Cybersecurity Measures

The College is committed to ensuring the security and confidentiality of its digital infrastructure, academic systems, and institutional data. To safeguard information assets and protect users from cyber threats, the following cybersecurity measures are implemented:

1. **Secure Access Control:** Access to institutional systems is restricted to authorized users through defined user credentials and role-based permissions.
2. **Strong Password Policy:** Users are required to maintain strong and confidential passwords for accessing college systems.
3. **Firewall Protection:** Network firewalls are deployed to prevent unauthorized access and protect internal systems.
4. **Anti-Virus and Anti-Malware Solutions:** All institutional computers are protected with updated anti-virus and anti-malware software.
5. **Regular Software Updates:** Operating systems and applications are periodically updated to address security vulnerabilities.
6. **Data Backup Mechanism:** Important academic and administrative data is regularly backed up to prevent data loss.
7. **Data Protection and Privacy:** Reasonable measures are taken to protect sensitive and personal data from misuse or unauthorized disclosure.
8. **Monitoring and Incident Response:** IT systems are monitored to identify suspicious activities and respond to cybersecurity incidents promptly.
9. **User Awareness:** Faculty, staff, and students are encouraged to follow safe computing practices and remain vigilant against cyber threats.
10. **Compliance with Guidelines:** The institution follows applicable government and regulatory cybersecurity guidelines from time to time.

The College continually reviews and enhances its cybersecurity practices to maintain a safe and secure digital environment for all stakeholders.