Need for Separate System Security Plan for Each Field Office

[Author’s name]

[Institute’s name]

Need for Separate System Security Plan for Each Field Office

**Summary**

The corporate organization of Red Clay Renovations is focused on delivering different remodeling services in the form of housing structures. It is vital to indicate that the business operations of this company, established in different countries, eventually increase the corporate horizon for the organization. The business positioning of this company involved the functioning of field offices, located in different geographical areas. Information security, is one major indicator for the company to ensure the success of the business (Nieles, Dempsey, & Pillitteri, 2017). The development of an explicit security plan gives all the stakeholders a brief understanding of the actual aspects of concern and offers better practical measures. It is significant to examine why it is important for the organization to offer a separate system security plan, in case of each field office. In other words, the practical implications of one system, can never be considered feasible for the business operations of another field office.

**Briefing Statement**

A system security plan (SSP) is characterized as the document that is helpful to illustrate different functions and aspects relevant to the entire information system. The prospects of hardware and software connections are greatly linked with the practical spectrum of SSP. The business functioning of Red Clay Renovations Corporation actively associated with the practical idea of SSP to meet the potential performance targets in field offices. The document in the form of SSP provides comprehensive information about the overall description, boundary, architecture, and control domains under the overall spectrum of the system (Bowen, Hash, & Wilson, 2007). The complete information on system packages is possible through the successful development of SSP.

**Purpose of System Security Plan**

It is significant to determine the fundamental need for developing a system security plan for the organization. The central aim of establishing SSP is to successfully ensure proper protection of the entire range of information security systems. The application of all the security system resources needs to be properly aligned with the broad domain of SSP. The documentation of information security protection is an integral practical measure, to determine the performance level of different security elements.

           The successful implications of SSP can be observed by developing a different system security plan, in case of different field offices of Red Clay Renovations. There is a need for establishing a separate security plan for each field office to successfully meet desired forms of security requirements. The practical idea of security system plan is based on critical evaluation of data integrity and proper confidentiality of the entire security system (Swanson, 1998). It is vital to establish a separate system security plan for different field offices to ensure proper protection in the forms of confidentiality level, integrity, and proper dissemination of information between different stakeholders.

**The need for Separate System Security Plan**

It is recommended for the policymakers to develop a separate system security plan for each field office, because it presents the unique form of information control. Different duties and job tasks of workers also evaluate through the framework of SSP, concerning the objective of information protection. Important system information in the forms of the system owner, name of the system, list of controls, and overall process of the system is also related to practical implications of SSP. Access control methods, in the case of each field office, also determine through the documented form of SSP (Force & Initiative, 2013). This idea of data protection requires critical scrutiny of passwords, digital cards, and the approach of biometrics under the domain of a separate system security plan, for each field office. Strengths and weaknesses of the information system can also be effectively observed through the development of a distinct security plan of action.

**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. M. (1998). *Guide for developing security plans for information technology systems*.