Wockhardt’s Cybersecurity Policy

Original

1. Introduction

At Wockhardt pharmaceutical, we are committed to maintaining the highest standards of cybersecurity to protect the confidentiality, integrity, and availability of our information assets. As a leading pharmaceutical company, we recognize the critical importance of safeguarding sensitive data, systems, and networks from evolving cyber threats. This Cybersecurity Policy outlines our commitment to implementing robust security measures and establishes guidelines for the responsible use and protection of digital assets.

2. Objective

The objective of this policy is to ensure the confidentiality, integrity, and availability of our Pharma IP, digital assets and the Operational Technology (OT) assets through the implementation of effective cybersecurity controls and practices. We aim to mitigate the risk of cyber threats, unauthorized access, data breaches, and other malicious activities that may compromise our assets.

3. Scope

This policy applies to all employees, contractors, vendors, and third parties who have access to Wockhardt Pharma's digital systems, networks, and information assets. It encompasses all aspects of cybersecurity.

4. Policy Guidelines

4.1. Information Security and Data Protection

a. **Data Classification**: All data shall be classified based on its sensitivity and criticality, and appropriate security controls shall be implemented to protect it.

b. **Access Controls:** Access to systems, applications, and data shall be granted based on the principle of least privilege, ensuring that users have only the necessary access rights.

c. **Data Encryption:** Sensitive data shall be encrypted during storage, transmission, and processing to protect it from unauthorized disclosure or tampering.

d. **Data Backup and Recovery:** Regular data backups shall be performed, and recovery procedures shall be in place to ensure the availability and integrity of critical data.

4.2. Network and System Security

a. **Firewall and Intrusion Prevention Systems**: Robust network firewalls and intrusion prevention systems shall be deployed to protect against unauthorized access and network-based attacks.

b. **Patch Management:** Regular patching and updates shall be applied to all systems, applications, and devices to address known vulnerabilities and protect against exploits.

c. **Malware Protection:** Up-to-date antivirus and anti-malware solutions shall be deployed on all endpoints and servers to detect and prevent malware infections.

d. **Network Segmentation**: Networks shall be segmented to restrict access and contain potential security breaches.

Ranked # 1 in Healthcare
GREAT PLACE TO WORK® Best Companies to Work for 2015 India

4.3 Security Operations Center (SOC) Monitoring

a. **Continuous Monitoring:** Wockhardt shall maintain a 24/7 SOC to monitor and detect potential cybersecurity incidents, unauthorized access attempts, and suspicious activities across our network and systems.

b. **Threat Intelligence:** The SOC shall leverage threat intelligence feeds and tools to proactively identify emerging threats and vulnerabilities, allowing for timely mitigation and response.

c. **Log Management and Analysis:** Logs from various security devices, servers, and applications shall be collected, analysed, and correlated to identify potential security incidents, anomalies, and patterns of malicious activity. Logs shall be retained as per Compliance requirement.

4.4. Incident Response and Recovery

a. **Incident Reporting:** All employees shall promptly report any suspected or detected security incidents to the security team.

b. **Incident Response Plan:** An incident response plan shall be established, outlining procedures for identifying, containing, and mitigating security incidents**.**

c. **Response Automation and Workflow Management:** Wockhardt shall leverage Security Orchestration, Automation, and Response (SOAR) capabilities to automate routine security tasks, streamline incident response processes, and enhance operational efficiency.

d. **Playbook Development**: Incident response playbooks shall be created and regularly updated to ensure standardized and effective response to various security incidents.

e. **Forensic Investigation:** In the event of a security breach, a thorough forensic investigation shall be conducted to determine the cause, extent of impact, and prevent future occurrences.

f. **Lessons Learned:** After each incident, a post-incident review shall be conducted to identify areas for improvement and update incident response procedures accordingly.

g. **Disaster Recovery: D**isaster recovery plans shall be developed and regularly tested to ensure the timely recovery and resumption of critical operations in the event of a disruption.

4.5 User and Entity Behavior Analytics (UEBA)

a. **User Behaviour Monitoring**: UEBA solutions shall be employed to analyse user activities, detect anomalies, and identify potential insider threats, compromised accounts, or unauthorized access.

b. **Baseline Establishment**: User behaviour baselines shall be established to establish normal patterns and detect deviations that may indicate security risks or malicious activities.

4.6. Vulnerability Assessments (VA)

a. **Schedule and Scanning:** Wockhardt Pharmaceutical shall conduct regular vulnerability assessments on its systems, applications, and infrastructure using industry-standard tools and methodologies.

b. **Patch Management**: Identified vulnerabilities shall be prioritized and remediated through effective patch management processes.

Original

Ranked # 1 in Healthcare
GREAT PLACE TO WORK® Best Companies to Work for 2015 India

4.7. Employee Awareness and Training

a. **Security Awareness Training:** All employees shall undergo cybersecurity awareness training to educate them about security risks, best practices, and their responsibilities.

b. **Password Security**: Strong password practices, such as complex passwords and regular password changes, shall be enforced to protect user accounts.

4.8. Third-Party Security

a. **Vendor Management:** Security requirements shall be incorporated into contracts with third-party vendors and suppliers to ensure the protection of our systems and data.

b. **Risk Assessment:** Third-party vendors shall undergo a risk assessment to evaluate their security controls and ensure they meet our standards.

4.9. Compliance and Regulatory Requirements

a. **Regulatory Compliance**: Wockhardt shall comply with all applicable laws, regulations, and industry standards concerning data protection and cybersecurity.

b. **Security Audits and Assessments**: Regular security audits and assessments shall be conducted to evaluate the effectiveness of our cybersecurity measures and identify areas for improvement.

By adhering to this policy, Wockhardt Pharma demonstrates its commitment to safeguarding Pharma IP, maintaining robust cybersecurity practices, and protecting sensitive information from unauthorized access, disclosure, and tampering.

This Cybersecurity Policy shall be reviewed periodically to ensure its effectiveness and relevance

End of the document

Original

Ranked # 1 in Healthcare GREAT PLACE TO WORK® Best Companies to Work for 2015 India