VIDYA
VIKAS
MANDAL

INFORMATION TECHNOLOGY POLICY

TABLE OF CONTENTS:

CHAPTER 1

INTRODUCTION

Commensurate with its Mission statement **"We at Vidya Vikas Mandal (VVM) are committed to excellence in education, empowering personalities and developing responsible members of society",** it is the purpose of this Executive Memorandum to set forth this Information Technology Policy of Vidya Vikas Mandal and provide guidance relating to responsible use of its Electronic and Digital Information System.

POLICY STATEMENT

I. This Policy shall be known as the Information Technology Policy

II. Any Information is a critical asset of Vidya Vikas Mandal (VVM). Accurate, timely, relevant, and properly protected information is essential to the success of the VVM's academic and administrative activities, and VVM commits to ensuring that all accesses to, uses of, and processing of VVM information is performed in a secured manner.

III. The Information Technology System plays a major role in supporting the day-to-day activities of VVM. The Information System includes, but shall not be limited to, Infrastructure - networks, hardware, software and data which are used to manipulate, process, transport or store Information owned by the VVM.

IV. This Policy provides a framework in which security threats to VVM's Information System can be identified and managed on a risk basis

V. This Policy establishes terms of reference, which shall ensure uniform implementation of Information security controls throughout VVM.

VI. VVM recognizes that failure to implement adequate information security controls could potentially lead to:

a. Financial loss

b. Irretrievable loss of important data

c. Damage to the reputation of VVM

d. Data theft

e. Piracy of data

f. Legal concerns

VII. This Policy, therefore, provides for measures which will minimize the risk to VVM from any unauthorized modification, destruction or disclosure of data, whether accidental or deliberate.

SCOPE OF THE POLICY

The Information Technology Policy applies to all staff and students of VVM and all other authorized users. VVM expects that all its staff and students observe the highest standards of ethical, personal and professional conduct, comply with its policies, and adhere to its approved codes of practice.

The Information Technology Policy relates to use of the following:

a. All VVM-owned/leased/rented and on-loan facilities.

b. All private systems, owned/leased/rented/on-loan, when connected to VVM network directly, or indirectly.

c. All VVM-owned/licensed data/programs, on VVM and private systems.

OBJECTIVES

The objectives of this Information Technology Policy and any other supporting policies of the VVM shall be to ensure the following:

1. Information shall be created, used and maintained in a secure environment.
2. All of VVM’s computing facilities, programs, data, network and equipment shall be adequately protected against loss, misuse or abuse.
3. All users shall be aware of and fully comply with this Policy and the relevant supporting policies and procedures.
4. All users shall understand their own responsibilities for protecting the confidentiality and integrity of the data they handle.

5. All users shall respect the rights of other IT resource users, the integrity of the physical facilities and controls, and all pertinent license and contractual agreements related to VVM’s Information Systems.

6. All users shall be aware of, and fully comply with, the Information Technology Act, 2000 as amended from time to time.

CHAPTER 2

INFORMATION TECHNOLOGY STRATEGIC PLAN

Vidya Vikas Mandal is of the opinion that its institutions need to become more strategic about technology and develop a master plan which would guide it in the utilization and implementation of technology. Fundamental to the planning process was the goal of developing a strategic plan that aligned with the mission, vision, and culture of the Institutions, as a whole.

This document is a result of that planning process and is intended to serve as the blueprint or road map for the Institution's use of technology during the next five years.

The planning approach required the following steps:

1. Develop a "future state" vision of how the use of Information Technology, in its broadest definition, should add value in support of the Institution's vision, mission and goals.
2. Develop goals and strategies to enable the Institution to move forward toward the desired "future state" in accordance with the guiding principles.
3. Assign responsible persons who will effectively accomplish the specific goals and strategies outlined in the plan.

