - CD/DVD/SD/Mini SD/Memory Sticks.
(vi) iPads.
(vii) Mobile Phones - Basic and Smartphones.
(viii) Data Access Points - MiFi Cards.

(b) These devices should be stored properly while not in use and shall have approved anti-virus software installed and up-to-date (if applicable). All users are required to have proper authorization of a portable device from their

For Vivekananda Global

Registrar

supervisor prior to being issued such device. The IT Cell will maintain a list of all issued devices and will monitor the user's activity of such devices.

64. **Internet Access**.

(a) The internet provides access to a variety of information, both good and questionable value and is not a secure means of communication. It is the responsibility of the user to ensure the VGU's Computer, Intranet, and Internet Use Policy is being followed. The IT Cell will monitor user activity through monitoring and filtering software to prevent access to sites which are illegal or against VGU policies.

(b) **Internet Redundancy**. Since internet availability is a must to carry out most of the VGU's IT operations, the IT Cell will ensure its 100% availability at all times. The IT Cell will cater for adequate redundancy by having internet access from two different highly reliable service providers to ensure no downtime. For electrical connection also, the IT Cell will cater for online UPS, so as to get uninterrupted power supply to critical components viz. routers, switches, modems, gateways, repeaters, etc.

65. **Remote Access**. Remote access to the VGU's computer system and information is only permitted through secure, authenticated and centrally managed access methods. This access must be approved by the user's supervisor and can only be used to conduct VGU business. The IT Manager will establish a VPN connection and will ensure the connection is authenticated and encrypted.

66. **IT Service Management including Preventive and Breakdown Maintenance**.

(a) The IT services falling within the authority and responsibility of the IT Cell shall include all applications and uses of the IT infrastructure of the VGU for its academic, administrative and other functional activities whether or not they are covered by the adopted ERP System, apart from the regular maintenance, upgradation and/or replacement of the IT infrastructure.

(b) Any data, literature, brochure, circular, announcements, or such other information whether own or outsourced, in whatever format, other than the e-Governance related pre-approved direct uploading by authorised 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 Deputy Director, Dean or the Registrar for its authenticity and for non-infringement of IP rights, where applicable and with additional approval of the Head IT.

(c) The Service Team of the IT Cell 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.

(d) 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.

For Vivekananda Global University, Jaipur

Registrar

(e) In any case, no service request (other than for uploading of data etc.) shall remain unattended/unresolved beyond the immediately following 12 working hours unless more time is otherwise necessitated by the exigencies and 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.

(f) **IT Work Order**. Any service request shall be made in the prescribed format (IT Work Order) either through the relevant ERP Platform, where available, or by electronic mail to the System Administrator from registered email address of the end user, or by call recording IT Help Desk at the IT Cell from official extension phone number of the end user to begin the troubleshooting process. The remedy will be addressed according to the severity of the problem. There are times when a problem is actually department or organization wide problem. These types of problems will require the IT staff to do further research and often requires them to coordinate solutions with third parties. 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.

(g) Any service request by the end user concerned for uploading data etc. in the website/social media, as specified in Para 67(b) above shall be submitted to the System Administrator at least 48 hrs prior to the expected date of uploading. IT Cell shall not be obliged to attend to any such request submitted at short notice.

(h) Apart from attending to the general service requests from time to time the Service Team of the IT Cell shall schedule periodic preventive maintenance of the entire IT Infrastructure including standalone equipments (Desktops) at the University, which will include checking and validation of essential support gadgets like UPS, Power Stabilisers, 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 any saved or unsaved files in the system.

(i) 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.

(j) The Service Team of the IT Cell 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 Deputy Head IT. Any observation by the Service Team for improper handling of the system or for authorised net browsing thereon shall be immediately reported to the Head IT who may initiate necessary warning/disciplinary action against the end user concerned.

67. **Network and Information Security and Risk Management**.

For Visva-Bharati Global University, Santiniketan

Registrar

(a) 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 IT Cell. In this regard, the IT Cell as well as the end users shall strictly adhere to the directions/guidelines specified herein.

(b) **Network Security**.

(i) 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.

(ii) 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.

(iii) IP address allocation shall be only by Dynamic Host Configuration Protocol (DHCP) and no manual IP allocation shall be permitted for any system unless specifically authorised by the IT Cell for valid reasons.

(iv) The IT Cell shall provide static IP addresses to the servers based on the location of the server which shall be accessed across the campus.

(v) 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.

(vi) 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.

(vii) The University may extend Wi-Fi facility to the end users, on their pre-registered device (Laptops/Mobiles), to access the Local Area Network within the campus for pre-authorised 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 IT Cell approved operating system with active antivirus software. Provided furthermore that the IT Cell 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 unauthorised purposes.

(viii) The University may extend remote desktop application facility to the end users, specifically authorised for the facility, subject to such conditions as may be specified by the IT Cell.

(c) **Information Security**.

(i) The IT Cell 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) on the Cloud Server to enable retrieval of data in the event of any exigency.

(ii) 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 IT Cell 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 Disk Drives.

(iii) The IT Cell shall conduct training programmes and workshops for orienting and familiarizing the end users, particularly the newly joining 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.

(d) **Risk Management**.

(i) 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 authorised technical staff of the IT Cell.

(ii) The IT Cell in order to ensure disaster recovery management shall be solely responsible for the management of all the servers including its timely upkeep and maintenance.

(iii) The IT Cell 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 for the University. This shall include daily check and documentation of down time analysis by the IT Team to improve the high availability factor.

(iv) The IT Cell shall ensure Disaster Recovery (DR) by evolving 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.

68. **Electronic Communication Systems**.

(a) The IT Cell 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.

For Vivekananda Global University, Jaipur

Registrar

(b) Every Department or Centre of the University 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 IT Cell 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. This shall be done on real time basis or as soon as such information is advised by the relevant administrative authority of the University.

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

(f) 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.

(g) 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 IT Cell unless required under exceptional circumstances as may legitimately warrant and approved by the Deputy Director, shall not directly access any Email account using the system information.

(h) The e-mail account allotted is intended only for official use of the recipient for recognised purposes and shall be liable for immediate deactivation without notice if it is found to be misused or used for any unauthorised /prohibited purposes.

