Project#3: System Security Plan (Field Office)

[Author’s name]

[Institute’s name]

Information System Security Plan

**1. Information System Name/Title:**

 Red Clay Renovations Company’s Information Technology Security Program (ITSP)

**2. Information System Categorization:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| System Name | Confidentiality | Availability | Integrity | Interconnection |
| ITSP | High | Moderate | Low | Moderate |

**3. Information System Owner:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Title | Agency | Address | Email Address | Phone Number |
| Natalie Randell | Chief of Staff | Red Clay Renovations Company | 12 High Street Wilmington, DE 19801 | nr@redclayrenovations.com | 910-555-2152 |

**4. Authorizing Official:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Name | Title | Agency | Address | Email Address | Phone Number |
| Anthony Morgan | Chief Information Officer (CIO) | Red Clay Renovations Company | 12 High Street Wilmington, DE 19801 | Morgan\_Anthony@redclayrenovations.com | 910-555-2150 |

**5. Other Designated Contacts:**

|  |  |  |  |
| --- | --- | --- | --- |
| Title | Address | Email Address | Phone Number |
| Chief Information Security Officer (CISO) | 12 High Street Wilmington, DE 19801 | William\_Spenser@redclayrenovations.com | 910-555-2149 |
| Information Systems Security Office (ISSO) | 12 High Street Wilmington, DE 19801 | Julia\_Smith@redclayrenovations.com | 910-555-2153 |

**6. Assignment of Security Responsibility:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Title | Address | Email Address | Phone Number |
| William Spenser | CISO | 12 High Street Wilmington, DE 19801 | William\_Spenser@redclayrenovations.com | 910-555-2149 |

****7. Information System Operational Status:****

The operational status of the information technology system of the company is recognized as the single prospect of Systems Development Lifecycles. It is noteworthy to mention that currently the organization of Red Clay Renovations Company currently does not have plans of system upgradation in the forms of major modification and under development.

 ****8.0 Information System Type:****

The core application of the company’s information technology system can be observed in the case of the approach of risk management. Currently, the company of Red Clay Renovations Company is facing immense risk hazards that require the adoption of a suitable information management system. Proper handling of cybersecurity is established as the major functional approach of information systems for the company.

****9.0 General System Description/Purpose****

The central function of the overall information security system is to successfully contribute to the overall forms of risk management strategies adopted by the company. The active role of the IT security program of the company is important to meet the standards of security controls under the domain of FIPS 199/200 standards. The development of proper interconnections between different company’s field offices is another core perspective under the domain of IT systems. The updating functions of the company’s information system can also be observed in the remodeling of the use of “smart home” and “Internet of Things” technologies. The application of these technological advances is helpful to approach to develop a better connection between different security protection domains.

****10. System Environment****

The technical system of the company consisted of different interrelated technological forms. The technical factors for the company can be observed under the domain of managed or enterprise. This perspective is useful in case of an extensive agency system that is comprised of operational domains in case of different field offices. The application of hardware and software configurations plays a critical role in ensuring necessary forms of information system management between different workstations and servers.

           The approach of primary hardware is further disseminated mainly in the forms of processor, primary data storage, secondary storage, input and output instruments. The functioning approach of hardware for the IT management system can also be considered in the forms of laptops and firewalls. It is noteworthy to mention that the purpose of considering processing in the form of the laptop is to successfully crafted and compile different networking reports. On the other hand, the focus of the approach of firewalls is to provide necessary protection to the security from various external resources.

           The approach of software is another crucial aspect associated with the overall form of the technical system of the company. The perspective of software is used by the company for multiple reasons and practical applications. Diverse options of software are under consideration under the domain of software technology services. The option of software can be mainly observed in the case of Windows 10, Microsoft Office, Adobe Acrobat Reader, Adobe Flash Player. The core aim of all these software approaches is to ensure successful technical applications. Windows 10 is recognized as the preferred operating system that prevailed in the case of an information management system of the company. All the computers or servers are the brand of Dell manufacturing organization.

           Identification of communication equipment is also a critical condition to enhance overall understanding in the form of a technical system that prevails in the organization. Communication networking is a necessary condition to align operations of different fields under the domain of collective business objectives. The domain of internet services is characterized as the central form of communication networking that builds the necessary connection between different stakeholders. Telephones, fax machines, pager, etc. are characterized as the main forms of communication devices utilized by the technical information department of the organization.