❖ LEARNING AND TEACHING:

1. Physical and Virtual Leaning Environment
    a. Revised course content on par with current scenario and pool of knowledge
    b. Access to and subscription to online webinars for networking with experts from across the globe
2. Student Information System
    a. Information relating to enrolment, accounts, fees, subject wise details should be available 'on click'
    b. Access to library layout and availability of books/ journals
    c. Pre-order food items in canteen/ Cashless system

- **RESEARCH:**

1. Supporting excellence in Academics
    a. Providing best online platform for better research methods and techniques for the teaching faculty
    b. Availability of resources online through college website portal
2. Support service desk for teaching faculty to raise tickets for obtaining research material online

- **ADMINISTRATIVE APPLICATIONS**

1. Devising methodology in the form of Compliance Manual for the Non-teaching staff to adhere to Compliances (Academic/ Administrative). The Manual shall be provided through Google sheets
2. Access to scanned documents for better search results and reporting
3. A bridge platform to connect all non-teaching staff members through software/ application to share knowledge, better mode of resolving errors and networking

- **SECURITY**

1. Storage backup of data across all Institutions
2. Provide an online architecture of security of the Infrastructure across all Institutions and provide a checklist for implementation
3. Security awareness education- Teaching and Non-teaching staff
4. Protection of data against viruses, worms and other intruders.
5. Implement user and usage authentication measures

CHAPTER 3

PERMITTED USE

1. VVM's Information System shall be used predominantly for VVM's operations, Institutions and related purposes. However, use of the VVM's Information System and resources for personal purposes shall be permitted by the Head of the Institution so long as it conforms to this Policy and does not interfere with VVM's operations or a user's performance of duties as a VVM employee.

2. Staff member shall be permitted to take IT resources outside the campus only on prior specific approval from the Head of the Institution.

3. The following conduct is strictly prohibited
    a. Access, download, printing, storage, forwarding, transmission or distribution of unlawful, obscene, defamatory, libelous, threatening, pornographic, harassing, or hateful material; or
    b. conduct that would be considered a criminal offence, or
    c. conduct giving rise to breach of contract, or break any law, or are otherwise inappropriate by using VVM's Information system

4. NOC: When any faculty or staff member retires or leaves the Institution for whatever reason, she/he shall produce a **No Objection Certificate** from the VVM Network / System Administrator of the institution, on the lines of a No Dues Certificate from the Library.

CHAPTER 4

POLICY ON USE AND MAINTENANCE OF VIDYA VIKAS MANDAL'S IT INFRASTRUCTURE

Computer System and Network

1. The Network/System Administrator shall be responsible for the core VVM network and Bandwidth Management (which includes provision and maintenance of internet facilities: email, web, etc.)

2. The System Administrator shall provide connectivity to each department/Institution, to the gigabit backbone, and also the necessary IP addresses, proxies, email relays, etc.

3. The System Administrator shall be responsible for allocation and control of the available bandwidth to all departments/Institutions of VVM and shall ensure that the appropriate bandwidth is provided depending on the usage requirements of the departments/Institutions. The System Administrator nor any other users shall be permitted to restrict the bandwidth for personal purposes, failing which the Head of the Institution shall take strict action.

4. In cases where additional bandwidth is required by the institution (during workshops, seminars, student events, etc), prior request should be sent by the Head of the Institution to VVM IT Committee well in advance.

5. The installation of hardware/software, setting up and configuration, virus cleaning, maintenance and upkeep of departmental computers shall be the sole responsibility of the respective Instructors/ Departments of the VVM Institutions. In case a particular department cannot perform the task, the System Administrator shall perform this task to ensure that all systems are updated and maintained.

6. If a department network “misbehaves” and causes problems for any other department or the entire campus, or disrupts services, the Head of the Institution shall notify the System Administrator who sequentially shall disconnect the department from the core network until the problem is fixed satisfactorily. The System Administrator shall notify the department (Staff as well as Students) before proceeding with any of such maintenance activities.

7. This Policy prohibits any use of pirated/illegal software. It shall be the responsibility of the Heads of the Institutions and System Administrator to ensure compliance in this regard.

8. A copy of all Software Licenses and their corresponding Keys shall be maintained with Heads of the Institutions of VVM, the designated office staff and concerned Department Head/In-charge.