69. **User Accounts, Email & Passwords**. The IT Cell assigns, updates and monitors all VGU email addresses and accounts. Additionally, the IT Cell monitors and updates all systems passwords as appropriate for each individual user. Every new employee whose position requires them to use a computer will be assigned an email account with a password at the time of hire. Each Reporting Officer must make an appropriate request for a new user setup to the IT Cell through an IT Work Order to set up a new user account. All computer users must change passwords every (6) six months. Each users' computer system will prompt them to change passwords automatically. The IT Cell reserves the right to have users change their passwords at any time if the system has been compromised.

70. **Relocation of Computers or Printers**. The IT Cell will be responsible for relocating all computer systems and peripherals. An IT Work Order must be submitted to the IT Help Desk email address at least 5 working days in advance of the relocation to avoid delays in the setup process. In the case of an extreme emergency, the user must contact the IT Manager.

For Vivekananda Global University, Jaipur

71. **Website**. The VGU Website is designed to provide outside access to information regarding the VGU and the University's governmental and entity operations. The following apply to the VGU Website: -

(a) Departments/Programs are responsible for ensuring their webpage is updated at least every 30 days.

(b) All content submitted for posting on the website must state a source. All external sources will be credited.

(c) Copyrighted material must be accompanied by a properly executed release from the author and/or photographer.

(d) Copies of properly executed release forms are required when posting photos of minors and non-users.

(e) The website calendar is provided for government/community events only.

(f) Links to websites found to be under construction or inactive will be removed. No links to personal websites will be posted.

72. **Teleconferencing/Audio Visual**. The IT Cell will assist all departments and centres with any teleconference or audio visual needs. To ensure a successful conference or presentation, the following must occur: -

(a) An IT Work Order must be received by the IT Cell at least 48 hours in advance to ensure adequate staffing is available for the request.

(b) Requests for teleconferencing that require more than 3 lines to be teleconferenced into a VGU's telephone line require at least five (5) business days advance notice.

(c) The IT Cell will call the Work Order initiator to ensure the details of the project and plan accordingly.

73. **Telephones/Communications**. The IT Cell manages and monitors all land lines, telephones and cellular telephones. Telephone lines, long distance codes, data cards, and cell phones must be first approved by the user's Reporting Officer. The Reporting Officer will make the request to the Deputy Head IT to install or add a line for a user via IT Work Order.

74. **Data Backup and Disaster Recovery Plan**.

(a) The VGU IT Cell provides complete automatic backup services on Cloud Server, which typically include, but are not limited to, laptops, desktops, servers etc. The process is designed to protect University's data and to be sure that it is not lost and can be recovered in the event of an equipment failure, intentional/unintentional destruction and/or disaster.

For Vivekananda Global University, Jaipur

Registrar

(b) Data is backed up not only to provide disaster recovery but also future retrieval. This applies to all equipment and data owned and operated in and by the university. The IT Cell's plan minimizes disruptions of critical functions and ensures the capability to recover operations expediently and successfully.

(c) Users are expected to ensure the safety of the data stored physically on their laptop/desktop/external drives. The IT team will provide all the assistance required for this purpose. For the safety of very critical data: -

(i) HODs can request IT support to create a folder for the department on the server that is backed up regularly. The files on this server drive will be made accessible to the users of the department authorized by the HOD.

(ii) Users are advised to maintain backup of their critical data either on external media, or on Google Drive.

(d) **Storage of Data Backups**. All the data will be stored on the Cloud Server Storage.

(e) **Schedule for Backups**. The schedule of backup will be decided by the IT Cell based on the necessity and rental charges of the Cloud Storage, so as to bring resilience and ensure that the Business Continuity norms are fulfilled.

75. **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) IT Cell 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 University premises.

76. **Complaint Registration, Rectification and Escalation Matrix**.

(a) **Complaint Registration and Rectification**.

(i) VGU has a well-established IT Help Desk to register complaints regarding IT services. The contact number of IT Help Desk Executive will be communicated through e-mail/circular.

(ii) Every IT related complaint will be registered by the IT Help Desk Executive after ascertaining the caller's details viz. name, mob No., location of problem, and exact nature of complaint. Each complaint will

For Vivekananda Global University, Jaipur

Registrar

be properly docketed and the complainant will be immediately intimated the Complaint No for tracking and giving feedback.

(iii) Complainant can also lodge the complaint by physically writing the details himself in the register maintained at the IT Help Desk.

(iv) IT Help Desk Executive will immediately get in touch with the IT Manager/Supervisor, and report the issue. He will also ask the IT Manager/Supervisor, the tentative timeframe in which the complaint will be attended to or fully rectified.

(v) Once the complaint is registered, a Digital Job Card will be created by the IT Help Desk Executive and forwarded to the IT Manager/ Supervisor through WhatsApp. The same Job Card will be forwarded to the senior most IT Technician of the respective field, who will attend the complaint. Once the job is over, the IT technician will forward the same to the complainant. The complainant once gets satisfied by the job would forward the Job Card to IT Manager/Supervisor with a message 'Completed'. IT Manager/Supervisor will forward this message to the IT Help Desk Executive. At this stage, the complaint would be considered as fully rectified, and the time noted in the register of job card closure.

(vi) In case, the response time is going to be more due to some other pressing needs, the IT Help Desk Executive will give an interim feedback to the complainant about the likely timeframe of rectification.

(vii) In case, the same complaint resurfaces, the complete cycle will be again followed with a new Complaint No.

(b) **Escalation Matrix**.

(i) Escalation Matrix is a tool used by VGU to manage the escalation process. The purpose of escalation matrix is to track all IT related issues encountered during our day-to-day work and their corresponding solutions to know where we stand on each issue at a time. This will help supervisory/managerial staff in making decisions regarding what problems need immediate attention, who should handle them and how best they should be resolved within our team or organization as a whole.

(ii) The IT Cell strives to provide the most effective and efficient IT services to the VGU employees and other users of the VGU network. If for some reason there is a complaint regarding the IT Cell services or staff, this should be expressed to the Cell. If this does not lead to improvement, the complainant should be directed through the appropriate chain of command viz. the Deputy Head IT, Head IT, and then the Deputy Director.

(iii) The escalation matrix format will also be used to track the number of issues that are reported, their severity, and whether they have been resolved or not.

For Vivekananda Global University, Jaipur

Registrar

(iv) Head IT will create a WhatsApp Group, as an Admin, with all the IT Managers or IT Supervisors, IT Technicians, IT Help Desk Executive, and his own Reporting Officer as a member.

