Assignment 1: Creating and Communicating a Security Strategy

First Draft Due Week 4

Final Due Week 6, worth 80 points

As an IT professional, you'll often be required to communicate policies, standards, and practices in the workplace. For this assignment, you'll practice this important task by taking on the role of an IT professional charged with creating a memo to communicate your company's new security strategy.

The specific course learning outcomes associated with this assignment are:

- Analyze the importance of network architecture to security operations.
- Apply information security standards to real-world implementation.
- Communicate how problem-solving concepts are applied in a business environment.
- Use information resources to research issues in information systems security.
- Write clearly about network security topics using proper writing mechanics and business formats.

Preparation

1. **Review the essential elements of a security strategy**

A successful IT administration strategy requires the continuous enforcement of policies, standards, and practices (procedures) within the organization. Review these elements to see how they compare:

Policy	The general statements that direct the organization's internal and external communication and goals.
Standards	Describe the requirements of a given activity related to the policy. They are more detailed and specific than policies. In effect, standards are rules that evaluate the quality of the activity. For example, standards define the structure of the password and the numbers, letters, and special characters that must be used in order to create a password.
Practices	The written instructions that describe a series of steps to be followed during the performance of a given activity. Practices must support and enhance the work environment. Also referred to as procedures.

2. **Describe the business environment**

You are the IT professional in charge of security for a company that has recently opened within a shopping mall. Describe the current IT environment at this business. You can draw details from a company you work for now or for which you have worked in the past. You'll need to get creative and identify the details about this business that will influence the policies you'll create. For example, does the company allow cell phone email apps? Does the company allow web mail? If so, how will this affect the mobile computing policy? Describe all the details about this business environment that will be necessary to support your strategy.

3. **Research sample policies**

Familiarize yourself with various templates and sample policies used in the IT field. Do not just copy another company's security policy, but rather learn from the best practices of other companies and apply them to yours. Use these resources to help structure your policies:

- Information Security Policy Templates
- Sample Data Security Policies
- Additional Examples and Tips

Instructions

With the description of the business environment (the fictional company that has opened in a shopping mall) in mind and your policy review and research complete, create a new security strategy in the format of a company memo (no less than three to five pages) in which you do the following:

1. **Describe the business environment and identify the risk and reasoning**
   Provide a brief description of all the important areas of the business environment that you've discovered in your research. Be sure to identify the reasons that prompted the need to create a security policy.

2. **Assemble a security policy**
   Assemble a security policy or policies for this business. Using the memo outline as a guide, collect industry-specific and quality best practices. **In your own words**, formulate your fictional company's security policy or policies. You may use online resources, the Strayer Library, or other industry-related resources such as the National Security Agency (NSA) and Network World. In a few brief sentences, provide specific information on how your policy will support the business' goal.

3. **Develop standards**
   Develop the standards that will describe the requirements of a given activity related to the policy. Standards are the in-depth details of the security policy or policies for a business.

4. **Develop practices**
   Develop the practices that will be used to ensure the business enforces what is stated in the security policy or policies and standards.

Format your assignment according to the following formatting requirements:

- This course is designed to prepare you for a career in IT. While most Strayer University courses require APA (essay) format, this course focuses on writing in a business format. Review this resource to learn more about the important features of business writing: The One Unbreakable Rule in Business Writing.
- You may use the provided memo outline as a guide for this assignment, or you may use your own. Get creative and be original! (You should not just copy a memo from another source.) Adapt the strategy you create to your "company" specifically. In the workplace, it will be important to use company standard documents for this type of communication.
- Do not cut and paste someone else's strategy. Plagiarism detection software will be used to evaluate your submissions.

Rubric

Grading for this assignment will be based on answer quality, logic/organization of the memo, and language and writing skills, using the following rubric.