****11. System Interconnections/Information Sharing****

The approach of interconnection/information sharing is used by the IT department of the company to develop the necessary connection between different operational networks. The central aim of the perspective of interconnections is to establish a direct interaction between two or more IT systems with the concern of distributing necessary information resources. It is crucial to indicate that the main Operations Center and the individual Field Offices are connected through the domain of the Internet via a business-grade Internet Services Provider. This approach of interconnection is adopted through the consideration of the standard Service Level Agreement (Bowen, Hash, & Wilson, 2007). The main form of interconnections considered in the forms of Virtual Private Network associations between the Operations Center and the required form of Field Office. The approach of VPN is used by the information security department to meet the objectives of protecting the confidentiality and integrity of information. The individual network infrastructure is implemented in case of field office that is observed considering domains of wireless local area network, wireless access points, switches, firewall, and intrusion assessment system.

The broader spectrum of Verizon Business services provided the services mainly in the forms of Wide Area Networking (WAN) and internet services. These spectrums of interconnection services explicitly define the overall network connections of the company. It is also significant to mention that the organization of Red Clay Renovations Company has its Active Directory server, multiple Web servers, Email Servers, Print Servers, and overall databases. All these approaches eventually played their role in the overall form of interconnections.

****12. Related Laws/Regulations/Policies****

Consideration and application of significant and relevant legal perspectives are necessary practical conditions to ensure better forms of integrity and confidentiality of important information. Legal practice is adopted by the field officer operational domain to attain useful information under the proper regulations. The security plan for the company is developed under the legal spectrum of the Privacy Act that prevails in the country. The operations are under control considering the legal approach of the Sarbanes-Oxley Act of 2002. This legal spectrum is considered by the management to determine the legal spectrum in case of a business approach (Swanson, Hash, & Bowen, 2006). The legal spectrum in case of operations of field center also actively linked with proper processing, storing, and transmission of Protected Health Information (PHI) considering the strict legal compliance of the HIPPA Security Rule.

 ****13. Minimum Security Controls****

           Application of suitable forms of security controls is necessary to condition to meet the standard of information system security plan for the company. The approach of security controls associated with the three main forms of management controls, operational controls, and technical controls (Swanson, Hash, & Bowen, 2006). The selection of the most appropriate form in the form of a control family is an essential practical measure to define the entire spectrum of the security control system.

 **13.1 Management Controls**

Management controls are developed to ensure the successful management of the information systems and the proper management of the entire risk prevails for the information system. It is significant to indicate that there are some aspects of technologies that are catered through the overall domain of management controls.

**13.1.1 [first control family]**

**CA: Security Assessment and Authorization (Management Controls Category)**

|  |  |  |
| --- | --- | --- |
| CA-1  | Security Assessment and Authorization Policies and Procedures  | CA-1  |
| CA-2  | Security Assessments  | CA-2 (1)  |
| CA-3  | System Interconnections  | CA-3 (5)  |
| CA-5  | Plan of Action and Milestones  | CA-5  |
| CA-6  | Security Authorization  | CA-6  |
| CA-7  | Continuous Monitoring  | CA-7 (1)  |
| CA-9  | Internal System Connections  | CA-9  |

Authorization is necessary condition to meet the objectives of developing necessary interconnection between different systems. This approach also helps to meet the objective of significant assessment considering the perspective of internal system connections between different system security activities (Force & Initiative, 2013). The desired plan of action can only be achieved through the development of proper security evaluation plan.

**13.1.2 [second control family]**

**PL: Planning (Management Controls Category)**

|  |  |  |
| --- | --- | --- |
| PL-1  | Security Planning Policy and Procedures  | PL-1  |
| PL-2  | System Security Plan  | PL-2 (3)  |
| PL-4  | Rules of Behavior  | PL-4 (1)  |
| PL-8  | Information Security Architecture  | PL-8  |

Appropriate planning is one crucial spectrum of the entire domain of information security system adopted by the company. Alignment of different and interconnected policy and procedures is necessary condition to attain the significant objectives and consideration from the overall system.

**13.2 Operational Controls**

Security methods are addressed under the main perspective of operational controls. The central aspect of consideration is to examine different mechanisms that are developed and established by concerned individuals. The option of operation controls is selected to enhance the overall performance of the security plan.

**13.2.1 [first control family]**

**SI: System and Information Integrity (Operational Controls Category)**

|  |  |  |
| --- | --- | --- |
| SI-1  | System and Information Integrity Policy and Procedures  | SI-1  |
| SI-2  | Flaw Remediation  | SI-2 (2)  |
| SI-3  | Malicious Code Protection  | SI-3 (1) (2)  |
| SI-4  | Information System Monitoring  | SI-4 (2) (4) (5)  |
| SI-5  | Security Alerts, Advisories, and Directives  | SI-5  |
| SI-7  | Software, Firmware, and Information Integrity  | SI-7 (1) (7)  |
| SI-8  | Spam Protection  | SI-8 (1) (2)  |
| SI-10  | Information Input Validation  | SI-10  |

Protection of improper information modification is necessary condition to achieve the ultimate objective of system integrity. Adoption of family control class in the form of system and information integrity is essential instrument to safeguard the entire spectrum of all the relevant policy and procedures.