(v) The IT Help Desk Executive will create an Excel Sheet and will keep posting it on the WhatsApp Group at 09:30 AM and 01:30 PM every day after fully updating it. The format of the escalation matrix is attached as **Appendix G**. ***This Excel Sheet is over and above the details maintained in the Complaint Register.***

(vi) Every week a new Excel Sheet will be created, however, all the old/outstanding complaints with the same Complaint No will be carried forward.

Detailed Policies on Specific Issues

77. **IT Provisioning/Deprovisioning Policy**. A policy on IT Provisioning and Deprovisioning is attached as **Appendix H**.

78. **Information Security Awareness, Training, and Education Policy**. A policy on Information Security Awareness, Training, and Education is attached as **Appendix I**.

79. **Incident Reporting and Management**. A policy on Incident Reporting and Management is attached as **Appendix J**.

80. **Data Breach Management Policy**. A policy on Data Breach Management is attached as **Appendix K**.

81. **Email and Calendar Policy**. A policy on Email and Calendar is attached as **Appendix L**.

82. **IT Audit and Monitoring Policy**. A policy on IT Audit and Monitoring is attached as **Appendix M**.

Important Contact Numbers

83. **IT Help Desk Executive**. The IT Help Desk is staffed every day by an IT Help Desk Executive throughout the working hours and can be contacted on Mobile No 8766696667.

84. **As per Escalation Matrix**.

(a) **IT Supervisor**. Mr. Mahaveer (Mob No 9610522552).

For Vivekananda Global University, Jaipur

Registrar

(b) **Deputy Head (IT)**. Mr. Kailash Sharma (Mob No 9529950162).

Reporting, Audits and Reviews

85. **Reporting**. The IT Cell shall provide progress reports to the Deputy Director on a fortnightly basis or as requested. Timelines of the Annual Report and Annual Budget narratives are determined on an annual basis. The IT Cell staff is responsible for ensuring all timelines are met according to the directives.

86. **Other Regulatory Matters**.

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

(b) No part of this SOP shall be amended or modified without express consent of the CEO of the University.

87. **Internal IT Audit**. Every month a team comprising of faculty and support staff members will carry out a comprehensive internal IT audit covering all facets of maintenance, service, and repair work, and comment on the efficacy of the IT Policy. The report will be put up to the Deputy Director through AVP (Establishment), and after due diligence rectification action on relevant issues will be taken by the Head IT post haste, and interim/completion report rendered to the Corporate Office.

88. **Policy Review Schedule**. This policy will be reviewed annually, or as new knowledge on the subject evolves and subsequent guidance is received.

Conclusion

89. The SOP aims to provide the VGU's employees, and system users, high quality technical services provided by the VGU's Information Technology Cell and to assist VGU computer users in finding the appropriate resource to answer their questions, resolve any computer or network related problems, update applications developed in-house, assist with specific program needs, and aid them in finding appropriate computer related tools to accomplish their job at the VGU.

90. Proper implementation of this SOP will go a long way to ensure data security and integrity.

Anil Bagaria

Place: - Jaipur

(Er Anil Bagaria)
Dy Director

Date: - 11 Jul 2024

For Vivekananda Global University, Jaipur

Registrar

DISTRIBUTION SHEET

S/No	Copy To	Quantity	Copy No
1.	Chairperson	01	1
2.	Vice Chairperson	01	2
3.	CF & AO	01	3
4.	President	01	4
5.	Pro President	01	5
6.	Registrar	01	6
7.	Dir, FOM	01	7
8.	Dy Dir	01	8
9.	Coordinator, IQAC	01	9
10.	Head IT	01	10
11.	Head (Maintenance & Infra)	01	11
12.	Head Procurement	01	12

For Vivekananda Global University, Jaipur

Registrar

Appendix A

DUTIES AND RESPONSIBILITIES OF HEAD IT

1. The Head IT will be overseeing all technology operations and conducting routine evaluations of network and data security according to established goals.

2. He will be creating and implementing the VGU's IT policy and best practices to support the implementation of strategies set by the upper management.

3. He will be analyzing the business requirements of all departments to determine their technology needs.

4. He will be locating and seizing chances to enhance and update the software and the systems. He will search constantly for and test new techniques and products.

5. He will coordinate IT Managers, supervise computer technicians and counsel IT staff on various duties and on work-related issues.

6. He will be creating workshops and training programmes for staff. He will be looking for opportunities to train and build teamwork skills.

7. He will be performing routine system audits. He will inspect the use of technological equipment and software to ensure functionality and efficiency.

8. He will be running routine system operations reports and sharing them with top employees.

9. He will be organizing and establishing deadlines for major IT projects such as system updates, migrations, upgrades, configurations and outages.

10. He will be providing a budget to the management, and undertake budget control and forecasting. He will assist in building relationships with vendors and creating cost-efficient contracts.

11. He will attend the necessary meetings, both departmentally and interdepartmentally, to ensure proper communication is fostered to ultimately benefit the operations of the University.

12. He will check the reports filed and the registers maintained.

13. He will ensure that the Local Purchase (LP) of maintenance stores is undertaken by the Procurement Section on priority, so that the repair work can be executed with minimum downtime. Moreover, fast-moving spares are procured in bulk, based on the consumption pattern, and kept in the Central Store.

14. He will assist the Head Procurement to purchase efficient and cost effective technological equipment and software.

For Vivekananda Global University

Registrar

15. He will hire new employees, warn employees when policies are violated, and recommend discharge of employees, when necessary.

16. Offer suggestions to the HR department concerning selection, recruitment, replacement, duty alterations, up-gradation, and so on.

17. Evaluate employees in order to upgrade them when openings arise.

For Vivekananda Global University, Jaipur

Registrar

Appendix B

DUTIES AND RESPONSIBILITIES OF DEPUTY HEAD IT

1. He will take the instructions/directions from the Head IT.

2. Maintaining data security is the prime responsibility of the Deputy Head IT. He will review all security alerts.

3. He will setup logs and review them to monitor possible security breaches.

4. He will maintain backups as needed to recover from deliberate security threats and damage.

5. He will use email security software to protect the VGU's network from email threats in the form of viruses and SPAM.

6. He will draw up the duty rosters. He will organize, supervise, and coordinate the work of IT Managers/Supervisors, and IT Technicians on a day-to-day basis.

7. He will ensure excellence in maintenance and repair work, proper execution of AMC contracts, and regular preventive maintenance to ensure 100% serviceability of all IT resources at all times. He will also prioritize the maintenance requirement to ensure that the downtime of important and critical IT equipment is minimized.