Points: 80	**Assignment 1: Creating and Communicating a Security Strategy**				
Criteria	**Unacceptable Below 60% F**	**Meets Minimum Expectations 60-69% D**	**Fair 70-79% C**	**Proficient 80-89% B**	**Exemplary 90-100% A**
1. Describe the business and identify the risk and reasoning Weight: 20%	Does not describe the business and does not submit or incompletely identifies the risk and reasoning.	Insufficiently describes the business. The risk is unclear and there is not a clear connection to a reason.	Partially describes the business. The risk is stated but the reasoning needs more supporting details. More details and a clear connection to the risk would improve this section.	Satisfactorily describes the business. The risk is identified and the reasoning has some supporting details.	Thoroughly describes the business. The risk is clearly identified and the reasoning has well-supported detail to connect the risk to the reasoning.
2. Assemble a security policy or policies for the business Weight: 25%	Does not submit or incompletely assembles a security policy or policies for the business.	The policy is missing major elements and does not communicate how it would support the business goal.	The policy includes some elements and partially indicates how it would support the business' goal, but was lacking supporting details.	The policy includes most elements and satisfactorily indicates how it would support the business' goal, but was lacking supporting details.	The policy includes all the necessary elements and clearly indicates how it will support the business' goal.
3. Develop standards Weight: 25%	Does not submit or incompletely develops standards.	The standards are not fully developed and do not describe the requirements of the activity.	The standards partially describe some of the requirements of the activity but lack the details necessary to make them complete.	The standards satisfactorily describe many of the requirements of the activity but could use more details.	The standards thoroughly describe all the requirements of the activity and include sound, in-depth details.

Points: 80	Assignment 1: Creating and Communicating a Security Strategy				
Criteria	**Unacceptable Below 60% F**	**Meets Minimum Expectations 60-69% D**	**Fair 70-79% C**	**Proficient 80-89% B**	**Exemplary 90-100% A**
4. Develop practices Weight: 25%	Does not submit or incompletely develops practices.	The practices do not include enough description to ensure the business can enforce what is stated in the policies and standards. The written instructions do not include steps or enough steps to make them complete.	The practices partially describe how to ensure the business can enforce what is stated in the policies and standards. The written instructions include some steps, but they could be expanded to make them complete.	The practices satisfactorily address how to ensure the business can enforce what is stated in the policies and standards. The written instructions include many of the necessary steps, but additional steps and details would improve the instructions.	The practices thoroughly address how to ensure the business can enforce what is stated in the policies and standards. The written instructions include all the necessary steps and have well-supporting details.
5. Clarity, writing mechanics, and business formatting require-ments Weight: 5%	The writing lacks clarity. Formatting is not appropriate for business.	The writing lacks some clarity. Formatting is not appropriate for business.	The writing is beginning to show clarity. Business formatting is partially applied.	The writing is mostly clear and business formatting is apparent. Some minor adjustments would improve the overall format.	The writing is professional and clear. The formatting is excellent and aligned with business requirements.

Additional Examples and Tips

Example 1: XYZ Inc. Company-Wide Employee Password Strategy

Policies

- All users must have a password.
- Passwords must be changed every six months.

Standards

- A password must have a minimum of six characters.
- A password must have a maximum of 12 characters.
- A password must contain letters, numbers, and special characters other than $.

Practices-Employee

- Create a password. The UserID should be an EmployeeID already generated by HR.
- Send a request to create the account to the Information Technology (IT) department.
- User receives a temporary password.
- Users must change their temporary password the first time they log in.

Example 2: Security Policy and Standards

Password Policy: Passwords are an important part of computer security at your organization. They often serve as the first line of defense in preventing unauthorized access to the organization's computers and data.

In order to define the password policy, it is important to identify the standards.

1. Multi-factor authentication
2. Password strength standard
3. Password security standards; how to keep the password secure

Tips and Points to Consider When Identifying Risks or Security Vulnerabilities

- Flaws in operating systems due to constant attack by malware
- Denial of services attacks
- Employees data theft
- User set a weak password or password that is easy to guess, such as a birthday or child's name.
- User leaves sensitive data on an unlocked, unattended computer
- Organization allows sensitive data on a laptop that leaves the building
- Data can be accessed remotely without using proper security

Memo Outline

Network Security Associates of Atlantis, Inc.
123 Watery Lane
Atlantis, USVI 91199

From: IT Security Dept.
Re: Security Policy

Date:

Section 1: General Policies and Motivation

Section 2: Passwords

Section 3: Biometrics

Section 4: Tokens

Section 5: Physical Security

Section 6: Email Policies

Section 7: Breach Reporting Responsibilities

Section 8: Mobile Policy and BYOD (Bring Your Own Device)