CLEAN DESK AND DIGITAL WORKSPACE POLICY

Redback Operations

Version	Modified By	Approver	Date	Changes made
1.0	Devika Sivakumar		04th August 2024	Initial Policy Creation

Contents

1. SCOPE

This Clean Desk and Digital Workspace Policy applies to all participants involved in Redback Operations, including students, mentors, tutors, and unit chairs. The policy is particularly focused on the Cybersecurity Team, including SecDevOps, GRC, Blue Team, Red Team, and Infrastructure Team members, as well as leaders, co-leaders, and mentors across all projects. This policy covers all digital and physical workspaces, with a special emphasis on the secure management of virtual machines (VMs), tools such as Suricata, MQTT, SIEM, Wazuh, and Nagios, and the use of Deakin University's VPN for remote access.

2. PURPOSE

The purpose of this policy is to ensure the smooth and secure operation of Redback's projects by protecting sensitive information, promoting a professional and organized workspace, and minimizing the risk of data breaches. This policy supports the integrity, confidentiality, and availability of Redback's data and digital environments, with particular attention to the operations of the Cybersecurity Team.

3. OBJECTIVES

The objectives of this Clean Desk and Digital Workspace Policy are to:

- **Enhance Security Posture:** Protect sensitive information from unauthorized access, particularly within digital workspaces.
- **Promote Operational Efficiency:** Ensure that workspaces, both physical and digital, are organized, secure, and conducive to productivity.
- **Ensure Regulatory Compliance:** Align with data protection laws, software licensing agreements, and internal security policies.
- **Support Incident Management:** Reduce the likelihood and impact of security incidents through robust workspace practices, particularly in digital environments.

4. DEFINITIONS

Term	Definition
Sensitive Information	Data that must be protected from unauthorized access, including project data, participant information, and security logs.
Clear Desk	A physical workspace free of sensitive or confidential information when not in use.
Clear Screen	A digital device screen that is locked or logged off when not in use to prevent unauthorized access.
Digital Workspace	The virtual environment in which participants interact with digital tools, applications, and data, including VMs, cloud services, and remote connections.
Virtual Machine (VM)	A software-based emulation of a computer system that provides the functionality of a physical computer.
VPN (Virtual Private Network)	A secure network connection that allows remote users to access Redback's internal resources securely.

5. General Guidelines for Digital Workspace

- **Clear Screen Requirement:** All digital devices (laptops, desktops, VMs) must be locked when unattended to prevent unauthorized access. Screens should be positioned to prevent unauthorized viewing.
- **Password Management:** Use strong, unique passwords for all systems, applications, and VMs. Passwords must be changed regularly and should not be shared.
- **Data Encryption:** Sensitive information stored on local devices, VMs, or during transmission must be encrypted using company-approved encryption tools.

- **Secure File Storage:** Files should be stored on secure company servers or approved cloud services, not on local devices, to ensure data integrity and security.
- **Software and Application Usage:** Only approved software and applications, including VMs and security tools like Suricata, MQTT, SIEM, Wazuh, and Nagios, may be used. All software must be regularly updated to protect against vulnerabilities.

6. Specific Guidelines for Cybersecurity Team

Use of Deakin University VPN

- **Secure Connection:** All members of the Cybersecurity Team must use the Deakin University VPN to securely access Redback's internal resources, VMs, and security tools such as Wazuh and Suricata.
- **Access Control:** Access to sensitive resources through the VPN must be restricted to authorized personnel only. Regular audits should be conducted to ensure compliance.
- **Data Transmission:** All data transmitted over the VPN must be encrypted, ensuring the confidentiality and integrity of sensitive information.

Virtual Machines (VMs) and Security Tools

- **VM Usage:** The Cybersecurity Team must ensure that all VMs are securely configured, regularly updated, and monitored for security incidents. VMs should be isolated from personal devices and used solely for Redback Operations.

- **Suricata and MQTT:** Team members using Suricata and MQTT must ensure secure configurations, with regular monitoring and alerting for potential threats. Suricata should be implemented in a way that supports intrusion detection and prevention across the network, while MQTT must be securely managed for IoT-related communication.

- **SIEM and Wazuh Implementation:** SIEM tools, along with Wazuh, must be configured to monitor, detect, and respond to security incidents in real-time. Logs should be aggregated and analyzed for potential security threats, with regular reports generated for review.

- **Nagios and Blue Team Operations:** The Blue Team, under the leadership of Devika Sivakumar, must ensure that Nagios is securely implemented within VMs for monitoring system health and detecting anomalies. Endpoint security measures should be enhanced, and regular vulnerability assessments should be conducted.

Pentesting and Red Team Activities

- **Simulated Attacks:** The Red Team, led by MD Samsul Kabir, must conduct regular penetration testing using the VMs to identify vulnerabilities within Redback's digital infrastructure. All findings must be documented and communicated to relevant teams for remediation.

- **Tool Security:** All pentesting tools must be securely configured and isolated within dedicated VMs to prevent accidental exposure of sensitive data or tools.