9. It shall be the responsibility of the System Administrator to ensure that systems in all the departments/Institutions are protected against harmful viruses and other applications that may disrupt the security of the existing networks present in the campus. All departments shall MANDATORILY have, both, authorized antivirus and firewalls setup on the systems and the System Administrator shall ensure compliance.

10. It shall be the responsibility of the System Administrator to document the Network infrastructure of the entire campus for maintenance purposes. All activities such as number of users, number of networks, periodic reports of virus scanning, traffic generated over network, the bandwidth available and its proper allocation etc., shall also be documented and submitted to the Head of the Institution, at the end of each Semester. Diagrammatic Models shall be provided wherever necessary in the documentation.

Administrator Passwords

Admin Passwords for all items listed below will be assigned by the System Administrator/ Lab Instructor and the same shall be shared with the Head of the Institutions

1. Official Email Admin Panel
2. NAS Server
3. Biometrics
4. Server/ Switch/Firewall Administrator
5. Campus Management Software Admin Panel
6. Institutional Website
7. Social Networking pages
8. Photo Copier Machines
9. Institutional Computer Systems
10. Payment Gateway Admin Panel

Official Website and E-Mail

1. Creation and Use: Official Email Ids shall be created/ suspended/ deleted by the System Administrator on official intimation by the Institutional Head/Office. Email ids provided by Mandal / Institution are to be strictly used for official communication only. Email Ids will be provided to staff individually or based on function/position. Email Ids will be in the format ‘function.institutionname@vvm.edu.in’ or ‘username@vvm.edu.in’ where username will be in the form ‘firstname.lastname’. Students, faculty and staff are advised to use email as the preferred mode of communication for administrative as well as academic purposes.

2. Any important documents / notices /orders / circulars, required for circulation, shall be sent through email as an attachment or placed on the web-page. This will significantly reduce the usage of paper and make retrieval of documents simpler.

3. The use of the official Id or the network (both on campus and from remote location) by any user will automatically bind him/her to the Terms and Conditions of ethical use as defined in the IT Policy from time to time. Inflammatory, divisive, abusive and

defamatory messages shall be avoided and shall attract necessary suitable disciplinary action.

4. Closure of account: If any faculty or staff is superannuated or leaves the Institution for whatever reason, his/her user-id will be closed after 2 weeks from the date of retiring/leaving. On notification, such users are responsible for taking a backup of all relevant data within a week of the notification.

5. Safety precaution to be undertaken by users:

   a. Users should avoid opening any mail or attachment that is from unknown or suspicious source. Even if it is from a known source, and if it contains any attachment that is of suspicious nature, user should ascertain its authenticity before opening it. This is to ensure the security of the user's computer, as well as VVM network as such messages may contain viruses.

   b. The user should avoid keeping his/her account open whenever he/she leaves the Computer or device for whatever reason. This could allow misuse of the account for which the authorized user would then be liable.

6. Official Website:

   a. The System Administrator or the person who has been assigned the task shall establish standards for designing and creating web pages considered as being "official" pages of the Vidya Vikas Mandal and its Institutions.

   b. The content to be updated on the website shall be approved by the VVM authority / Head of the Institution. Content shall be reviewed on a timely basis to assure accuracy.

   c. Originators of all web pages using Information System associated with the Vidya Vikas Mandal shall comply with Vidya Vikas Mandal policies and ~~s~~hall be responsible for complying with all applicable laws and regulations including copyright laws, obscenity laws, laws relating to slander and defamation, and laws relating to piracy of software.

Wireless Network:

1. The System Administrator shall be responsible for the management and safety of the WIRELESS NETWORK infrastructure in the VVM Campus.

2. No Devices such as Router, Switch, Access Point, and Software Hotspots which have bearing on Network Security are allowed to be connected to the VVM Network without the prior consent from the System Administrator.

