BHARATIYA VIDYA BHAVAN'S
SARDAR PATEL INSTITUTE OF TECHNOLOGY
(Empowered Autonomous Institute Affiliated to University of Mumbai)
[Knowledge is Nectar]
Department of Computer Science Engineering

Course - Ethical Hacking

UID	**2022301002** **2022301012** **2021300101**
Name	**Viraj Bhalerao** **Sanket Pingale** **Adwait Purao**
Class and Batch	**TE COMPS (B) Batch B**
Date	**27/04/2024**
Experiment	**10. Cyber Security Policies**
Aim	**Design the Cyber Security Policies to help the cyber security auditor**
Policy	**Internet Of Things Policy**
Theory	**IoT Security Policy Checklist** **1. Device Authentication** • Is there a documented procedure for authenticating IoT devices before connecting to the network? • Are strong authentication mechanisms (e.g., certificates, biometrics) enforced for device authentication? • Are default credentials disabled or changed upon device deployment? **2. Data Encryption** • Is all data transmitted between IoT devices and endpoints encrypted using strong encryption algorithms? • Are secure communication protocols (e.g., TLS) employed for data encryption? • Is data encryption enforced both in transit and at rest? **3. Access Control** • Is there a defined process for managing access to IoT resources and data? • Are access control lists (ACLs) or role-based access control (RBAC)

	used to restrict access based on user roles? • Is access to sensitive IoT functionalities or data restricted to authorized users? **4. Firmware and Software Updates** • Is there a policy for regular updates to device firmware and software? • Are updates tested in a controlled environment before deployment to production? • Is there a mechanism in place to ensure timely patching of known vulnerabilities? **5. Network Security** • Are IoT networks protected using firewalls, intrusion detection/prevention systems (IDS/IPS), and network segmentation? • Is network traffic monitored for anomalies and unauthorized access attempts? • Are IoT networks segmented to isolate critical assets and reduce the attack surface? **6. Physical Security** • Are physical access controls in place to prevent unauthorized access to IoT devices and infrastructure? • Are physical security measures (e.g., locks, access control systems) implemented to safeguard IoT assets? • Is there regular monitoring of physical security controls to detect and address vulnerabilities? **7. Data Privacy** • Are policies established for collecting, storing, processing, and sharing IoT data in compliance with privacy regulations? • Is explicit consent obtained from users for data collection and processing activities? • Are measures in place to protect the privacy of IoT data throughout its lifecycle? **8. Incident Response** • Is there an incident response plan for detecting, reporting, and responding to security incidents involving IoT devices? • Are roles and responsibilities defined for incident response team members? • Are regular drills and exercises conducted to test the effectiveness of the incident response plan?

	9. Vendor Security Assurance • Are security assessments conducted when selecting IoT vendors or suppliers? • Are security requirements included in contracts and agreements with vendors? • Is vendor compliance with security standards and best practices monitored regularly?
Conclusion	Thus, we have successfully learned about Cyber Security Policies and also defined Policies for Internet of Things Policy.