VPM's K. G. Joshi College of Arts and N. G. Bedekar College of Commerce, (Autonomous) Thane

Information Technology Security Policy

The purpose of this policy is to provide College employees and students with guidance on acceptable and unacceptable use of the College's Information Technology (IT) resources. Computing, networking, telephony, and information resources at VPM' Joshi Bedekar College, Thane are available to advance education, teaching, research, and administration service missions.

1. Security Measure

- Users of IT resources must not knowingly place the security of information or systems at risk. At all times, Users must: Set a strong password
- Always comply with the Information Security and Data Classification Policy regarding collecting, classifying, labelling, securing, storing, using, copying, transferring, and disposing of information.
- Keep your passwords and pin codes secure and never share them with any individual.
- Take precaution prior to opening any attachment or clicking on links within electronic messages.
- Never use personal e-mail accounts to conduct College business.
- Comply with the College's Local Administrators Policy and never install untrusted software or applications on IT infrastructure or resources.
- Ensure that personally owned devices that may come in contact with IT resources are protected with antivirus software, a personal firewall, and regularly install security updates and patches to operating systems, applications, and web browsers.
- No individual shall knowingly breach, compromise, endanger or threaten the College's IT resources, attempt to do so, or allow others to do so. This includes probing, scanning, assessing, penetrating, or affecting the availability of College IT resources. Users must report any misuse of IT resources to the IT Service Desk, or to the Chief Information Officer. Failure to report misuse may result in the assumption that the User who witnessed the misuse was party to the act.
- VPM' Joshi Bedekar College, Thane reserves the right and responsibility to protect the College and community members from security threats and inappropriate use of IT infrastructure and resources by taking actions, including but not limited to:
- Monitoring computers, mobile devices, systems, networks, services, accounts, web activity, and user activity.
- Denying a user, the right to access IT resources at any time the College deems necessary.

2. Compliance

- Use of the College's IT resources is subject to, and must comply with, all applicable laws and College policies and procedures, including this policy. Non-compliance with applicable laws and regulations may result in civil liability or criminal prosecution. The College reserves the

right to restrict or deny access to its IT resources, to monitor your use of those resources and to take actions it deems necessary or appropriate to protect College IT resources. By using the College's IT resources, Users are confirming agreement with this policy.

- In addition to the above, Users of IT resources must also comply with:
    - Applicable collective agreements, terms and conditions of employment and code of conduct;
    - Copyright Laws including, but not limited to, the sharing of pirated software, audio, and video.
    - Licensing agreements; and
    - Any other agreements between the College and an external service provider.

3. Noncompliance

Noncompliance with this policy may result in any one or combination of the following sanctions:

- Verbal warnings;
- Written warnings;
- Restricted access to, or complete withdrawal of access to IT resources;
- Suspension from work;
- Termination;
- Recovery of costs due to damages or fees; and/or
- Criminal or civil action.

4. Responsibility

- The Chief Information Officer i.e. VPM Management and Server room Personal will review this policy every five years or earlier where required.

IQAC Coordinator	**Principal**
Dr. Pradnya V. Rajebahadur	**Dr. Suchitra A. Naik**