3. All the traffic on the network shall be logged and monitored centrally on the firewall, switches and servers.

4. All logs will be kept on the device as per availability of space on servers.

5. Reports of the sites visited by an individual will be noted, recorded and provided to the VVM / institutional authority on specific request by the Competent Authority.

6. Effort will be made to provide WIRELESS NETWORK everywhere on campus however there might be variations in signal strength and WIRELESS NETWORK coverage shall not be claimed as matter of right by any user.

7. WIRELESS NETWORK will normally be provided for registered VVM users on prior request only. However, it may also be extended to guests visiting VVM Campus on authorization by respective authority in advance.

8. WIRELESS NETWORK may also be temporarily provided at locations where wireless access points exists, for group access to participants attending official Conferences and Seminars etc. on formal request to the Network/ System administrator at least 3 working days in advance of the event by respective authority.

9. WIRELESS NETWORK access to users shall be provided on registering their device with the Network/ System administrator.

10. Any Bona fide Student may register by producing his/her Institution ID card and permission from head of department / institution.

11. Staff may register their laptop for WIRELESS NETWORK access with the System administrator

12. Wireless devices without Antivirus will be denied WIRELESS NETWORK facility. If any virus activity is noticed from a wireless active device, the device will be disconnected from the WIRELESS NETWORK till it is virus free. The individual owner of the device will be solely responsible to clean the device from Viruses.

13. The System administrator will register the Device on WIRELESS NETWORK and is not responsible to rectify networking or software faults arising within the Device during the time of registration.

14. The Device information will be noted and the user will be provided WIRELESS NETWORK access according to validity of admissions.

15. Students will be allowed WIRELESS NETWORK on Laptops and notebook only.

16. Faculty members and staffs of VVM may normally be provided with connections on one approved device (laptop/notebook/tab). In addition, they may normally be permitted to register one personal mobile device if permitted by the competent authority.

17. Laptops purchased under various schemes or projects by the institutions will be registered in the institution's name.

18. The Filtration of sites shall be carried out based on website category. A website category will be decided by the IT Committee of the VVM and the Heads of the institutions.

19. The following category of sites will be permanently blocked.

    a) Pornography

    b) Malicious sites

    c) Proxy Avoidance

    d) Spam URLS

    e) Hate Crimes

    f) Dating

    g) Gambling

    h) Games

    i) Any other site deemed undesirable by the VVM administration from time to time.

20. Users' request for white listing of a particular site should be forwarded through the Head of the institutions. The VVM IT Committee will examine the request.

21. Some sites such as Online Shopping, Entertainment will normally be disabled for all users. But these may be enabled for education purposes, only on prior request.

22. Any deliberate attempt by an individual to bypass the firewall/web-filter through any process / software or to breach firewall or wireless security by any means will be liable for disciplinary action, including debarring from further use of VVM Network.

Installation of Antivirus:

All connected devices at VVM must be installed with antivirus software.

CHAPTER 5

POLICY ON ELECTRONIC CONTENT: STORAGE AND ACCESS

Any Electronic Content (E-Content) created by teachers shall be uploaded on the Network Attached Storage (NAS) Server. The same may be uploaded after converting it into a Read only file if he/she so wishes. Such E-Content shall be available to all authorized users as reference material.

Any user who is desirous of using the e-content uploaded by the creator shall abide by the fair use policy. Fair use of the E-content shall entail giving reference and due acknowledgement to the creator.

Faculty will be responsible to download or upload the content of a particular course that he/she is teaching in a particular semester. While uploading the content, approval has to be obtained from Head of Department / Institution and the norms of content creation or modification are to be strictly followed.

Access to the content will be provided only during the semester and the duration of the course. On completion of the semester, access to the content is denied or disabled.

System administrator would ensure that the data on the NAS server is free of viruses, worms etc.

System administrator will not be responsible for the loss of information due to infection by viruses, worms etc. which is beyond his/her control.

CHAPTER 6

POLICY ON DATA BACKUP AND SECURITY

1. The Administrators so appointed at each Individual Institutions of VVM for handling the Campus Management Software shall be responsible for data back-up from the Software periodically on NAS server.