8. He will compile the requirement of maintenance stores from the various maintenance supervisors and project it to the Procurement Department. He will regularly liaise with the Procurement Department for the procurement of fast-moving spares to ensure that the minimum stock balance is maintained at all times, and there are no interruptions in the supply.

9. He will inspect and approve all supply requisitions for the IT Cell, and to maintain par stock, inventory control, and cost-control procedures for all spares.

10. Maintain a time logbook for all employees within the department.

11. He will assign the IT Technicians to the various IT Managers and Supervisors based on their AOR and workload, as also additional assigned tasks.

12. He will collate the Daily Work Sheet of every IT Technician prepared by the various IT Supervisors, based on which the workload and proficiency of each IT Technician will be assessed.

13. He will supervise the discipline and conduct of his entire staff.

14. He will also monitor the progress of the assigned tasks, and make an all-out endeavor to complete them in a reasonable timeframe.

For Vivekananda Global University, Jaipur

Registrar

15. He will personally monitor that all the complaints are attended to by the concerned staff at the earliest. In case, there is an undue delay, he will escalate the complaint to the Head IT for an early resolution.

16. He will keep the Head IT updated on all the important IT management issues.

17. He will assist in training the new employees and upskilling of the existing employees.

18. He will get the stores issued to the various IT Supervisors directly from the Central Store.

19. He will maintain a pool of outsourced third-party contractors, so that in case the maintenance/repair work is beyond the capability of in-house IT Technicians, the same can be outsourced.

20. He will propose amendments to the Head IT to refine the SOP on IT, as and when required.

21. He will ensure proper communication within the department by conducting regular meetings with all personnel.

22. He will ensure that the facial biometric of the new joining faculty or staff is done in the first half of the day of joining.

23. He will act responsibly and reply to each and every mail within 24 hours.

For Vivekananda Global University, Jaipur

Registrar

Appendix C

DUTIES AND RESPONSIBILITIES OF IT MANAGERS/SUPERVISORS

1. One of the nominated IT Managers will officiate as the Head/Deputy Head IT, in case of his/her leave/absence.

2. One of the nominated IT Manager/Supervisor will log onto the email appliance to monitor mail activity with the intent of detecting email threats.

3. The IT Manager/Supervisor will log on to the server remotely to ensure the network's security is effective.

4. The IT Manager/Supervisor will ensure that the network is equipped with a firewall to secure encrypted tunnel for remote users to gain a secure connection from outside the network.

5. The IT Manager/Supervisor will ensure that the network is equipped with content filtering which allows for control of the users internet access to the web. This service is used to monitor user's website visits and block inappropriate websites.

6. They will assist the Head IT in all respect in the full implementation of the SOP on IT, and the instructions issued by the management from time to time.

7. They will be responsible for the complete maintenance and repair works, as also the upgradation of the IT infrastructure and resources at VGU. They will coordinate, monitor and take regular follow-ups in case the work is being executed by an outside agency.

8. Before undertaking any repair/maintenance work, they will coordinate with the Block Marshals and Housekeeping Supervisors, so that other activities/operations are not hampered. They will maintain a close liaison between the maintenance and housekeeping departments.

9. They will check, supervise, and approve the repair/maintenance work carried out by the IT Technicians.

10. They will ensure that all the IT resources are properly maintained and kept in a serviceable condition at all the times.

11. They will assist the IT technicians in their daily difficulties.

12. They will update record books, registers, and files.

13. They will check and report OOO (out-of-order) IT resources, and thereafter, take suitable action to repair it.

For Vivekananda Global University, Jaipur

Registrar

14. They will ensure that all the IT technicians are optimally utilized and adequately tasked for the entire duration of the duty.

15. They will monitor the progress of work assigned to each IT technician.

16. They will mark the attendance of each IT technician, and give a feedback to the Deputy Head IT, in case, someone underperforms or leaves the duty mid-way.

17. They will brief the IT technicians about the location and nature of complaint, likely stores required, and tentative timeframe to complete the repair work, and thereafter, ensure that they are implemented in toto.

18. They will disseminate the next day's workplan, a day prior only, to avoid wastage of precious morning/working hours.

19. They will take daily morning and evening feedbacks from the IT Help Desk Executive about the outstanding complaints, as also important updates on occurrence, from the IT Technicians, Block Marshals and the Housekeeping Supervisors to prioritize work and attend to them swiftly according to the level of urgency.

20. They will carry out random checks during the course of repair work to oversee that the IT Technicians are performing their duties diligently. Any deviation/lapses will be immediately reported to the Deputy Head IT, and suitable rectification/disciplinary action, if required, taken.

21. They will control the stock of tools, equipment, repair materials, and issue equipment and repair materials as per demand.

22. They will also prepare the requisitions for used-up repair materials and new maintenance products for the approval of the Deputy Head IT.

23. They will also ensure that the IT Technicians wear the VGU ID Card around his/her neck all the time.

24. They will promptly act to any IT maintenance complaint received from the IT Help Desk, and depute a team for its early rectification.

25. Immediately report any safety or security hazard to the security department or to the management.

Vivekananda Global University, Jaipur
Registrar

Appendix D

DUTIES AND RESPONSIBILITIES OF IT TECHNICIANS

1. Keep all IT resources fully maintained and serviced.

2. Monitor the work being executed by the AMC operators.

3. Random checking of all IT resources and undertaking preventive maintenance.

4. On receipt of complaint, promptly reaching the site and correctly assessing the scope of repair. Projecting the demand of spares.

5. Perform any maintenance/repair task as per the trade work, as instructed, if within the technical expertise and capability.

6. Notifying IT Managers/Supervisors of necessary repairs. Give periodic feedbacks about the progress.

7. Whenever free, assist other IT team members to complete their trade work.

8. Execute the repair work so well that there is no breakdown in near future.

9. Carry out proper site-clearance after the repairs.

For Vivekananda Global University, Jaipur

Registrar

Appendix E

DUTIES AND RESPONSIBILITIES OF IT HELP DESK EXECUTIVE

1. He will receive complaints on all IT related issues such as maintenance and repairs, replacement, upgradation, relocation etc.

2. He will maintain all the registers kept at the IT Help Desk.

3. He will act as a pivotal person in receiving and disseminating information amongst the IT maintenance staff.

4. He will attend to all the phone calls received at the IT Help Desk, and thereafter, pass on the requirement to the concerned person along with the job card.

5. He will make the entries of job closure once the job card duly signed by the complainant is received. He will also mark all the unattended or partially completed complaints before closing for the day. In case, complainant refuses to sign the job closure, IT Manager after verifying the quality of repair work will confirm to IT Help Desk Executive to close the job card.

