**Week 3 Written Assignment**

Ayomide Stephen Oyedele

EC-Council University

**CIS 300: Fundamentals of Information Systems Security**

Dr. Franklin Orellana

January 28, 2024

**Richman Investments Remote Access Control Policy Definition**

Richman Investments, as a global investment and consulting firm, recognizes the critical importance of implementing a robust remote access control policy to safeguard its IT infrastructure. This policy aims to establish a secure and efficient framework for remote access to systems, applications, and sensitive data. As the company expands its operations globally, it becomes imperative to ensure consistent access controls across all offices while prioritizing security and compliance.

This policy covers all employees, contractors, and third-party vendors requiring remote access to Richman Investments' IT resources. The scope encompasses desktops, mobile computers, and wireless devices used by the 5,000 employees distributed across eight North American offices.

**ACCESS CONTROLS:**

**Systems Access Control:**

Authentication Mechanism:

* Use multi-factor authentication (MFA) for all remote access.
* Implement strong password policies and regular password updates.

Authorization:

* Define role-based access controls (RBAC) to ensure that users have the minimum necessary permissions.
* Maintain a centralized identity management system for efficient user provisioning and de-provisioning.

**ENDPOINT SECURITY:**

Enforce the use of company-approved and regularly updated security software on remote devices.

Require endpoint compliance checks before granting access.

**Applications Access Control:**

Role-Based Access Controls (RBAC):

* Define roles based on job responsibilities and grant access permissions accordingly.
* Regularly review and update access rights based on employee roles.

Single Sign-On (SSO):

* Implement SSO to streamline and simplify user access to multiple applications.
* Enhance security by integrating SSO with MFA.

Application Whitelisting:

* Restrict applications to a predefined whitelist, preventing unauthorized applications from running on remote devices.
* Regularly update and review the application whitelist.

**DATA ACCESS CONTROL:**

Encryption:

* Enforce end-to-end encryption for data in transit, especially for sensitive applications and information.
* Implement data encryption on remote devices to protect data at rest.

Data Classification:

* Classify data based on sensitivity and assign access controls accordingly.
* Implement strict controls on the access and sharing of sensitive data.

Logging and Monitoring:

* Enable comprehensive logging for remote access activities.
* Regularly monitor logs for suspicious activities and conduct periodic audits.

**CONNECTIVITY:**

Virtual Private Network (VPN):

* Utilize VPN technology to establish secure and encrypted connections for remote access.
* Implement split tunneling to ensure that only traffic destined for the corporate network goes through the VPN.

**JUSTIFICATION:**

* The chosen access controls align with industry best practices and address the specific needs of Richman Investments:
* MFA and RBAC ensure a layered defense against unauthorized access.
* SSO enhances user experience without compromising security.
* Application whitelisting prevents malicious applications from compromising systems.
* Encryption safeguards data during transmission and storage.
* VPNs establish secure connections for remote access.

**ENFORCEMENT AND COMPLIANCE:**

Violations of this policy may result in disciplinary action, including termination, legal action, and loss of access privileges. Regular audits and compliance checks will be conducted to ensure adherence.

**REVIEW AND REVISION:**

This policy will be reviewed annually and updated as needed to address emerging threats, technological advancements, and changes in business requirements.

Richman Investments' remote access control policy establishes a comprehensive framework to protect the company's IT infrastructure, ensuring secure and efficient remote access. By implementing these controls, Richman Investments aims to strike a balance between enabling global collaboration and safeguarding sensitive information.

References:

1. NIST. (2020). NIST Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. National Institute of Standards and Technology.

2. Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30. National Institute of Standards and Technology.