2. The Exam Committee of Individual Institutions of VVM shall take a backup of data semester wise/ annually on NAS server.

3. The Accountants of Individual Institutions of VVM shall take a backup of Tally Data on daily basis on an External Hard disk provided for the purpose and the NAS server.

4. The Librarians of Individual Institutions of the Mandal shall take a backup of NewGenLib Data on daily basis on an External Hard disk provided for the purpose and the NAS server.

5. The designated office staff belonging to Individual Institutions of VVM shall be responsible for data backup of the Digitized Data on daily basis on the NAS server.

CHAPTER 7

USE/DAMAGING THE INTEGRITY OF VIDYA VIKAS MANDAL'S OR OTHER IT SYSTEMS

This category includes, but is not limited to, the following activities:

1. **Compromising System Security:** Use of systems, networks, messaging systems and internet access is a privilege that may be revoked at any time for inappropriate conduct. Users are expected to act responsibly and respect others. The System Administrator holds the right to conduct surprise Inspection of networks or Internet access for the purpose of security.

2. **Unauthorized access or use:** Users shall not seek to obtain unauthorized access to IT Systems, nor permit or assist any other user in doing the same. For example, a non-Vidya Vikas Mandal organization or individual may not use VVM's IT Systems without specific authorization. Privately owned computers may be used to provide public information resources, but such computers may not host sites or services for non-Vidya Vikas Mandal organizations or individuals across the VVM network without specific authorization.

3. **Disguised use:** Users shall not conceal their identity when using IT Systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

4. **Distributing computer viruses:** Users shall not knowingly distribute or launch computer viruses, worms, or other rogue programs.

5. **Modification or removal of data or equipment:** Users shall not remove or modify any VVM owned or administered equipment or data from IT Systems without specific authorization. Lab Instructors/IT infrastructure users shall be responsible for reporting missing items if any to the Head of the Institution. Any lost and found IT equipment shall be handed over to the Institution's office. Strict action will be taken against violators

CHAPTER 8

ENFORCEMENT PROCEDURES

[Complaints of Alleged Violations] An individual who believes that he or she has been harmed by an alleged violation of this Policy shall file a complaint in accordance with established VVM Grievance Procedures (including, where relevant, those procedures for filing complaints of sexual harassment or of racial or ethnic harassment) for students, faculty, and staff. The individual is also encouraged to report the alleged violation to the System Authority overseeing the facility most directly involved, or to the Principal’s Office, which shall investigate the allegation and (if appropriate) refer the matter to VVM disciplinary and/or law enforcement authorities.

[Reporting Observed Violations] If an individual has observed or otherwise is aware of a violation of this Policy, but has not been harmed by the alleged violation, he or she shall report any evidence to the Systems Authority overseeing the facility most directly involved, or to the Principal’s Office, which shall investigate the allegation and (if appropriate) refer the matter to VVM disciplinary and/or law enforcement authorities.

[Disciplinary Procedures] Alleged violations of this Policy shall be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students as per VVM regulations. The System Administrator may participate in the disciplinary proceedings as deemed appropriate by the relevant disciplinary authority. Moreover, at the direction of the appropriate disciplinary authority, the System Administrator or IT committee is authorized to investigate alleged violations.

[Penalties]Individuals found to have violated this Policy shall be subject to penalties provided for in other VVM policies dealing with the underlying conduct.
Violators shall also face IT-specific penalties, including temporary or permanent reduction or elimination of some or all IT privileges. The relevant disciplinary

authority shall determine the appropriate penalties in consultation with the IT committee.

[Legal Liability for Unlawful Use] In addition to VVM discipline, Users shall be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System, in accordance with the Information Technology (Amendment) Act, 2008.

[Appeals]Users found in violation of this Policy shall appeal or request re-consideration of any imposed disciplinary action in accordance with the appeals provisions of the relevant disciplinary procedures. Incidents that are reported shall attract penalties or punitive action by appropriate authorities constituted by VVM.