6. He will create an Excel Sheet and keep posting it on the WhatsApp Group at 09:30 AM and 01:30 PM every day after fully updating the details of the complaints to escalate the issues.

7. He will put up the complaint register to the IT Manager the next day morning.

For Vivekananda Global University, Jaipur

Registrar

Appendix G

ESCALATION MATRIX FORMAT

Complaint No	Complainant Name	Time	Mob No	Exact Location of Complaint	Exact Nature of Complaint	Addressed/ Redirected To & Time	Completed (Partially / Fully) or Not Attended	Digital Job Card Received or Not	Remark

SUMMARY				
	Carried Forward	Registered Today	Total	Remarks
No of Registered Complaints				
No of Complaints Fully Addressed				
No of Complaints Partially Addressed (With Complaint Nos)				
No of Complaints Yet to be Addressed (With Complaint Nos)				

For Vivekananda Global University, Jaipur

Registrar

Appendix H

IT PROVISIONING/DEPROVISIONING POLICY

1. **Policy Statement**. This document outlines the rules, regulations, and procedures for provisioning and deprovisioning accounts and access rights on VGU IT Systems.

2. **Reason for Policy**. Having a standard provisioning and deprovisioning policy for accounts and access rights for the entire University allows for the adherence to Central, State and local, legal, regulatory, and statutory requirements, as well as minimizes University risk for unauthorized access to University systems, information, and facilities.

3. **The Policy**. All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of University information collected, processed, stored, or transmitted in accordance with the standards outlined in this policy.

4. **Responsibilities**.

(a) President, CEO, Pro Presidents, CA, Vice President, Registrar: -

(i) Are responsible for safeguarding VGU's electronic information and information systems.

(ii) Must ensure that each member of the organization understands the need to protect the University's electronic information and information systems.

(iii) Must communicate this policy to all members of their organization/vertical.

(iv) Must establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance as stated in this Policy.

(b) Deans, COE, Associate Deans, Director CDOE, HoDs and Centres/Cells Heads: -

(i) Are responsible for safeguarding the electronic information and information systems of each business unit in their area of oversight.

(ii) Must ensure that the members of each business unit in their area of oversight understands the need to protect the University's electronic information and information systems.

For Vivekananda Global University, Jaipur

Registrar

(iii) Must communicate this policy to all members of each business unit in their area of oversight.

(iv) Must establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance as stated in this policy.

(v) Must ensure that when the status of an employee within their organization changes (transferred, terminated, or otherwise separated) the appropriate deprovisioning procedure is followed to notify the system owners of the change in authorization to systems for which the employee had previously authorized access.

(c) Information or System Owner Responsibilities, include but are not limited to:

(i) **Provisioning**.

(ai) Establish access control rules appropriate for the classification of information within the system and types of users who will be accessing the system, access rights, and restrictions for specific user roles toward their assets, with the amount of detail and the strictness of the controls incorporating separation of duties.

(aii) Establish and document appropriate logical and physical access controls.

(aiii) Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance as stated in this policy.

(aiv) Provide users and service providers a clear statement of the business requirements to be met by access controls.

(av) Establish formal access authorization procedures to their electronic information and information systems.

(avi) Maintain an inventory of requests for access with pertinent information such as user ID, contact information, etc.

(avii) Perform and comply with the policy requirements relevant to their information systems.

(aviii) Review access entitlements to their information systems as stipulated in this policy or when requested by the IT Cell, and/or audit and advisory services.

For Vivekananda Global University, Jaipur

Registrar

(ii) **Deprovisioning.**

(ai) Review Daily Report and requests from Operational Units/Faculties for those transferred, terminated, or otherwise separated from the University and ensure the access rights to information and assets associated with information processing facilities and services are removed or suspended.

(aii) Upon notification from Deans, HODs or Reporting Officers, remove access as requested for employees who have changed status within each operational unit in their area of oversight.

(aiii) Changes of a user's employment, contract, or agreement should initiate the removal of all access rights that were not approved for the new employment.

(aiv) Access rights removed or adjusted should include those of physical and logical access. Removal or adjustment can be done by removal, revocation, or replacement of keys, identification cards, information processing facilities, or subscriptions.

(av) Documentation that identifies access rights of employees and contractors should include a record of the removal or adjustment of access rights.

(avi) If a departing employee or external party user knows passwords for user IDs remaining active, these should be changed upon termination or change of employment, contract, or agreement.

(avii) Have access rights of employees and external parties to information and information processing facilities reduced or removed before the employment terminates or changes, depending on the evaluation of risk.

(aviii) Have the access rights of all employees and external party users to information and information processing facilities removed upon termination of their employment, contract, or agreement, or adjusted upon change.

(d) The User Responsibilities, include but are not limited to:

(i) Adhere to all policies that govern acceptable use of organizational systems;

(ii) Use the organization-provided IT resources for defined purposes only; and

(iii) Report anomalies or suspicious system behavior.

For Vivekananda Global University, Jaipur

Registrar

Appendix I

INFORMATION SECURITY AWARENESS, TRAINING, AND EDUCATION POLICY

1. **Policy Statement**. This policy establishes the requirement for Information Security Awareness Training for all members of the VGU community who have access to the University's information systems and to information classified as "Critical" or "Restricted" in accordance with the University's security and privacy policies, Central, and State laws, and expectations before access to information or services is granted.

2. **Reason for Policy**. To ensure that the University community is informed and trained on the need for information security and in proper procedures for handling information classified as "Critical" or "Restricted" and the actions to be taken to maintain security and respond to suspected security incidents.

3. **Applicability of This Policy**. This policy applies to all members of the University community.

4. **The Policy**.

   (a) Access to the University's information technology resources is a privilege that requires all individuals with access to Critical or Restricted data to act responsibly and guard against abuses.

   (b) Therefore, both the community as a whole and each individual user have an obligation to abide by the following requirements and responsibilities.

5. **Requirements**.

   (a) President, CEO, Pro Presidents, CA, Vice President, Registrar, Vice President, Registrar must:

      (i) Establish, maintain, and disseminate documentation such as Technology Standards, Procedures, and/or Guidelines to ensure compliance as stated in this policy for the organizations under their purview.

      (ii) Ensure that all members of the University community under their purview, including third party stakeholders (business associates, partners, contractors), that have access to Critical or Restricted data or Privileged Access complete the assigned Security Awareness Training (SAT) upon arrival at the University and the annual refresher thereafter.

