INFOSEC - policy

Assignment 4

Authors

Vilhelm Park - vp222dv

Alex Brumen - ab225kn

Nour Alasadi - na222wp

Physical and environmental security

Purpose

The purpose of this Policy is to make sure the physical and environmental is secure inside the company. That different areas are secure and isolated from unauthorized employers.

This Policy informs the Loco company staff and administrators to isolate areas in the building, Get different privileges for different employers, set up security cameras to monitor and log the activity inside the company.

The goal of physical and environmental security is to:

- Keep unauthorized employees from different areas in the company.
- Improve locks inside the building.
- Setup security cameras to monitor activity inside the company.
- Improve the Alarm system when no employers are at work.

Information related to:

- Door locks and padlocks.
- Closed-circuit television (CCTV)
- Alarm systems

Definitions

Authorization – An user with access to a location/control mechanism in the system.
Availability – Make sure everything is ready and the setup is correctly inside the security configuration.
Unauthorized access – A user that does not have access to an area in the system gets access.

Who is Affected By This Policy

The person who is affected by this is the staff and administrator at Loco news. All employees at Loco news are at risk because the privilege is not set to different employers.

Countermeasures

Responsibilities

Responsibilities are related to us as security workers and the employers themselves for taking care of the information that is stored in rooms and sensitive areas. The administrator should also have a responsibility when it comes to the employers at Loco news related to access control in the different areas. All employees do have access to different areas with different security and this is a responsibility for each employer. The employers that leave the building at the end of the day should have control over the alarm system to make sure everything in the building is secure at night, or when no employers are at work.

Understanding the different responsibilities:

- Understand the security by isolating areas in the building.
- Understand the different security rating in locks,
- Have control over the building's activity by monitoring the area.

Availability

The security system should suit every employer and administrator to get their work done. The security improvement is ready when every part is configured and set up correctly inside Loco news. The security futures will be control, privileges, isolation, and protection of authorized rooms in the building. The security futures that are locks, CCTV, and the alarm will be configured correctly by an IT-employer that makes sure everything is correct and can make sure the security is reliable. The alarm system should be implanted in all rooms and all doors that do have access to the buildings inside. The alarm should always be active when no employers are at work.

Operations security

Purpose

The purpose of this policy is to make sure that the company has protection from malware and that they have some sort of backup for sensitive information. That there is a policy for what is allowed to do on the internet and what software is allowed to be downloaded. It's also to make sure that Loco news has started using logging and monitoring, while also having some countermeasure to technical vulnerabilities.

This Policy informs the Loco News staff and administrators to make sure that employees can't download anything they want on their work computers and laptops. Also some specific guides on what to not do on the internet. They will also be informed to always have a backup for their most sensitive information such as news that Loco news got exclusive rights to. There will also be some information on why logging and monitoring are important to implement and how to do it. Then finally there will be some discussion on how Loco news can countermeasure technical vulnerabilities.

The goal of Operations security is to:

- Create a basic guideline for what the employees are allowed to download on their work computers and laptops.
- Give some basic information on what to not do on the internet.
- Setup backup for sensitive information.
- Implement basic logging and monitoring.
- Implement a basic technical vulnerability protocol.

Information related to:

- Work computers and laptops
- Backup
- Logging and monitoring
- Technical vulnerability

Definitions

Malware - Malicious software that originates for the sole purpose of causing harm to victims' computer systems and works in opposition to the victims who accidentally contracts it to their computers.

Technical vulnerability – weakness in the technical equipment, easily abused by people who want to harm the equipment.

Who is Affected By This Policy

The people who are most affected are the employees, but also the administrator at Loco news to some extent. All work computers and laptops are at risk since the employees have responsibilities over their computers and don't have any restrictions. The computers and laptops are at risk to contract malware it could affect everyone on Loco news especially since there is currently no backup for any data. Another issue related to employees about their responsibilities towards work-related devices is that there is no logging or monitoring, so if someone contracts malware it will be hard to track down. Technical vulnerabilities can also affect the whole company depending on what the vulnerabilities are.

Countermeasures

Protection against malware

Loco news currently has basic antivirus software on their computers, but as security workers, we will recommend buying more robust antivirus software that is for companies. We will recommend the company to implement a policy for the employees. The policy should include some basic rules such as the employees are not allowed to download unauthorized software, the only authorized software should be deemed safe and related to work. We will also recommend sending your employees on a course where they learn about basic computer security, this and the policy will help keep the computers safer. This is because if the employees have responsibilities over their computers and they have no knowledge about computer security they might download software that contains malware. Other bad cases can happen, but this is one of them.