Logging and Monitoring

- **Continuous Monitoring:** Tools like Suricata, SIEM, and Nagios should be configured to provide continuous monitoring of all critical systems. Alerts should be set up to notify the relevant team members immediately in case of any detected anomalies or potential breaches.

- **Incident Response:** In the event of a detected security incident, there should be a clearly defined incident response plan that involves all relevant sub-teams. The plan should include steps for isolating affected systems, investigating the root cause, mitigating the threat, and documenting the incident for future reference.

7. Digital Workspace Procedures for Remote Work

- **Secure Home Office Setup:** Home office setups must be secure, with company-provided VPNs used for accessing Redback's network, VMs, and security tools. Sensitive work should be conducted on VMs, not on personal devices.
- **Public Wi-Fi Precautions:** Avoid using public Wi-Fi for work tasks. If necessary, use a secure VPN to access VMs and other resources.
- **Device Security:** Ensure that all devices used for remote work, particularly those connecting to VMs and security tools, are secured with strong passwords, encryption, and are regularly updated with security patches.

8. Compliance and Monitoring

- **Regular Audits:** Conduct regular audits to ensure compliance with this policy across all teams and projects. These audits should include checks on software usage, VM security, and adherence to secure digital workspace standards.
- **Monitoring Tools:** Utilize monitoring tools, such as Suricata, SIEM, and Nagios, to continuously monitor VM and network activity, ensuring real-time detection of potential security threats.
- **Reporting Violations:** Participants are required to report any violations or concerns regarding this policy to their respective team leader or the IT department immediately.

- **Disciplinary Actions:** Non-compliance with this policy may result in disciplinary actions, including verbal or written warnings, and in severe cases, involvement of academic authorities.

9. Roles and Responsibilities

Role	Responsibility
Participants	Adhere to the policy and maintain secure digital workspaces. Report any security incidents or policy violations immediately.
Team Leaders and Mentors	Enforce the policy within their teams. Conduct periodic checks and support participants in understanding and complying with the policy.
IT Support	Provide tools, support, and guidelines for secure digital workspace practices. Ensure all devices and systems, including VMs, are configured according to security standards.
Security Team	Develop, review, and update the policy. Conduct regular audits and provide training to ensure compliance. Lead incident response and remediation efforts.

10. Team-Specific Responsibilities

- **SecDevOps Team (Lead: Candice Smith):** Implement secure development practices, ensuring that all software and applications, particularly in VMs, comply with security standards.
- **GRC Team (Lead: Rohit):** Ensure compliance with regulatory requirements and internal policies, conducting regular risk assessments focused on digital environments.
- **Blue Team (Lead: Devika Sivakumar):** Monitor and defend against potential threats in the digital workspace, focusing on Nagios, SIEM, and Wazuh implementations in VMs. Ensure endpoint security and reporting capabilities are up to date.
- **Red Team (Lead: MD Samsul Kabir):** Test and assess the security posture through simulated attacks, particularly within VMs. Provide feedback for strengthening defenses.

- **Infrastructure Team (Lead: Drew Baker):** Ensure the digital infrastructure, including VMs and cloud services, supports secure operations and adheres to the policy standards.
- **Cybersecurity Mentor (Daniel McAulay):** Oversee the integration of cybersecurity practices across all teams. Ensure continuous improvement of security measures, particularly in digital workspaces.

11. Review and Updates

This policy will be reviewed annually and updated as necessary to reflect changes in technology, business practices, or regulatory requirements. Reviews will be initiated by the Chief Information Security Officer (CISO-The Acting Director of the company/ Cybersecurity Lead/Mentor) in collaboration with team leaders.

12. Key Assets and Data Categories

IT Assets:

- Personal Laptops (Windows, Linux)
- Cloud Services (approved by the IT department)
- Company servers, VMs, and data storage solutions
- Suricata, MQTT, SIEM, Wazuh, and Nagios monitoring systems

Data Categories:

- Project-specific data (e.g., VR SunCycle, Elderly Wearable Technology, Athlete Wearable Technology, Player Tracking, BugBox)
- Cybersecurity data (e.g., security logs, incident reports, VM configurations, monitoring data from Suricata, MQTT, SIEM, Wazuh, and Nagios)
- Participant data (e.g., access logs, user credentials, compliance reports)

13.Framework References

This policy aligns with recognized standards and best practices, including:

- **ISO 27001:2022 Controls:** Covering access control, operations security, network security management, and secure software development practices.
- **CIS Controls:** Encompassing inventory and control of software assets, secure configuration, continuous vulnerability management, audit log management, and incident response.

Conclusion

This Clean Desk and Digital Workspace Policy provides a comprehensive framework for securing both physical and digital workspaces at Redback Operations. By adhering to this policy, participants contribute to a secure, compliant, and efficient working environment, ensuring the integrity and security of Redback's operations, particularly within the digital realm used extensively by the Cybersecurity Team.

Appendix

For additional guidelines and best practices, refer to the following resources:

- Australian Signals Directorate - Guidelines for System Hardening

(Australian Signals Directorate, Guidelines for System Hardening, May 12, 2024)