   (b) Deans, COE, Associate Deans, Director CDOE, HoDs and Centres/Cells Heads must ensure that business units, schools, and departments, including third party stakeholders (business associates, partners, contractors), under their purview that have access to Critical or Restricted data

For Vivekananda Global University, Jaipur

Registrar

complete Security Awareness Training (SAT) upon arrival at the University and the annual refresher thereafter.

(c) Users with access to University Information Technology Systems, information classified as "Critical" or "Restricted," or with Privileged Access must:

(i) Complete all assigned training related to Information Security Awareness, as well as all mandatory, annual training courses as provided by the University;

(ii) Adhere to all assigned and mandatory training related to Information Security Awareness as provided by the University; and

(iii) Follow all of the University's applicable Information Technology policies, procedures, technical standards, and guidelines.

(d) IT Risk, Policy and Compliance must:

(i) Implement, maintain, and provide on-going information technology security awareness, training and education using various techniques such as awareness sessions, training, newsletter articles, email communication campaigns, and intranet website;

(ii) Review the annual security awareness training content, working with all other relevant parties, to update training content as it pertains to Information Security Awareness topics;

(iii) Provide an activity report to the Deputy Director and Head IT, upon request.

(e) University Ethics and Compliance (UEC) must:

(i) Establish and maintain the University's Security Awareness Training (SAT) program working with all other relevant parties to ensure appropriate content to communicate the aim of information security and the potential impact on the University based on user behavior;

(ii) Ensure SAT is assigned to all members of the University community with access to the University's information technology resources or with access to critical or restricted data or with privileged access upon their arrival at the University or with a job function change and at least yearly thereafter;

(iii) Review the annual SAT content, working with all other relevant parties, to update training content as it pertains to compliance topics.

For Vivekananda Global University, Jaipur

Registrar

Appendix J

INCIDENT REPORTING AND MANAGEMENT

1. **Policy Statement**. This policy establishes responsibility and accountability for ensuring that security incidents are identified, contained, managed, investigated, and remediated.

2. **Reason for Policy**. To establish the requirement that all business and academic units manage security incidents appropriately.

3. **Applicability of This Policy**. This policy applies to all members of the VGU community including faculty, staff, students, covered entities, contractors, non-employees, and agents of the University.

4. **The Policy**.

(a) The actions that may represent a risk to the University's electronic information, information systems, payment account acceptance, and processing methods or information technology infrastructure require a timely response to mitigate the risk to those assets and to the University's business services and operations.

(b) To assist with these efforts, all members of the VGU community must report any suspicious activity, unauthorized access, and missing or stolen equipment. In addition, any damage to VGU's electronic information, information systems, or the information technology infrastructure which includes data services or cloud providers must also be reported. Such security events can negatively impact the confidentiality, integrity, and/or availability of the University's electronic information and information systems and threaten its businesses and overall mission.

5. **Requirements**.

(a) President, CEO, Pro Presidents, CA, Vice President, Registrar must: -

(i) Ensure the implementation of this policy by the organizations under their purview.

(ii) Ensure the support of investigations and remediation of information security events or incidents involving their offices/verticals.

(iii) Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance as stated in this Policy.

(b) Deans, COE, Associate Deans, Director CDOE, HoDs and Centres/Cells Heads must:

For Vivekananda Global University, Jaipur

Registrar

(i) Ensure that each business unit in their respective areas of oversight report security incidents in a timely manner. Unauthorized use, disclosure, loss, or theft of Critical or Restricted information is a potential data breach and needs to be managed via VGU's Policy on Data Breach Management highlighted at **Appendix K**.

(ii) Any unauthorized use, disclosure, loss, or theft of Critical or Restricted information is to be reported to the University Ethics and Compliance Office.

(iii) Ensure that each business unit in their respective areas of oversight report loss or theft of physical assets to the VGU's Security Section.

(iv) Ensure that each business unit in their respective areas of oversight develop, implement, and maintain a departmental Information Security Incident Response Plan, including identification of causes and resolution of weaknesses that may have led to the incident, and ensure that Reporting Officers and IT Cell are aware of and understand the plan.

(v) Ensure that each business unit in their respective areas of oversight maintain their network contact information with IT Cell.

(vi) Ensure that the departments respond and remediate security incidents within the required time constraints as stipulated by the IT Cell.

(vii) Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance as stated in this Policy.

(c) All users must

(i) Report any suspected unauthorized use, disclosure, loss, or theft of Critical, Restricted, or Internal information immediately to their Reporting Officer and the IT Cell.

(ii) Maintain confidentiality of incidents in or pertaining to the University and share information only with their Reporting Officer and IT Cell.

(d) IT Risk, Policy and Compliance must:

(i) Receive and forward incident reports regarding University computers to departments within one business day.

(ii) Advise departments on creation of security incident response plans.

(iii) Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance as stated in this Policy.

For Vivekananda Global University, Jaipur

Registrar

6. This section provides a framework for reporting and managing any major incidents that affect the operations of the IT Systems to include the following: -

(a) Any major incidents affecting the University's information and IT systems.

(b) Loss, disclosure, or corruption of information or devices.

(c) Near misses and information technology concerns.

7. The goal of Incident Management is to restore the IT service to its normal operation and to manage unplanned events which result in disruption of IT services: -

(a) Interruption to the normal operation of an important IT service.

(b) Report or notice of a reduction in the quality of an important IT service.

(c) Failure of a Configuration Item (Cfg-Item) that has not yet impacted an IT service.

8. The aim is to support the prompt and consistent management of any major IT incidents to minimize any harm to IT services/operations of the University and reduce the risk of future breaches of IT services. To this end all users of University IT systems need to: -

(a) Understand their roles in reporting and managing such incidents

(b) Report all actual or suspected incidents immediately on the following contact addresses: itcell@vgu.ac.in , and +91 9460572995 (Shri Jaideep).

9. The policy supporting procedures provide a clear and consistent methodology to help to ensure that actual and suspected major incidents and near misses are: -

(a) Reported promptly and escalated to the right people who can take timely and appropriate action.

(b) Recorded accurately and consistently to assist investigation and highlight any actions necessary to strengthen IT controls.

(c) Only critical IT incidents will be reported through this process, the normal incidents/day by day calls will go through the helpdesk ticketing system.

(d) Maintaining adequate logs and evidence to enable investigation of incidents and preserve the chain of custody where this information is required for legal or evidential purposes.

