Southern New Hampshire University

IT 241: Case Study Two Guidelines and Rubric

Overview: This case study analysis is the second of two formative tasks that will support your understanding of the key course concepts of human behaviors that could potentially cause a security threat. These case study analyses will inform your approach for the milestone tasks and the final project.

Prompt: Review the security policy template on the California Department of Technology website. For each of the six sections, summarize the content for the organization you have selected for the final project.

Specifically, the following critical elements must be addressed:

- **Introduction:** Provide a brief description of what this policy will state and why it is needed. State the security stance of your organization.
- **Roles and Responsibilities:** Detail the specific responsibilities of each identifiable user population, including management, employees, and residual parties.
- **Policy Directives:** Describe the specifics of the security policy.
- **Enforcement, Auditing, and Reporting:** State what is considered a violation and the penalties for noncompliance. The violation of a policy usually implies an adverse action that needs to be enforced.
- **References:** List all references mentioned in the policy, including organization standards, procedures, and government codes.
- **Control and Maintenance:** State the author and owner of the policy. Describe the conditions and process in which the policy will be reviewed. A policy review should be performed on at least an annual basis to ensure that the policy is current.

Guidelines for Submission: Your case study should be submitted as a three- to four-page Word document (in addition to the title page and references). Use double spacing, 12-point Times New Roman font, one-inch margins, and APA citation format.

Instructor Feedback: This activity uses an integrated rubric in Blackboard. Students can view instructor feedback in the Grade Center. For more information, review these instructions.

Critical Elements	Proficient (100%)	Needs Improvement (75%)	Not Evident (0%)	Value
Introduction	Accurately describes the policy	Does not sufficiently describe the policy	Does not describe the policy	10
Roles and Responsibilities	Accurately details the specific responsibilities	Does not sufficiently detail the specific responsibilities	Does not provide the specific responsibilities	20
Policy Directives	Sufficiently describes the specifics of the security policy	Does not sufficiently describe the specifics of the security policy	Does not describe the specifics of the security policy	20
Enforcement, Auditing, and Reporting	Sufficiently states what is considered a violation and the penalties for noncompliance	Does not sufficiently state what is considered a violation and the penalties for noncompliance	Does not state what is considered a violation and the penalties for noncompliance	20
References	Sufficiently lists all references	Does not sufficiently list all references	Does not list all references	10

Control and Maintenance	Sufficiently describes the conditions and process in which the policy will be reviewed	Does not sufficiently describe the conditions and process in which the policy will be reviewed	Does not describe the conditions and process in which the policy will be reviewed	15
Articulation of Response	Submission has no major errors related to citations, grammar, spelling, syntax, or organization	Submission has major errors related to citations, grammar, spelling, syntax, or organization that negatively impact readability and articulation of main ideas	Submission has critical errors related to citations, grammar, spelling, syntax, or organization that prevent understanding of ideas	5
			Earned Total	**100%**