* + 1. **[second control family]**

**AT: Awareness and Training (Operational Controls Category)**

|  |  |  |
| --- | --- | --- |
| AT-1  | Security Awareness and Training Policy and Procedures  | AT-1  |
| AT-2  | Security Awareness Training  | AT-2 (2)  |
| AT-3  | Role-Based Security Training  | AT-3  |
| AT-4  | Security Training Records  | AT-4  |

The operational control family in the form of Awareness and Training (AT) is also selected in case of system security operations of the company. The central aim of this form of consideration is to provide necessary form of knowledge to all the shareholders effectively and efficiently. The objective of security awareness needs to be successfully implemented by offering different systematic aspects and practical considerations. The objective of individual accountability is also contained through the different classes under the domain of awareness and training.

**13.3 Technical Controls**

All the matters of security executions are addressed under the spectrum of technical controls set for the selected information management system. The application of computer systems is established through the practical idea of technical controls (Nieles, Dempsey, & Pillitteri, 2017). The main focal point of this form of controls is to ensure the successful application of automated protection in case of unauthorized access or improper use of information. It also provides aid to the overall security considerations.

* + 1. **[ first control family]**

**AC: Access Controls (Technical Controls Category)**

|  |  |  |
| --- | --- | --- |
| AC-1  | Access Control Policy and Procedures  | AC-1  |
| AC-2  | Account Management  | AC-2 (1) (2) (3) (4)  |
| AC-3  | Access Enforcement  | AC-3  |
| AC-4  | Information Flow Enforcement  | AC-4  |
| AC-5  | Separation of Duties  | AC-5  |
| AC-6  | Least Privilege  | AC-6 (1) (2) (5) (9) (10)  |
| AC-7  | Unsuccessful Logon Attempts  | AC-7  |
| AC-8  | System Use Notification  | AC-8  |
| AC-11  | Session Lock  | AC-11 (1)  |
| AC-12  | Session Termination  | AC-12  |
| AC-14  | Permitted Actions without Identification or Authentication  | AC-14  |
| AC-17  | Remote Access  | AC-17 (1) (2) (3) (4)  |
| AC-18  | Wireless Access  | AC-18 (1)  |
| AC-19  | Access Control for Mobile Devices  | AC-19 (5)  |
| AC-20  | Use of External Information Systems  | AC-20 (1) (2)  |
| AC-21  | Information Sharing  | AC-21  |
| AC-22  | Publicly Accessible Content  | AC-22  |

The option of control family in the form of control access is selected for the operational domain of company on its location of Wilmington. The central aim of this form of consideration is to eliminate the option of improper use of different system resources concerning the connection between different interconnected systems. The prospect of access makes decisions about the accessible form for different entities in case of system-based access controls.

* + 1. **[ second control family]**

**IA: Identification and Authentication (Technical Controls Category)**

|  |  |  |
| --- | --- | --- |
| IA-1  | Identification and Authentication Policy and Procedures  | IA-1  |
| IA-2  | Identification and Authentication (Organizational Users)  | IA-2 (1) (2) (3) (8) (11) (12)  |
| IA-3  | Device Identification and Authentication  | IA-3  |
| IA-4  | Identifier Management  | IA-4  |
| IA-5  | Authenticator Management  | IA-5 (1) (2) (3) (11)  |
| IA-6  | Authenticator Feedback  | IA-6  |
| IA-7  | Cryptographic Module Authentication  | IA-7  |
| IA-8  | Identification and Authentication (Non-Organizational Users)  | IA-8 (1) (2) (3) (4)  |

Timely and successful exploration of all the aspects of authentication policy and procedural domain is necessary condition to meet the standards of technical control domain of the system. This form of defense mechanism is important to eliminate different risks of data theft or concerning the approach of system security. This form of control system eventually helps system control stakeholders to ensure successful form of authentication.

**14. Information System Security Plan Completion Date:**

The completion data of information security plan is 17th of November, 2019

**15. Information System Security Plan Approval Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**References**

Bowen, P., Hash, J., & Wilson, M. (2007). Information security handbook: A guide for managers. *NIST SPECIAL PUBLICATION 800-100, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*. Citeseer.

Force, J. T., & Initiative, T. (2013). Security and privacy controls for federal information systems and organizations. *NIST Special Publication*, *800*(53), 8–13.

Nieles, M., Dempsey, K., & Pillitteri, V. (2017). *An introduction to information security*. National Institute of Standards and Technology.

Swanson, M., Hash, J., & Bowen, P. (2006). Revision Guide for Developing Security Plans for Federal Information Systems. *NIST Special Publication*, *800*, 18.