Network Security Policy for Logistic Company

Team/Student Name(s): Team 5 - Mario Mateus & Loy Campbell  |  Business Advisor Name: Dr. John Smith  |  Professor: Dr. Yair Levy, Professor of Information Systems and Cybersecurity

INTRODUCTION

Information that clients are providing in logistic company can be compromised by criminals in order to submit a custom entry under legitimate company’s name to import counterfeit and counterfeited goods into the United States. The real company information, obtained otherwise, can only be legally obtained through a proper legal process. The organization must first request access to the information database. The organization also obtains customs release fees related to border services, etc. as well as applicable duties and taxes, if any. The organization must then submit a request for the information to the US Customs and Border Protection Service. The organization must then provide the requested information to the US Customs and Border Protection Service. The organization must then provide the requested information to the US Customs and Border Protection Service.

LOGISTICS INC. is an integrated logistic company that offers a wide range of logistic services and exporting including custom brokers services, which provides a database of the required information for importing and exporting goods. This database includes the necessary information, namely, the package identification number, the country of origin, the date of shipment, the name of the consignee, and the name of the shipper. This database is subsequently used in customs declaration and in the tracking of the goods.

The organization must ensure that all information is accurate and up-to-date. The organization must also ensure that all information is properly protected and that it is accessible only to authorized personnel. The organization must also ensure that all information is properly stored and that it is accessible only to authorized personnel.

Every employee is required to follow the rules of the facility and to report any suspicious activity. The organization must also ensure that all information is properly protected and that it is accessible only to authorized personnel. The organization must also ensure that all information is properly stored and that it is accessible only to authorized personnel.

Facts:

- Organizational
  - The organization is integrated by a group of 10 people that is divided into two departments and each department has different technical infrastructure and technical activities.
  - One department is in charge of legislating goods that are being imported (custom brokers), while another department is responsible for importing and exporting services. Both departments have independent sets of hardware and software they use and they have different contracts to provide technical services.

- Technical
  - The organization’s wide range of internal controls will be improved by the following measures:
  - Each department has its own network, controls, and infrastructure.
  - Additional, each department controls their IT technical services to separate first-party vendors. Furthermore, each department controls access to their network infrastructure.

Despite of the organization’s restrictions placed on internal access control, a great threat is generated by the lack of wireless security. Wireless access has a phone connection without a password for visitors, allowing intruders to access the network.

SOLUTIONS AND PLANS

We consider that the company should ensure that all information is protected and that it is accessible only to authorized personnel. The organization must also ensure that all information is properly stored and that it is accessible only to authorized personnel.

Remote Access Policy
- Purpose
  - The purpose of this policy is to define standard practices for setting up wireless access points created on a computer network. These practices are designed to ensure that all policies and procedures are in place to protect the organization’s information.

- Scope
  - This policy applies to all company networks and to all computers that connect to the company network.

Remote Access Policy
- Purpose
  - To ensure that all remote access is secured and that all access is monitored and controlled.

Wireless Communication Policy
- Purpose
  - The purpose of this policy is to ensure that all wireless communications are secure and that all communications are monitored and controlled.

Wireless Communication Standard
- Purpose
  - This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a public network. Only those wireless infrastructure devices that meet these requirements specified in this standard are granted by the organization. The organization is responsible for ensuring that all wireless infrastructure devices that are provided to employees, contractors, and employees of other companies that connect to the public network meet these requirements. This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a public network. Only those wireless infrastructure devices that meet these requirements specified in this standard are granted by the organization. The organization is responsible for ensuring that all wireless infrastructure devices that are provided to employees, contractors, and employees of other companies that connect to the public network meet these requirements.

Technical controls (SW & HW):
- Purpose
  - To control access to information systems and to ensure that only authorized personnel have access to the information systems.

CONCLUSIONS

The network security policy will include the following elements:

- Network policies
  - The policy should include general guidelines for the overall network security policy.

- Network access control
  - The policy should include specific guidelines for the overall network access control policy.

- Network configuration management
  - The policy should include specific guidelines for the overall network configuration management policy.

- Network monitoring and analysis
  - The policy should include specific guidelines for the overall network monitoring and analysis policy.

- Network equipment and software management
  - The policy should include specific guidelines for the overall network equipment and software management policy.

- Network security incident management
  - The policy should include specific guidelines for the overall network security incident management policy.

- Network security governance
  - The policy should include specific guidelines for the overall network security governance policy.

This policy will provide a comprehensive framework for the organization to implement and maintain a secure network environment.