(e) The University will deploy lawful and proportionate measures to protect information systems by monitoring its IT networks and systems to detect and alert staff in case of system outages.

For Vivekananda Global University, Jaipur

Registrar

10. **Line of Responsibility**. The below is established for critical Incident Management:

(a) The IT team must use the currently approved documented critical incident management process and will be reported, recorded, managed, and appropriately communicated through the approved Incident Management Form.

(b) All members of the IT team are responsible for ensuring the Incident Management Process is followed.

(c) Upon resolution of an incident, the end user will be notified that the incident has been resolved and restored to normal business function.

(d) Once the incident has been resolved, the user will have seven (7) calendar days to reopen the incident.

11. **Compliance & Monitoring**. Incidents will be reviewed on a periodic basis by the Incident Management Process Owner (Head IT/Dy Head IT) to audit for policy compliance. The Head IT/Dy Head IT will monitor and review all information on such incidents and make a regular report to senior management recommending further action and along with issues and risks. This is to ensure that the procedures, guidelines, and standards set forth in the Incident Management Process are adhered to.

12. **Review**. The Incident Management Section will be reviewed: -

(a) Annually, by the Incident Management Process Owner.
(b) Upon an update to the Incident Management Process.
(c) Upon request of the Policy Steering Committee.

For Vivekananda Global University, Jaipur

Registrar

Appendix K

DATA BREACH MANAGEMENT POLICY

1. **Policy Statement**.

(a) The VGU collects information about individuals only if permissible by law and university policy and when it meets appropriate business purposes. It is the university's policy to protect information it receives, handles, and stores in all instances, and to comply with laws pertaining to the safeguarding of Restricted information.

(b) In accordance with this policy and implementing guidelines, the university community must be educated and vigilant about requirements for collecting, retaining and restricting access to information classified as Restricted and identifying potential security breaches (i.e. incidences where information may have been accessed by unauthorized persons), and reporting such security breaches to IT Cell for immediate evaluation and action. The university shall be committed to carefully and expeditiously investigating potential security breaches.

(c) In situations, where notification to potential victims of security breaches is determined to be required by law or otherwise appropriate, the university will do so in the most expedient time possible and without unreasonable delay.

2. **Reason for Policy**. To establish a uniform data breach management and notification process and to ensure University wide compliance with Centre(s) and State's regulatory breach notification obligations.

3. **The Policy**.

(a) **Reporting Security Breaches**. Any unit or individual aware of a potential breach of security containing Restricted information must immediately report the potential breach of security to their Reporting Officer and the Operational Unit Head. To report anonymously, he/she should contact the IT Cell at itcell@vgu.ac.in and mark the mail as **'Security Breach - Need Urgent Attention'**.

(b) **Investigation of Reported Security Breaches**.

(i) Without undue delay, upon receiving notification of a report, the VGU IT Cell will invoke incident response procedures commensurate with the potential breach of security. The VGU IT Cell shall make an initial evaluation and determination if the potential breach of security can be investigated and managed by a single responder. Even when a potential breach of security is investigated by a single responder, all applicable law, regulation and policy will be complied with.

For Vivekananda Global University, Jaipur

Registrar

(ii) If the VGU IT Cell determines a significant breach is possible, the breach shall be referred expeditiously to the Corporate Office, which will constitute a committee Information Protection Evaluation Team (IPET) comprising of the following individuals and representatives of the following offices: -

(ai) Vice President, Corporate Office.

(aii) Senior Faculty Member from Computer Science & Engineering Department.

(aiii) Proctor/Head Security.

(aiv) Deputy Head IT Cell.

(iii) Without undue delay a Chair of IPET shall convene a meeting to expeditiously conduct a factfinding investigation concerning the possible breach of security or compromise of systems. All members of IPET are required to participate in the meeting, but the excused absence of any members should not delay the meeting or the investigation. The IPET is encouraged to speak directly to persons who may have information regarding the matter being investigated (e.g., data owners). The investigation shall conclude without undue delay.

(iv) In conducting its investigation, members of IPET and any others assisting the IPET, may be required to obtain and review Restricted information in electronic or hardcopy format related to the incident. Extreme care and caution should be used to ensure that such information is protected and that there are no further security breaches resulting from the investigation.

(v) During the course of an investigation, the IPET has the authority to provision additional internal or external resources, such as computer forensics, to help determine whether it was possible that an exploit of a vulnerability led to the exposure of Restricted information.

(c) **Report of IPET and Recommendations**.

(i) Without undue delay, upon the conclusion of an investigation, a Chair of IPET shall oversee the preparation and retention of a written report based on the criteria of the regulatory requirements.

(ii) A Chair of IPET shall forthwith submit the written report and recommendation to the President and CEO. The members of IPET shall make themselves available to answer any questions about the investigation and report. A copy of the report will be made available to the Head IT and Operational Unit Head from where the breach occurred, the Head Security, and the Proctor.

For Vivekananda Global University, ...

Registrar

(iii) The Vice President shall make a written final determination regarding notification without undue delay.

(d) **Notification**. Notifications shall meet the breach notification requirements of the IT Act 2000, and the subsequent amendments thereof.

(i) A log of all breaches involving less than 500 individuals will be maintained and monthly submitted to the Corporate Office. For breaches involving 500 or more individuals, notice shall be provided to the individuals.

(ii) Prior to effecting any notification and without undue delay, the IPET with the assistance of Security Staff shall report the breach of security and any information pertaining to the breach to the nearest Police Station by lodging a FIR, and if need be by filing the cybercrime complaint on the National Cyber Crime Reporting Portal for investigating and handling, which may include dissemination or referral to other appropriate law enforcement entities. In cases where notification of more than 1,000 persons at a time is required, the Chair of IPET in conjunction with the appropriate VGU supportive staff shall also provide notification to all consumer reporting agencies that compile or maintain files on consumers on a nationwide basis.

(iii) Units where a potential security breach has been substantiated shall be responsible with other supportive units (e.g. Registrar, Alumni Relations, and Human Resources) for providing the Proctor Office with a list of affected individuals and their current contact information. The Proctor Office will create breach notification letters, which shall be signed by a representative of the Proctor Office and the department head for the unit where the incident occurred. The Proctor Office shall make notifications within the regulatory requirements and without undue delay. The cost of the breach remediation shall be borne by the department where the incident occurred.

(iv) In the case of potential breaches referred to IPET, whether notification is required or not, the Corporate Office will review or consult with the Operational Unit Head to determine whether or not any material weaknesses existed in the controls and processes leading to the breach, and suggest improvements to minimize future events.

