IHP4 — IHP4 TASK 2: ETHICS AND CYBERSECURITY

LEGAL ISSUES IN INFORMATION SECURITY — C841

PRFA — IHP4

COMPETENCIES

4045.1.1 : Compliance Legal Requirements
The graduate describes the legal requirements to address compliance with cybersecurity policies and procedures with an organization.

4045.1.3 : Security Awareness Training and Education (SATE)
The graduate outlines legal issues that should be included within the security awareness training and education (SATE) program of an organization.

4045.1.4 : Ethical Issues for Cybersecurity
The graduate discusses the implications of ethical issues for specific cybersecurity actions within an organization.

INTRODUCTION

Information security professionals must understand how to apply ethical security principles and processes to their organizations. These standards should define the organization's specific needs and demands to assure data confidentiality, integrity, and availability. An organization's employees must be aware of the security challenges it is facing.

In this task, you will analyze ethical challenges related to information security and develop a training plan for an organization, which will raise awareness of these challenges, convey strategies, and prevent unwanted developments.

SCENARIO

Review the attached "TechFite Case Study" for information on the company being investigated. You should base your responses on this scenario.

REQUIREMENTS

Your submission must be your original work. No more than a combined total of 30% of the submission and no more than a 10% match to any one individual source can be directly quoted or closely paraphrased from sources, even if cited correctly. The similarity report that is provided when you submit your task can be used as a guide.

You must use the rubric to direct the creation of your submission because it provides detailed criteria that will be used to evaluate your work. Each requirement below may be evaluated by more than one rubric aspect. The rubric aspect titles may contain hyperlinks to relevant portions of the course.

*Tasks may **not** be submitted as cloud links, such as links to Google Docs, Google Slides, OneDrive, etc., unless specified in the task requirements. All other submissions must be file types that are uploaded and submitted as attachments (e.g., .docx, .pdf, .ppt).*

A. Address ethical issues for cybersecurity by doing the following:
   1. Discuss the ethical guidelines or standards relating to information security that should apply to the case study.
      a. Justify your reasoning.
   2. Identify the behaviors, or omission of behaviors, of the people who fostered the unethical practices.
   3. Discuss what factors at TechFite led to lax ethical behavior.

B. Describe ways to mitigate problems and build security awareness by doing the following:
   1. Describe **two** information security policies that may have prevented or reduced the criminal activity, deterred the negligent acts, and decreased the threats to intellectual property.
   2. Describe the key components of a Security Awareness Training and Education (SATE) program that could be implemented at TechFite.
      a. Explain how the SATE program will be communicated to TechFite employees.
      b. Justify the SATE program's relevance to mitigating the undesirable behaviors at TechFite.

C. Prepare a summary directed to senior management (*suggested length of 1–2 paragraphs*) that states TechFite's ethical issues from Part A and the related mitigation strategies from Part B.

D. Acknowledge sources, using in-text citations and references, for content that is quoted, paraphrased, or summarized.

E. Demonstrate professional communication in the content and presentation of your submission.

File Restrictions

File name may contain only letters, numbers, spaces, and these symbols: ! - _ . * ' ( )
File size limit: 200 MB
File types allowed: doc, docx, rtf, xls, xlsx, ppt, pptx, odt, pdf, csv, txt, qt, mov, mpg, avi, mp3, wav, mp4, wma, flv, asf, mpeg, wmv, m4v, svg, tif, tiff, jpeg, jpg, gif, png, zip, rar, tar, 7z

RUBRIC

A1:DISCUSSION OF ETHICAL GUIDELINES OR STANDARDS

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
A discussion of the ethical guidelines or standards relating to information security that	The discussion illogically addresses the ethical guidelines or standards relating to informa-	The discussion logically addresses the ethical guidelines or standards relating to information

should apply to the case study is not provided.	tion security that should apply to the case study, or it is unclear how the ethical guidelines or standards relate to the case study.	security that should apply to the case study.

A1A:JUSTIFICATION OF STANDARDS OR GUIDELINES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
A justification of the reasoning of the ethical considerations or guidelines is not provided.	The justification illogically addresses the reasoning of the ethical considerations or guidelines.	The justification logically addresses the reasoning of the ethical considerations or guidelines.

A2:DESCRIPTION OF UNETHICAL BEHAVIORS

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The unethical behavior of individuals or groups is not identified.	The identification of unethical behavior of individuals or groups is inaccurate.	The identification of the unethical behavior of individuals or groups is accurate.

A3:FACTORS

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
A discussion of the factors at TechFite that led to lax ethical behavior is not provided.	The discussion of the factors at TechFite that led to lax ethical behavior is unclear or illogical.	The discussion of the factors at TechFite that led to lax ethical behavior is clear and logical.

B1:INFORMATION SECURITY POLICIES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
A description of 2 information security policies that may have minimized the criminal activity, negligent acts, and threats to intellectual property is not provided.	A description of 2 information security policies that may have minimized the criminal activity, negligent acts, and threats to intellectual property is provided, but *at least* 1 of the policies is	The description addresses 2 information security policies, specific to the case study that may have minimized the criminal activity, negligent acts, and threats to intellectual property.

not relevant or applicable to the case study.

B2:SATE KEY COMPONENTS

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
A description of key components of a SATE program is not provided.	The description of key components of a SATE program that could be implemented at TechFite is not relevant or applicable to the case study.	The description of key components of a SATE program that could be implemented at TechFite is relevant and applicable to the case study.

B2A:SATE COMMUNICATION

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
An explanation of how the SATE program will be communicated to TechFite employees is not provided.	The explanation of how the SATE program will be communicated to TechFite employees is illogical.	The explanation of how the SATE program will be communicated to TechFite employees is logical.

B2B:SATE RELEVANCE

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
A justification of the SATE program's relevance to mitigating the undesirable behaviors at TechFite is not provided.	The justification of the SATE program's relevance to mitigating the undesirable behaviors at TechFite is illogical.	The justification of the SATE program's relevance to mitigating the undesirable behaviors at TechFite is logical.

C:CHALLENGES AND STRATEGIES SUMMARY

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
A summary directed to senior management that states TechFite's ethical issues and the related mitigation strategies is not provided.	A summary directed to senior management that states TechFite's ethical issues and the related mitigation strategies is provided, but the summary is not complete or does not align with the information provided in Parts A and B.	A complete summary directed to senior management that states TechFite's ethical issues and the related mitigation strategies is provided, and the summary aligns with the information provided in Parts A and B.

D:SOURCES

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
The submission does not include both in-text citations and a reference list for sources that are quoted, paraphrased, or summarized.	The submission includes in-text citations for sources that are quoted, paraphrased, or summarized and a reference list; however, the citations or reference list is incomplete or inaccurate.	The submission includes in-text citations for sources that are properly quoted, paraphrased, or summarized and a reference list that accurately identifies the author, date, title, and source location as available. Or the candidate does not use sources.

E:PROFESSIONAL COMMUNICATION

NOT EVIDENT	APPROACHING COMPETENCE	COMPETENT
Content is unstructured, is disjointed, or contains pervasive errors in mechanics, usage, or grammar. Vocabulary or tone is unprofessional or distracts from the topic.	Content is poorly organized, is difficult to follow, or contains errors in mechanics, usage, or grammar that cause confusion. Terminology is misused or ineffective.	Content reflects attention to detail, is organized, and focuses on the main ideas as prescribed in the task or chosen by the candidate. Terminology is pertinent, is used correctly, and effectively conveys the intended meaning. Mechanics, usage, and grammar promote accurate interpretation and understanding.

SUPPORTING DOCUMENTS

TechFite Case Study.docx