APPLICATION CONTROL POLICY

Redback Operations

Version	Modified By	Approver	Date	Changes made
1.0	Devika Sivakumar		06th August 2024	Initial Policy Creation

Contents

1. SCOPE

This Application Control Policy applies to all participants within Redback Operations, including students, mentors, tutors, and unit chairs. The policy is particularly relevant to the Cybersecurity Team, encompassing sub-teams such as SecDevOps, GRC, Blue Team, Red Team, and Infrastructure Team. It also extends to all project-based teams working on initiatives such as VR SunCycle, Elderly Wearable Technology, Athlete Wearable Technology, Player Tracking, and BugBox. The policy covers all digital environments, including virtual machines (VMs), cloud services, and various tools used for project work and cybersecurity operations.

2. PURPOSE

The Application Control Policy establishes a framework for managing, approving, and monitoring the software applications used within Redback Operations. This policy aims to prevent unauthorized or malicious software from being used, thereby protecting the integrity of the digital environment and ensuring compliance with internal and external security standards. By enforcing controlled application usage, this policy supports the secure execution of all project and cybersecurity activities.

3. OBJECTIVES

The objectives of this Application Control Policy are to:

- **Enhance Security Posture:** Safeguard Redback Operations against the risks posed by unauthorized or malicious software.
- **Ensure Compliance:** Align with legal, regulatory, and internal security standards related to software usage.
- **Maintain Operational Integrity:** Ensure that only authorized and tested applications are used, preserving the stability and reliability of digital environments.
- **Support Incident Response:** Provide clear procedures for handling incidents involving unauthorized applications.

4. DEFINITIONS

Term	Definition
Application Control	A security measure that restricts the execution of unauthorized software to mitigate risks associated with malware and other security threats.
Whitelisting	The practice of allowing only pre-approved software applications to be executed within the digital environment.
Blacklisting	The process of blocking known malicious or unapproved software from being executed.
Virtual Machine (VM)	A software-based environment that emulates a physical computer, allowing users to run applications and perform tasks in an isolated digital space.
Critical Applications	Software that is essential for the execution of specific project tasks, cybersecurity operations, or overall organizational activities.

5. GUIDING PRINCIPLES

Principle	Description
Security	Protect the digital environment by ensuring that only secure and authorized software applications are used.
Compliance	Adhere to applicable regulations, internal policies, and industry standards related to software management and control.
Operational Efficiency	Ensure that the application control measures support productivity without compromising security.
Transparency	Maintain clear documentation and processes for the approval, management, and monitoring of applications.

6. APPLICATION CONTROL PROCEDURES

Application Approval and Whitelisting

1. **Application Submission**: Participants who require new software for their tasks must apply request to the IT Support Team or Security Team. The request must include the application's name, purpose, source, and justification for its use.

2. **Evaluation Criteria**: The IT or Security Team will evaluate the requested application based on:

    - **Security**: The application's security features, such as encryption, patch history, and vendor reputation.

    - **Compatibility**: Compatibility with existing systems, VMs, and digital environments.

    - **Compliance**: Adherence to licensing agreements, regulations, and internal policies.

    - **Operational Need**: The application's relevance to the project or task at hand.

3. **Approval Process**: Upon successful evaluation, the application will be approved and added to the whitelist, allowing it to be installed and executed within Redback's digital environment.

4. **Whitelisting Management**: The whitelist of approved applications will be maintained by the IT Support Team and reviewed periodically to ensure it remains up-to-date and relevant.

Blacklisting and Unauthorized Applications

1. **Identifying Threats**: Any application identified as malicious, unauthorized, or irrelevant to project work will be added to the blacklist by the Security Team. This includes applications flagged during monitoring, audits, or by third-party security advisories.

2. **Blocking Execution**: Blacklisted applications are automatically blocked from being executed on any system within the Redback digital environment, including VMs and personal devices used for project work.

3. **Responding to Violations**: If an attempt to execute a blacklisted or unauthorized application is detected, the incident must be reported immediately to the Security

Team. The involved system will be isolated, and an investigation will be conducted to determine the cause and impact.

Continuous Monitoring and Logging

1. **Application Monitoring**: The Security Team must continuously monitor application usage across all systems, VMs, and digital environments. This includes monitoring the installation, execution, and update activities of all applications.

2. **Log Management**: All application-related activities must be logged, including successful and unsuccessful attempts to install, execute, or update applications. These logs will be integrated into the SIEM (Security Information and Event Management) system for real-time analysis and long-term storage.

3. **Anomaly Detection**: The SIEM system will be configured to detect anomalies, such as attempts to run unauthorized software, unusual patterns in application usage, or potential security breaches. Alerts will be generated and reviewed by the Security Team.

