# IT Policy

**Purpose:** The IT Policy outlines NEISSR's guidelines and expectations for the appropriate and secure use of information technology resources. This policy is designed to ensure the confidentiality, integrity, and availability of data, protect against unauthorized access or misuse, and promote responsible and ethical use of IT resources within the institution.

1. **Acceptable Use of IT Resources:**
    - All users of IT resources provided by the institution are expected to use them responsibly, in accordance with applicable laws, regulations, and ethical standards.
    - Users must respect copyright and intellectual property rights, refrain from engaging in illegal activities, and adhere to the institution's policies and procedures related to IT resource usage.

2. **User Account Management:**
    - User accounts and access privileges will be granted based on legitimate business needs and in compliance with the principle of least privilege.
    - Users are responsible for safeguarding their account credentials and should not share them with others. Users must promptly report any suspected unauthorized access or compromised accounts to the IT department.

3. **Data Security and Confidentiality:**
    - Users must protect sensitive and confidential data by following established security protocols, such as using strong passwords, encrypting data when necessary, and utilizing secure file transfer methods.
    - Users should not access, modify, or share data without proper authorization, and should report any data breaches or security incidents to the IT department immediately.

4. **Video surveillance:**
    - Cameras are located at strategic point of the campus, entrance and exit point with a signage. No cameras are hidden from the preview of the students and faculty.

5. **Social Media:**
    - Employees must be aware of responsible usage of social media.
    - The content of the social media is to be edited by the concerned authority before publishing in public domain.

6. **Software and Hardware Usage:**
    - Only authorized and licensed software and hardware should be installed and used on institution-provided IT resources.
    - Users must not engage in unauthorized modification, distribution, or duplication of software, and should adhere to the institution's policies regarding software installation and updates.
7. **Network and Internet Usage:**
    - Users should utilize institution-provided networks and internet access for work-related purposes and refrain from activities that consume excessive bandwidth or pose security risks.
    - Access to inappropriate, offensive, or malicious websites is strictly prohibited. Users should exercise caution when clicking on links or downloading files from the internet to mitigate the risk of malware or phishing attacks.

8. **Mobile Device and BYOD Policy:**
    - Users should comply with the institution's mobile device policy, including guidelines for the secure use of personal mobile devices (BYOD) when accessing institutional resources or handling sensitive data.
    - Lost or stolen mobile devices should be reported immediately to the IT department to initiate appropriate security measures, such as remote wiping of data if necessary.

9. **Data Backup and Disaster Recovery:**
    - Users should regularly back up important data and files to ensure their availability in the event of data loss or system failures.
    - The institution will implement disaster recovery measures to minimize service disruptions and ensure the timely restoration of IT resources in the event of a disaster or system failure.

10. **Compliance and Policy Enforcement:**
    - The institution will regularly review and update the IT Policy to align with changing technologies, regulations, and best practices.
    - Violations of the IT Policy may result in disciplinary action, including but not limited to loss of IT privileges, disciplinary warnings, or legal consequences as applicable.
    - Any concern or complaint about the operation of the system should be addressed to the concerned authority without delay.

By adhering to this IT Policy, NEISSR contributes to a secure and efficient IT environment that protects the institution's data, systems, and resources. The policy ensures compliance with legal

and ethical standards, promotes responsible IT usage, and supports the institution's overall goals and objectives.