Category	Minimum Security Baseline Standards
Password management	Passwords must have a minimum length of 10 characters.
	Passwords must be a combination of alphanumeric characters, special symbols, and mixed case.
	Passwords must be checked against a database of commonly used passwords like password123, qwertyui
	Account lockout must be configured after a maximum of five failed login attempts.
	Default credentials must never be retained for any IT system.
Asset management	Maintain an up-to-date inventory of all IT assets owned by the Institute, including hardware, software, and data.
	All assets owned by the Institute must have a designated owner responsible for their security and management.
	Data classification must be implemented to categorize data as Sensitive, Confidential, Internal or Public.
	All assets owned by the Institute must be classified as Critical or Non-critical, depending on the classification of the data residing in the system and the availability requirements.
	Ensure that all software owned by the Institute - including operating systems and application systems - are appropriately licensed, supported, has automatic updates enabled.
	Inventory of all IT assets that connect to the network, including those that are not owned by the Institute, must be recorded and kept.
	Use private IP addresses for all systems where internet access is not necessary.
User management	All user accounts, including guest accounts, must be created with due approval.
	All users must be allotted a unique ID.
	User accounts must be managed and access reviewed regularly.
	Disable administrative access to users unless a need-assessment is done and approved by the CISO.
	Administrative accounts and Service accounts must be owned by DIGITS personnel or the Department-designated System Administrators only.
	User access deactivation request must be submitted immediately upon the completion of the tenure / project / requirement.
	Accounts inactive for more than 60 days must be disabled.
Access management	All users must be authenticated before accessing any information systems.
	Multi-factor authentication (MFA) is required for accessing sensitive or critical systems, including emails, VPN, cloud-based systems and other systems as deemed necessary by the CISO.

	Access must be granted based on the principle of least privilege and need-to-know basis.
	Implement SoD (Segregation of Duties) principle for critical functions to prevent malevolent activity without collusion.
Network security	Deploy firewalls and intrusion detection/prevention systems (IDS/IPS) to monitor and control incoming and outgoing network traffic.
	Ensure only secure and necessary network services can be accessed from outside the Institute's network.
	Firewall rules must be configured to deny all inbound traffic by default.
	All requests for external connectivity must be accompanied by the approval of the respective Dean, and will also be reviewed and approved by the CISO.
	All firewall rules must be reviewed and revalidated at least once a year. Firewall rules that are no longer necessary must be disabled.
	Network should be properly segmented, with separate VLANs for different functional requirements.
	Communication between different VLANs should be denied by default and only be allowed specifically on basis of need with necessary restrictions on ports / applications / hosts.
	Use network segmentation to isolate sensitive or critical systems from other areas of the network.
	Disable all unencrypted protocols such as Telnet, and use secure protocols such as SSH, SSL, or IP Security (IPSec) encryption for all remote connections to routers/switches/servers.
	Implement VPNs for secure remote access to internal networks.
	Implement protection against Denial of Service / Distributed Denial of Service attacks.
	Monitor/Block the communication to malicious IPs and Domains regularly shared by CERT-In and other threat intelligence.
	Deploy proxy servers and allow access for internet for clients through proxy server only.
	Implement Media Access Control (MAC) address binding for all systems/IT devices.
	Implement Network Access Control for authentication before providing network access, including for guest devices. Systems that do not meet the posture compliance must be placed in a separate VLAN.
WiFi security	Communication between client and Wireless Access Points (WAP) must be secured using WPA-2 or higher level of encryption.
	Configure separate guest WLAN for internet access to guests.
Endpoint security for organisation owned assets	Install and maintain anti-malware and endpoint detection and response (EDR) solutions on all endpoints.

	Install host firewall to control and log all inbound and outbound activities.
	Ensure that all devices have up-to-date security patches, firmware updates, and operating system updates.
	Enforce device encryption for all laptops, desktops, and mobile devices accessing sensitive data.
	Disable the use of external storage devices (e.g., USB drives) unless approved.
	Systems must be configured to lock after maximum 15 minutes of inactivity.
Activity logging	All devices placed within the network should have logging enabled.
	All authentication events must be logged.
	All IT systems must use DIGITS-defined Network Time Protocol Server.
	Logs must always contain the original client IPs.
	Logs must be retained for a minimum of 180 days.
Data protection	Ensure encryption of sensitive data both at rest and in transit using industry-standard encryption protocols.
	Implement regular backups of critical data. The frequency of the backup must be in mutual agreement with the Data Owners.
	Verify the integrity of the backups at least once a year.
	Securely dispose of data, devices, and media that are no longer needed, ensuring all sensitive data is irrecoverable.
Application security	Conduct security assessments of applications, including vulnerability scans and penetration testing, before deployment and periodically thereafter.
	Conduct security assessments of applications, including vulnerability scans and penetration testing, before deploying any major changes to applications.
	Keep all software, applications and libraries up-to-date with the latest security patches.
	All internet-facing web applications must be protected through a Web Application Firewall, with rules appropriately configured allow-listing and deny-listing model.
	WAF can be deployed in monitoring mode during initial implementation to observe traffic patterns without blocking legitimate requests. WAF rules must be switched to blocking mode at the earliest.
	Regularly update the WAF with the latest threat signatures to detect known vulnerabilities and attack patterns.
	Leverage behavioural analysis and anomaly detection to identify zero-day vulnerabilities or unknown attack vectors.

