Strayer University

[**Creating and Communicating a Security Strategy**](https://blackboard.strayer.edu/bbcswebdav/institution/CIS/333/1188/CIS333_ASSIGNMENT_1.pdf)

Week 6

[**Creating and Communicating a Security Strategy**](https://blackboard.strayer.edu/bbcswebdav/institution/CIS/333/1188/CIS333_ASSIGNMENT_1.pdf)

for the

Course of

Networking Security Fundaments

02/11/19

By

Kennedy Kabaso.

Professor: Curtis Bunch.

[**Creating and Communicating a Security Strategy**](https://blackboard.strayer.edu/bbcswebdav/institution/CIS/333/1188/CIS333_ASSIGNMENT_1.pdf)**.**

**Introduction**

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.

# Overview

The company’s name is Book Smart Inc and it is a startup company. It is working with major companies to sell different books all over the world. The internal company is a new facility which is a two-story stand-alone building. It is currently consisting of ten employees with a revenue of $10 million but is expected to grow to thirty employees with revenue of $30 million over the next two years. The company is mostly involved in selling books like amazon. It is an E-business activity which sales online only. In addition, its sales directed at consumers and to various business. An ecommerce company come with some challenges which must be taken seriously. It exposes the organization to possible attacks and threats which have been the most challenging issue for most network and the web administrators.

# Purpose

# This policy defines the requirements for all our computers used at Book Smart Inc to protect the

# data of our customers.

# Scope

This policy applies to all access to the computers in our company which can be remotely and, on the premises, so that our assets are protect from all kind of attack. All broken company computers would be properly disposed, and their hard drives, properly shielded to ensure they is no leakage of our customer information anywhere.

1. **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.

As this is the ECommerce business, our customer data is the most important asset to protect. To make sure this is done, we have established a safe and secure network for our company which will protect our assets which is our primary goal. This would be done by protected our network and computer using best practice so that customer transactions are encrypted. Moreover, they should be an internal network, which is to protect the internal assets and an external one, which is opened to the public for the ecommerce. It is put on a Demilitarized Zone (DMZ). Also, the network structure of our company is made up of two firewalls. The external firewall deal with the public and the internal one deal with our local area network which is the intranet. The IT department will use firewalls, intrusion detection systems and virus scanners to provide some assurance that the security policies for the internal and the external network are properly implemented. In addition, CIA must be applied to our company, which is a widely used benchmark for evaluation of information systems security, focusing on the three core goals of confidentiality, integrity and availability of information.

The servers of Book Smart Inc are the place where they hackers wants to get into most of the time. The Web Server host websites and delivers web content from the company websites over the internet. It follows a network protocol known as hypertext transfer protocol (HTTP**)** which handle web traffic, the Mail Server which is an application in a network whose purpose is to act as a post office. This server stores incoming mail for distribution to local employees and sends out outgoing messages. In addition, it handles the mails from our customers and employees all over the world. It uses a simple mail transfer protocol (SMTP), and finally, the File Server for the central storage and management of data files so that other computers on our company network can access the files. It allows employees to share information over a network of our company without having to physically transfer files by some other external storage devices. All these are connected to the switch and a single cable would connect to the Router which link to the internet. Moreover, a firewall is configured with strong restriction to order to handle the security of the network before connected these servers to the internet. This should be made difficult for some hankers to break into the network. To make it easy for employees to work anywhere near the building of the company, the wireless access point is provided to them. To safeguard security of company network systems, make sure a higher level of connection is given and prevent interference with other users of the wireless, some security policies should be put in place. The access points will be provided and installed by IT department. They will have rights to disconnect any unauthorized access point that it discovers on the company Network. This will limit the number of access point on the premises. In order to protect our data from being access by any user, the VPN access policies will be put in place with only authorized users who have to go through the authentication process. To increase the production and protect the company assets, an Internet usage policy will be put in place. Computer software protected by copyright is not to be copied using company assets. Personal use of company computer is permitted, but the use of resources for other things not related to company work during working hours is considered an irresponsible use. 

1. **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.

To be a trusted company, our customers data needs to be kept safe by protect the confidentiality, by preserve the integrity and by promote the availability of it for authorized use.

