# Project #3: System Security Plan

## WARNING: YOU MUST PARAPHRASE INFORMATION USED IN THIS ASSIGNMENT. Copy/Paste is only allowed for the names and designators of security controls and/or control families. All other information used in this assignment must be rewritten into your own words.

## Company Background & Operating Environment

Red Clay Renovations is an internationally recognized, awarding winning firm that specializes in the renovation and rehabilitation of residential buildings and dwellings. The company specializes in updating homes using “smart home” and “Internet of Things” technologies while maintaining period correct architectural characteristics. Please refer to the company profile (file posted in Week 1 > Content > CSIA 413 Red Clay Renovations Company Profile.docx) for background information and information about the company’s operating environment. In addition to the information from the company profile, you should:

* Use the Wilmington Headquarters (staff) office as the target for the System Security Plan
* Use Verizon FiOS as the Internet Services Provider (see <http://www.verizonenterprise.com/terms/us/products/internet/sla/> )

## Policy Issue & Plan of Action

A recent risk assessment highlighted the need to formalize the security measures required to protect information, information systems, and the information infrastructures for the company’s headquarters and field offices. This requirement has been incorporated into the company’s risk management plan and the company’s CISO has been tasked with developing, documenting, and implementing the required security measures. The IT Governance board also has a role to play since it must review and approve all changes which affect IT systems under its purview.

The CISO has proposed a plan of action which includes developing system security plans using guidance from **NIST SP-800-18 *Guide for Developing Security Plans for Federal Information Systems****.* The IT Governance board, after reviewing the CISO’s proposed plan of action,voted and accepted this recommendation. In its discussions prior to the vote, the CISO explained why the best practices information for security plans from NIST SP 800-18 was suitable for the company’s use. The board also accepted the CISO’s recommendation for creating a single *System Security Plan* for a *General Support System*since, in the CISO’s professional judgement, this type of plan wouldbest meet the“formalization” requirement from the company’s recently adopted risk management strategy.

## Your Task Assignment

As a staff member supporting the CISO, you have been asked to research and then draft the required *system security plan* for a *General Support System.* In your research so far, you have learned that:

* A general support system is defined as “an interconnected set of information resources under the same direct management control that shares common functionality.” (See NIST SP 800-18)
* The Chief of Staff for the company is the designated *system owner* for the IT support systems in the Wilmington, DC headquarters offices.
* The **system boundaries** for the Wilmington, DE office’s*General Support System* have already been documented in the company’s enterprise architecture (see the case study).
* The **security controls** required for the Wilmington, DE office’s IT systems have been documented in a security controls baseline (see the controls baseline attached to this assignment).

|  |
| --- |
| Section 13 of this document will take you the most time to research and write because it requires the most original writing on your part. You must write a description for EACH CONTROL CATEGORY (managerial, operational, and technical). Then, paste in the table from the Security Controls Baseline. THEN, write a descriptive paragraph explaining how these specific controls will work together to protect the Red Clay Renovations IT Infrastructure for the Wilmington, DE Offices (Headquarters). |

**URLs for Recommended Resources For This Project**

|  |  |  |
| --- | --- | --- |
| **Title** | **Type** | **Link** |
| Service Level Agreement (SLA) Internet Dedicated Services | Verizon Enterprise | Web Page | <http://www.verizonenterprise.com/terms/us/products/internet/sla>/ |
| NIST SP 800-100 *Information Security Handbook: A Guide for Managers* | PDF | <https://doi.org/10.6028/NIST.SP.800-100> |
| NIST SP 800-12 R1: An Introduction to Information Security | PDF | <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf> |
| NIST SP 800-18: Guide for Developing Security Plans for Federal Information Systems | PDF | <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf> |
| NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations | PDF | <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> |

## Research:

1. Review the information provided in the case study and in this assignment, especially the information about the headquarters and field offices and the IT systems and networks used in their day to day business affairs.
2. Review NIST’s guidance for developing a *System Security Plan* for a general support IT System. This information is presented in
	1. NIST SP 800-12 R1 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf> Pay special attention to Chapter 2 and Section 5.4
	2. NIST SP 800-18. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf>Pay special attention to the *Sample Information System Security Plan* template provided in Appendix A.
3. Review the definitions for IT Security *control families* as documented in NIST SP 800-12 R1 Chapter 10. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf>
4. Review the definitions for individual controls as listed in Appendix F *Security Control Catalog* in NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations.* <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>You should focus on those controls listed in the security controls baseline provided with this assignment.

## Write:

1. Use the following guidance to complete the System Security Plan using the template from Appendix A of NIST SP 800-18.
	1. Sections 1 through 10 will contain information provided in the assigned case study. You may need to “interpret” that information when writing the descriptions. “Fill in the blanks” for information about the company or its managers which is not provided in the case study, i.e. names, email addresses, phone numbers, etc.). Make sure that your *fictional* information is consistent with information provided in the case study (name of company, locations, etc.).
	2. Section 11 should contain information about the Wilmington, DE headquarters office’s Internet connection Do not include the table. Use the *business* Internet Services Provider listed at the top of this assignment file. Describe the system interconnection type in this section and service level agreement.
	3. Section 12 should contain information derived from the case study. You will need to identify the types of information processed in the headquarters offices and then list the laws and regulations which apply. For example, if the case study company processes or stores *Protected Health Information*, then this section must include information about HIPAA. If the company processes or stores credit card payment information, then this section must include information about the PCI-DSS requirements. For the Headquarters Offices you also have financial information which may be covered by regulations issued by the Securities and Exchange Commission.
	4. Section 13 of the SSP will take the most research and writingtime.You MUST provide the required descriptive paragraphs for the three categories AND the explanations as to how the security controls within the control families will be used to secure the IT infrastructure. You MUST use the selected security control families and security controls as provided security controls baseline.



* + 1. Create 3 sub sections (13.1 Management Controls, 13.2 Operational Controls, and 13.3 Technical Controls). You must provide a description for each category (see the definitions provided in Annex 11.B *Minimum Security Controls* in [NIST SP 800-100 *Information Security Handbook: A Guide for Managers*](https://doi.org/10.6028/NIST.SP.800-100)).
		2. Using the information provided in the security controls baseline, place the required control families and controls under the correct sub section.
		3. Use the exact names and designators for the security control families and individual security controls. BUT, you MUSTparaphrase any and all descriptions. Do NOT cut and paste from NIST documents.
	1. Section 14: use the due date for this assignment as the *plan complete date.*
	2. Section 15: leave the approval date blank. You will not have any other text in this section (since the plan is not yet approved).
1. Use a professional format for your System Security Plan.Your document should be consistently formatted throughout and easy to read.
2. You must include a cover page with the assignment title, your name, and the due date. Your reference list must be on a separate page at the end of your file. These pages do not count towards the assignment’s page count.
3. Common phrases do not require citations. If there is doubt as to whether or not information requires attribution, provide a footnote with publication information or use APA format citations and references.
4. You are expected to write grammatically correct English in every assignment that you submit for grading. Do not turn in any work without (a) using spell check, (b) using grammar check, (c) verifying that your punctuation is correct and (d) reviewing your work for correct word usage and correctly structured sentences and paragraphs.
5. Consult the grading rubric for specific content and formatting requirements for this assignment.

## Submit For Grading

Submit your *System Security Plan* in MS Word format (.docx or .doc file) for grading using your assignment folder. (Attach the file.)