SVKM'S NMIMS®
Deemed to be UNIVERSITY

Cyber Security Policy

NMIMS has a well-defined Cyber Security policy. This policy is applicable to all staff members (teaching, non-teaching, and third parties), students, independent contractors, suppliers, partners, and anybody else who has access to NMIMS's networks, data, or information systems. It includes any hardware, software, and networks that the NMIMS own, use, implement, or control.

Table of Contents

1. Objective

This cybersecurity policy aims to provide guidelines, principles and procedures to ensure the confidentiality, integrity and availability of the information systems, data and assets belonging to the Deemed University "Narsee Monjee Institute of Management Studies (NMIMS)", its affiliated educational institutions and its stakeholders. The purpose of this policy is to protect sensitive information, maintain privacy of personal data and mitigate cybersecurity risks.

2. Roles and Responsibilities

- Chief Information Security Offer (CISO) in concurrence with Senior management is in charge of developing the organization's overall cybersecurity strategy, and fostering a climate of security awareness among all employees.
- The IT & Security departments (CISO) are in charge of implementing and maintaining technical security controls, keeping an eye on systems, performing risk analyses, controlling access privileges, and responding to security incidents.
- All employees and students have a duty to abide by this policy, report security events, and take part in cybersecurity awareness and training programs.

3. Security Measures & Actions

We use FortiGate NGFWs firewalls in our Network Infrastructure, The Unified Threat Protection (UTP) and the Enterprise bundles licenses which includes the FortiGuard services such as FortiCare Support, Firmware & General Updates, Intrusion Prevention, Antivirus, Web & Email Filtering, SDWAN and Cloud Sandbox .It gives us comprehensive protection against known and unknown threats (e.g., ransomware, malicious botnets, zero-day, and encrypted malware). Firewalls policies are reviewed with regular interval. Following security measures are taken regularly.

- Access Control: Access is granted based on job roles and responsibilities, such as Students, Staff and Faculty. Regular access reviews are conducted every year. We are using "Captive Portal" for user to browse the Internet and that facilitates the management of access by users in the wireless network.
- Network Security: Firewalls, intrusion detection and prevention systems, and secure network configurations are implemented to protect against unauthorized access, external threats, and network vulnerabilities.
- Network Segmentation: Network segmentation is implemented to divide the organization's network into separate segments, based on security requirements, and to restrict lateral movement within the network. This helps contain potential breaches and limit the impact of security incidents.
- A Web Application Firewall (WAF) is implemented to protect web applications and websites from common security threats, such as SQL injection, cross-site scripting (XSS), and other application-layer attacks. The WAF is be configured to provide continuous monitoring, detection, and mitigation of web-based threats, and regular updates and maintenance of the WAF is regularly conducted to ensure optimal security posture.
- Endpoint & Malware Protection: All devices and systems are having up-to-date antivirus software, malware protection, and regular scanning and updates to prevent and detect malware infections. We are using Symantec Endpoint Protection software suite which provide us comprehensive endpoint security and protection. The suite includes advanced malware protection, application control, exploit

prevention. We ensure that all detections are mitigated, cleaned and reported. We ensure to have latest update of Virus signatures.

- Email Security: We are using Microsoft 365 cloud services as an email service including Spam Email Filter. All the spams with critical level are handled by Administrator.
- Data Encryption: We have implemented all our communication between Applications over Internet by HTTPS and TLS 1.1 minimum. User data is encrypted internally as well while communicating with Intra applications.
- Incident Response: We have communicated process and dedicated email id through which Incidents are reported to IR team by all stakeholders. Incident Response team then perform Investigation and Root Cause Analysis (RCA) and different Mitigation, Containment and Remediation applicable case to case are done and recorded for future references.
- Security Monitoring: We have enforced security rules on firewalls to monitor and filter incoming and outgoing traffic. We are manually monitoring security threats and proactively work on events alerts emails generated by Security devices.
- Security Testing: We perform Security Audits (VAPT) by Third Party experts for network infrastructure, applications (Web, Mobile), SAP. These audits are Black box and Grey box in nature. We follow up with stakeholders for mitigation of the findings and outcome of these audits. As of today there is zero Critical vulnerability exist in our infrastructure. We share dashboards with stakeholders for visibility on security posture.
- Patch Management and Security Updates: We perform patch management by combination of automatic and manual as and when necessary for assets that are susceptible to cyberattacks, helping us to reduce overall security risk.
- Printing Security: We are using HP Secure Managed Print Services that adds extra layers of security. Print sensitive documents to shared printers without security worries and reduce waste from accidental and forgotten print.
- Physical Security: We have at each campus and locations implemented security cameras and access control gates operated by smart cards with biometrics such as face and thumb impression. Control Centers are monitored by Security personnel 24by7.

4. Security Awareness and Training

Regular security awareness and training programs are conducted for employees, students, and other stakeholders to promote a culture of cybersecurity. These include educating them about threats, best practices, policies, and procedures related to information security.

We take following actions for training and awareness:

- Regularly organize training for staff on cybersecurity best practices & Awareness.
- Publish and communicate Cyber Security Newsletters every month to all staff.
- Sharing information time to time on Global security incidence/Zero day/Vulnerability, etc. with all Staff.

5. Compliance and Audit

Periodic security audits, vulnerability assessments, and risk assessments of Network, Applications, Data & IT Assets are conducted to evaluate the effectiveness of security controls, identify vulnerabilities, and ensure compliance with relevant laws, regulations, and industry standards.

We perform security audits, vulnerability assessments, and risk assessments of Network, Applications, Data & IT Assets by qualified third party experts duly selected by CISO and Management team.

6. Policy Review and Revision

This cybersecurity policy is reviewed and updated periodically as necessary to reflect changes in technology, evolving threats, regulatory requirements, and organizational needs. Reviews involves key stakeholders, Higher management representative's and also incorporate lessons learned from security incidents and audits.

7. Policy Change and versioning

Ver	Date	Section	Action	Changes	by
1.1	31 Aug 2023	Security Measures & Actions	Entire Cybersecurity Policy reviewed for changes and released.	Updated all necessary sections	CISO /Higher Management
	31 Aug 2023			Reviewed	IT- Director / Dy. Director
				Maintained	CISO

REGISTRAR
SVKM's NMIMS
V L Mehta Road,
Vile Parle (West),
Mumbai-400 056

Checked by:
Bhushan Kulkarni
Deputy Director IT

Verified by:
Deepak Gursahani
Director IT

Approved by:
Ashish Daptardar
Register

SVKM'S NMIMS
MUMBAI 56