(e) **Records Management**. The Head IT shall maintain the records pertaining to each reported incident for a period defined by applicable regulatory requirements. Those records shall include all requirements defined by each applicable regulation.

For Vivekananda Global University, Jaipur

Registrar

Appendix L

EMAIL AND CALENDAR POLICY

1. **Policy Statement**. Having a common email and calendar system, including an email policy, for the entire University promotes collaboration and communications, improves business continuity, and allows for more effective handling and security of data. University Email and Calendaring systems and services supply email, calendaring, and many other collaborative tools in support of the University's mission of education, research, and public service, and to conduct the University's operations. Access to and use of the VGU's Email and Calendaring systems and services is a privilege accorded at the discretion of the University. Use of the University Email and Calendaring systems and services is subject to legal and policy restrictions that apply to all University property and the constraints necessary for the reliable operation of electronic communication systems and services.

2. **Reason for Policy**. The Email and Calendar policy detailed below allows the University to meet Central, State and local, legal, regulatory, and statutory requirements. Therefore, both the VGU community as a whole and each individual user have an obligation to abide by the measures and requirements established within this policy.

3. **The Policy**. All email and calendaring used to conduct University Business must be created, stored, processed, and transmitted via the approved procedures and using the official University Email and Calendaring systems. Forwarding or auto-forwarding of restricted electronic health information (e-PHI) to a non-VGU email service is a violation of University policy.

For Vivekananda Global University, Jaipur

Registrar

Appendix M

IT AUDIT AND MONITORING POLICY

1. **Policy Statement**. This policy is to protect VGU's IT assets, protect information systems from unauthorized activities, and to ensure compliance with applicable laws and regulations and, as needed, to comply with subpoenas, court orders and e-discovery.

2. **Reason for Policy**. To establish an Audit and Monitoring policy for the University's Information Technology environment.

3. **The Policy**.

(a) **Introduction**.

(i) The University maintains information assets that are essential to the University's mission.

(ii) The University has the right and obligation to audit and monitor access to its electronic information, information systems, and information technology infrastructure, some of which are protected by Central and State laws and regulations. It uses the information produced from audit and monitoring activities to protect against, anticipate, and respond to threats to the confidentiality, availability, and integrity of its information assets and to ensure that policies and programs protecting its information assets continue to be effective.

(iii) These activities are not intended to restrict or utilize the content of legitimate academic and business communications.

(b) **Requirements**.

(i) President, CEO, Pro Presidents, CA, Vice President, Registrar, Deans must: -

(ai) Ensure the implementation of this policy by the organizations under their purview.

(aii) Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance with this Policy.

(ii) HODs and Centre/Cell Heads must establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance with this Policy.

(iii) Information Owners must:

For Vivekananda Global University, Jaipur

Registrar

(ai) Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance with this Policy.

(aii) If a security breach event is discovered, adhere to the security requirements outlined in Policy on Incident Management.

(aiii) Identify transactions, events, or activities that are sensitive or critical to the appropriate function of the system or to the information housed in the system that are unlawful, unauthorized, suspicious, or indicative of unusual activity and ensure those actions are appropriately monitored. The actions may include but are not limited to:

(aa) User activities that have not been explicitly authorized;

(ab) Excessive unsuccessful log-in attempts;

(ac) Attempts to use privileges that have not been authorized; and

(ad) Unauthorized modifications to information systems.

(iv) System Owners must:

(ai) Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance with this Policy.

(aii) If a security breach event is discovered, adhere to the security requirements outlined in VGU's Policy on Incident Management highlighted at **Appendix J**.

(aiii) Identify transactions, events, or activities that are sensitive or critical to the appropriate function of the system or to the information housed in the system that are unlawful, unauthorized, suspicious, or indicative of unusual activity and ensure those actions are appropriately monitored. The actions may include but are not limited to:

(aa) All actions undertaken by system administrators who have elevated privileges and access rights;

(ab) User activities that are not explicitly authorized;

(ac) Excessive unsuccessful log-in attempts;

(ad) Attempts to use privileges that have not been authorized; and

For Vivekananda Global University, Jaipur
Registrar

(ae) Unauthorized modifications to information systems.

(aiv) Ensure Audit logs:

(aa) Are retained to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

(ab) Contain sufficient information such that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

(ac) Alert in the event of an audit logging process failure;

(ad) Are protected from unauthorized access, modification, and deletion.

(av) Review the audit logs on a periodic basis, investigating and reporting on unauthorized or suspicious activity.

(avi) Cooperate when dealing with auditors, assisting as needed, and providing documentation that information identified as Critical or Restricted is properly protected when transmitted.

(v) VGU IT Cell must:

(ai) Establish, maintain, and disseminate documentation, such as Technology Standards, Procedures, and/or Guidelines, to ensure compliance with this Policy.

(aii) If a security breach event is discovered, adhere to the security requirements outlined in University Policy on Incident Management.

(aiii) Identify transactions, events, or activities that are sensitive or critical to the appropriate function of the system or to the information housed in the system, that are unlawful, unauthorized, suspicious, or indicative of unusual activity and ensure those actions are appropriately monitored. The actions may include but are not limited to: -

(aa) All actions undertaken by system administrators who have elevated privileges and access rights;

(ab) User activities that are not explicitly authorized;

(ac) Excessive unsuccessful log-in attempts;

(ad) Attempts to use privileges that have not been authorized; and

For Vivekananda Global University, Jaipur

Registrar

(ae) Unauthorized modifications to information systems.

(aiv) Ensure the clocks of all relevant information processing systems are synchronized to a single reference time source.

(av) Ensure Audit logs:

(aa) Are retained to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity;

(ab) Contain sufficient information such that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions;

(ac) Alert in the event of an audit logging process failure; and

(ad) Are protected from unauthorized access, modification, and deletion.

(avi) Review the audit logs on a periodic basis, investigating and reporting on unauthorized or suspicious activity.

(avii) Cooperate when dealing with auditors, assisting as needed, and providing documentation that information identified as Critical or Restricted is properly protected when transmitted.

4. **Non-Compliance and Sanctions**. Failure to comply with this SOP may result in denial or removal of access privileges to the University's electronic systems, disciplinary action under applicable University policies and procedures, civil litigation, and/or civil or criminal prosecution under applicable Central, State and Local statutes.

For Vivekananda Global University, Jaipur

Registrar