The Confidentiality of data is to keep its privacy from any unauthorized user. Those authorized users should be given only enough privilege to perform their duties, and no more. Some other synonyms for confidentiality are privacy*,*secrecy*,* anddiscretion. Moreover, the Confidentiality of the data are intended to ensure that no unauthorized access to information is permitted and that accidental disclosure of sensitive information is not possible. The only way to get to those data is by using login user IDs and passwords. Since a password is important to get into the network of the company, it must have a minimum of eight characters, a maximum of twelve character and must contains a combination of numbers, upper case and lower-case characters.

In addition, every employee must change his or her password change every three months. Also, the employees who leave work or terminated should have their account disable immediately.

The Integrity of data is to keep it pure and trustworthy by protecting system data from intentional or accidental changes. This can be done by prevent unauthorized users from making modifications to data, prevent authorized users from making unauthorized modifications and maintain internal and external consistency of data. Therefore, any person changes must be documented and the person making the change.

The Availability of data is to keep it and resources available for authorized use, especially during emergencies. In addition, there is a business continuity plan in place. This will put the company on a continually pace to ensure the business can continue to exist in the event of a disaster. Moreover, there is a software defensive method and a disaster recovery plan which make sure everything runs smoothly. Therefore, authorized users must be in the database, more data in the cloud must be available which can be access by authorized user only.

Having a password which is more than twelve characters long is not a good security measures because employees will be forced to write it down somewhere. Therefore, less than twelve character, but more than six is the acceptable length. In order to control, the productivity time of employees, web filtering standards should be put in place. This will restrict what websites our employees can visit on company computers. As we are dealing with sensitive data which need the best protection, so it is important to use the best VPN protocol which is situatable for this. Therefore, **Secure Socket Tunneling Protocol**is a VPN protocol which is good for this because it comes with one notable benefit and it has been fully integrated with every Microsoft operating system. This protocol will support all our system in the company because our operation systems are updated with the latest one.

1. **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.

#### The confidentiality, integrity and availability of information must be achieved by granting access only to authorized personnel. In addition, applying encryption to information that will be sent over the Internet is going to be taken seriously because of the type of the business we are involved in. All the employees must use their access card into the building and not letting other people behind access. All Bluetooth devices more especially mobile phone must use Secure Simple Pairing with encryption enabled on our company network. In addition, the broadcast of SSID must be disabled. To make the hackers not search on google for some information of the devices, the default SSID name, the default login and password must be changed on any new device connected to the company network. All employees must user their social security number as their Employee IDs, their log user name should be the first initial plus last name and the password should be setup by the IT departments which can be changed after the first log in. They employees who don’t abiding by those polices should be given verb warning the first time, write warning the second time and the termination of employment the third time. Any visitor who user our company assets badly should be locked from using our computers or the Network. The DMZ should be placed between the two firewall and this will make it difficult for the external network which is poison with malware to infect our private network.

# 5. Definitions and Terms

The following definition and terms are used in this document.

* **Applications**: It is any program, or group of programs, that is designed for the end user
* **Business Continuity: It** is the planning and the preparing of a company to make sure it overcomes serious incidents such as the disasters and continues its normal operations within a short period of time.
* **Demilitarized zone: It is a physical subnetwork that contains and exposes an organization's external facing services to the Internet which is very dangerous due to security issues.**
* **Economy:** It is the wealth and resources of a country or region, especially in terms of the production and consumption of goods and services.
* **Firewalls: There are network security system designed to prevent unauthorized access to or from a private network.**
* **Network:** It is a set of computers connected for the purpose of sharing resources.
* **Risk Management: It** is the process of identifying, assessing and controlling any threats to a company's investment and its revenue such as financial, accidents and natural disasters.

### **Risks**: Are the uncertain event or condition that, if it occurs, have positive or negative effect on a project's objectives.

### **Security Policies**: There are written documents that states how a company plans to protect its physical and assets from any intruder.

* **Wireless Attacks:** It is the kind of an attack by which a trick of a wireless access point is made.
* **Wireless:** A wireless network is a computer network that uses wireless data connections between network nodes

1. **Bibliography.**
2. (Kerzner i) Kerzner, Harold R. *Project Management - Best Practices: Achieving Global Excellence, 3rd Edition*. John Wiley & Sons P&T, 01/2014.
3. Roberts, D. (2013). *Unleashing the power of IT*. (2nd ed.). Hoboken, NJ: John Wiley &
4. Sons, Inc.