Backup

Loco news has no backup currently for sensitive information, and their security is not the best from what can be seen, so we recommend that the company will implement a backup plan. In the backup plan, there should be some information on how often Loco news should create backups. We would recommend that whenever the company gets exclusive rights to some big news or some sensitive information for some party they should make sure that the information is encrypted and put in a backup. The backup plan should then have documentation on how to retrieve the information if the worst comes to the worst. If the information is in a physical state and the backup is stored in a physical location, make sure that the location is in a place that can not be damaged by floods, fires, and so forth. Also make sure that the location is not in the server room since other people from the neighboring company have access to that location, the people responsible for the backup are the only ones that should have access to the physical location.

Logging and monitoring

Since the company has currently no logging or monitoring there is no way to know what happened if something goes wrong. For example, the whole system gets hacked, without logging

it will be hard to track where the problem started and how to prevent it from happening in the future. We recommend that Loco news will implement some logging that will log whenever a worker does something in the computers, the logging should include the date to show when the activity happened and the user id to show who did it. Make sure that the data is synchronized for all employees so that the employees that might be in other timezones still get the date as all the other employees. The login should only be authorized for the employees that get the responsibility of monitoring the logs. The employees that handle monitoring should keep up on what the other employees do and how they do things. The monitoring team should also be the ones that handle investigations whenever there is a breach of security. Logging and monitoring is also related to policy that is recommended to be implemented in the earlier section, since if there is an employee that breaches the policy the logging system will determine who breach it, how they breached it, and give it to whoever handles disciplinary issues in Loco news.

Technical vulnerabilities

Loco news has never run into technical vulnerabilities, but that doesn't stop them from running into it in the future. The IT department in Loco news should keep themselves up to date regarding the companies technical equipment and monitor the equipment to as fast as possible notice if there is a vulnerability. The security team recommends that Loco news will have a team that handles cases when a technical vulnerability is noticed, this team should have the most knowledgeable employees regarding computer security. The team should analyze the vulnerability and how severe it is, depending on the severity, and look for countermeasures. If multiple vulnerabilities got noticed at the same time the team should determine which vulnerabilities are the most severe and start looking for countermeasures. Whenever the team acts on the countermeasure someone in the team must keep a logo of what they did to counteract the vulnerability, in case they run into similar issues in the future. The logs could then be reused.

Access control

Purpose

The purpose of this policy is to make sure the company is secure against unauthorized individuals viewing or entering a facility with sensitive information. That there is a policy for who enters a facility or sending (emails) and computers (desktops and laptops).

This Policy should establish a system (an id-card with a security pin) that is required to be scanned and entered for a person to enter a facility or use a computer. This segment will explain how to establish such security and what requirements are needed and what each is used for and explain in detail what each part is and why it is important.

Definition

Keypad - A device that has a small display and keyboard of numbers (number pad). This is for personnel to enter their pin/password to enter a facility.

REX - Request to exit, is a system that ensures a lock from the outside but no lock for the inside. This is to prevent personnel from being required to enter the pin in order to open the lock.

Who is affected by this policy

All employers and employees are affected. All members of Loco news are at risk of unauthorized individuals reading or viewing confidential information /documents.

Countermeasures

After interviewing an administrator in Loco news, it was noted that “no such controls are in place”. This puts the company at risk since the consequences could be detrimental. A sensitive document in the wrong hands could result in companies going bankrupt. If securing a device is important then securing a room is equally if not more important. Implementation of access control is most advised for ensuring security in a room

How to install

There are ways to establish an access control system. The most secure Access control is installed with an Access controller (the decision-maker device that decides if the individual can proceed to enter the room or not), a keypad that allows employees and employers to enter their pin so that the access controller grants them access to the facility. The doors should have both a door strike or magnetic lock and door contact. The door contact is for personnel to identify if the door is locked or unlocked, the door strike or magnetic lock is for the door to release the lock when personnel enters their unique credentials. Lastly is a REX (request to exit) system, meaning that from the outside - the door is locked. However from the inside - out the door does not require the individual to enter any password or pin or any unique credentials in order to exit the room.

Benefits

The benefits of having an Access control is much more than a device or a pin code in your phone. With access control, you can document which personnel entered what room last and that is not even covering the increased security in the room. With the help of access control, it will secure confidential information from being viewed by unauthorized individuals. These documents or computers need to be kept hidden and only authorized should be able to access these sensitive files and documents.