Software Updates and Patching

1. **Regular Updates**: All approved applications must be kept up to date with the latest security patches and updates. The IT Support Team is responsible for scheduling and applying these updates across all relevant systems.

2. **Controlled Rollout**: Before deploying updates or new applications, they must be tested in a controlled environment, such as a dedicated VM, to ensure compatibility and security. Only after successful testing will the updates be rolled out to the broader digital environment.

3. **Patch Management**: A patch management schedule will be maintained, ensuring that all critical updates are applied promptly, and that legacy applications are reviewed for potential security risks.

7. APPLICATION USAGE IN SPECIFIC TEAMS

SecDevOps Team

- **Development Tools**: All development tools, IDEs (Integrated Development Environments), and CI/CD (Continuous Integration/Continuous Deployment) pipelines must be approved through the whitelisting process. Regular code reviews and security scans must be conducted using approved tools.

- **Containerization**: Any containers or containerized applications must be built using approved base images, and all containers must be scanned for vulnerabilities before deployment.

GRC Team

- **Compliance Tools**: All tools used for governance, risk management, and compliance activities must adhere to regulatory requirements. The GRC Team must ensure that only compliant software is used, and that all usage is documented for audit purposes.

Blue Team

- **Defensive Tools**: Tools such as SIEM, Wazuh, Nagios, and endpoint protection software must be carefully configured and regularly updated to protect the environment. The Blue Team is responsible for monitoring these tools and ensuring they operate within approved parameters.

Red Team

- **Pentesting Applications**: All penetration testing tools must be pre-approved and isolated within dedicated VMs. The Red Team must document all activities and ensure that no residual data or tools are left behind after testing.

- **Tool Security**: Red Team tools must be securely stored, with access restricted to authorized participants. Any new tools or updates must go through the standard approval process before use.

Infrastructure Team

- **Infrastructure Management Tools**: All tools used for managing servers, VMs, network devices, and cloud services must be approved and configured securely. The Infrastructure Team is responsible for ensuring that these tools do not introduce vulnerabilities into the environment.

- **Patch Management**: The Infrastructure Team must coordinate with the IT Support Team to ensure that all infrastructure-related applications and tools are kept up-to-date and secure.

Compliance and Auditing

- **Regular Audits**: The Security Team must conduct regular audits to ensure compliance with the Application Control Policy. Audits will include a review of the application whitelist and blacklist, an analysis of logs, and a check for unauthorized software.

- **Policy Violations**: Any violation of the Application Control Policy, whether intentional or unintentional, must be reported immediately. Consequences for violations may include restricted access to systems, additional training, or disciplinary action, depending on the severity.

8. ROLES AND RESPONSIBILITIES

Role	Responsibility
Participants	Adhere to the policy, use only authorized applications, and report any issues or violations immediately.
IT Support Team	Manage the application whitelist and blacklist, handle approval requests, apply updates, and monitor compliance.
Security Team	Monitor application usage, conduct regular audits, manage incident response, and maintain SIEM integration for application control.
Team Leaders and Mentors	Ensure that participants understand and comply with the Application Control Policy and support the approval process for necessary tools.
CISO	Oversee the application control framework, ensure alignment with security goals, and lead the review and update process for the policy.

9. REVIEW AND UPDATES

This policy will be reviewed annually, or as needed based on changes in technology, security threats, or project requirements. The CISO will initiate reviews in collaboration with the IT Support and Security Teams, ensuring the policy remains relevant and effective.

10. KEY ASSETS AND DATA CATEGORIES

IT Assets:

- Laptops (Windows, Linux)
- Virtual Machines (VMs)
- Cloud Services and infrastructure
- SIEM, Wazuh, Nagios, and other monitoring tools

Data Categories:

- Project data across various teams (e.g., VR SunCycle, Elderly Wearable Technology)
- Application usage logs and security incident reports
- Compliance records related to software usage

11.FRAMEWORK REFERENCES

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

- **ISO 27001:2022 Controls:** Covering secure software management, access control, and operations security.
- **CIS Controls:** Addressing secure configuration, continuous vulnerability management, audit log management, and incident response.

CONCLUSION

This Application Control Policy is designed to ensure that Redback Operations maintains a secure and compliant digital environment. By controlling the software applications used within the organization, this policy supports the secure execution of projects and cybersecurity operations, while protecting against unauthorized or malicious software.

APPENDIX

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

- Australian Signals Directorate - Application Control Strategies

(Australian Signals Directorate, Guidelines for Application Control, May 12, 2024)