Mobile app security	Conduct security assessments of mobile applications, including vulnerability scans and penetration testing, before deployment and periodically thereafter.
	Conduct security assessments of mobile applications, including vulnerability scans and penetration testing, before deploying any major changes.
	Mobile applications must implement SSL Pinning to prevent man-in-the-middle attacks.
	No secret keys used by the application should be stored unencrypted in the application storage.
	User data should not be stored in unencrypted/plain-text form on the device.
	The final build of the application must not contain any test code and all debug logs must be disabled.
	Obfuscation of the code by packers, encryptors and related tools must be implemented.
	Only permissions required for essential functionality of the application must be sought from the user.
Cloud Security	Use encryption for data stored in the cloud and implement access controls to manage cloud access securely.
	Regularly review third-party cloud service providers for compliance with contractual security obligations.
	Implement controls to prevent inadvertent public access of storage accounts.
Email security	Scan all emails, attachments, and downloads on the mail gateway.
	Implement Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) and Domain-Based Message Authentication Reporting & Conformance (DMARC).
Patch management	All software and hardware patches on critical systems must be deployed within 14 calendar days.
	All software and hardware patches on non-critical systems must be deployed within 60 calendar days.
	All patches must be deployed after due testing.
Vulnerability management	All critical systems must be scanned for vulnerabilities at least once a month.
	All non-critical systems must be scanned for vulnerabilities at least once in six months.
	All critical systems must undergo Penetration Testing at least once a year.
	All non-critical systems must undergo Penetration Testing at least every two years.
	All vulnerabilities with CVSS Score equal to more than 7.0 must be closed within 14 days for critical systems and 60 days for non-critical systems.
IT outsourcing	Wherever any IT activity is outsourced, it must be ensured that the contract specifies the information security requirements, and the same are complied with.

	The following information security requirements should be documented as part of the contract: i. General policy on information security. ii. Procedures to protect organisational assets. iii. Restrictions on copying / disclosure. iv. Controls to ensure return of information/assets in their possession at the end of the contract. v. The right to monitor and the right to terminate services in the event of a security incident or a security breach. vi. Right to audit contractual responsibilities or to have the audits carried out by third parties. vii. Arrangements for reporting, notification and investigation of security incidents and breaches.
	Access to Institute's IT systems for third parties must be shared only after signing of an Non-Disclosure Agreement.
	Information security audit report of the vendor must be made available to the Institute on periodic basis or when required.
	Detailed list of all components of the software (including open source) / solution in the form of Software Bill Of Material (SBOM) shall be provided by the vendor. Vendor is also responsible for informing any identified vulnerabilities in the system to the Institute within reasonable time period.
	Data collected and processed by the vendor should be protected appropriately and made available to the Institute as and when required.
	Third party personnel must comply with the information security policies, processes and procedures of the Institute.
	Any third party found in violation to this policy shall be subjected to termination of contract and/ or will be handled as per applicable laws, rules & regulations.
Social media security	Official social media platform accounts access should be restricted and limited to the designated officials and systems only.
	Do NOT use personal email account for operating official social media account.
	MFA must be enabled for all official social media accounts.
	All official social media accounts must be configured as verified wherever possible.
MFD security (printers, scanners, photocopiers)	Disable default services like FTP, HTTP, SSH, SMB, Telnet, etc that would not be necessary.
	Configure NTP on office printer, enable logs and monitor.
	Restrict internet access for all printers.
	Ensure remote administration of printer with secure connection only .

	Ensure printer firmware is updated to the latest available from OEM. Firmware update/upgrade/patch must only be downloaded from OEM website.
Physical Security	Restrict physical access to sensitive areas such as data centres, server rooms, and labs to authorised personnel only.
	Implement environmental controls, including fire suppression, temperature control, and uninterruptible power supply (UPS) system for locations where servers are placed.
	Monitor access to physical spaces using surveillance cameras and access logs.
Security Awareness and Training	Conduct mandatory security awareness training for all faculty, staff, researchers, students, interns and contractors at onboarding and at least once every three years thereafter.
	Promote security awareness through regular communications, such as campaigns and newsletters.
	Provide specialised training for individuals handling sensitive data or managing critical systems.
	Ensure that all third-party personnel who have access to Institute's IT resources also undergo annual trainings.
Incident Response	Establish SOPs for commonly observed information and cyber security incidents.
	Maintain logs of all security incidents and conduct post-incident reviews to improve response and preventive measures.
	Establish and validate a Cyber Crisis Management Plan for responding to high-impact incidents.
Audit and Compliance	Ensure compliance with applicable legal and regulatory security requirements, including data protection laws.
	Conduct regular security audits and vulnerability assessments to ensure compliance with the MSBS.
	Address audit findings promptly, and track remediation efforts until completion.
	Maintain records of audits and compliance assessments for accountability and future reference.