/Users/apple/Library/Containers/com.microsoft.Outlook/Data/Library/Caches/Signatures/signature_2105988401

**​​**

**Security**

**00203280**

**D/618/7406**

**Section (3)**

**Security report**

**Submitted to**

**Sami Al-Mashaqbeh**

**Submitted by**   
**Obada Al-Halaybeh**

**Summer –2024**

1. First, I used this table to determine the risk level.

A table with text on it

Description automatically generated

**Where E is extreme, H high, M medium and L low.**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Asset | Threat/ vulnerability | Existing  controls | Impact | Likelihood | Level of risk | Suggested control |
| Employee information  customer information | Malware infection that will lead to data leaks and alteration  This will affect the confidentiality of the data and the integrity (from the CIA) | Old anti-malware  Disabled external storage devices | Catastrophic | Almost certain | E | Update the anti-malware and the operating systems and applications / get a (HIDS) / put formal policy for banding all external devices on the company devices / install firewalls |
| Internal network departments (HR/finance)  critical servers (database servers and application servers) | Data breach  This will affect the (Confidentiality from the CIA) | Network segmentation  Expired firewall licenses | Doomsday | Likely | E | Update the firewall / put an IDS and IPS / create more secure segmentation |
| Database servers  Customer data | Information leaks or data breach and  changing sensitive information (integrity and Confidentiality from the CIA) | MD5 cryptography  regular backups  SSL/TLS and SHA1 | Doomsday | likely | E | Get newer encryption system / get a privet or secure cloud to save critical information |
| Remote administration services | Unauthorized access that will affect the Confidentiality and integrity  As if the attacker modified data | Old OpenSSH  version | Major | Likely | E | Update the OpenSSH |
| File servers  Communication servers | Phishing  Ransomware infection  This will affect the availability of the data (availability and Confidentiality from the CIA) | None | major | Possible | E | Get email monitoring app to block suspicious mails / create police for mandatory awareness training |
| All the data in the data center | Unauthorized access (Confidentiality / integrity)  Fire/water/humidity/dust/ high temperature (availability)  Electric outage (availability)  (it affects all 3 from the CIA) | None | Doomsday | likely | E | Install HVAC(heating, ventilation, air conditioning systems) / install fire suppression mechanism / install UPS (when the power goes off) / get a biometric scan in addition for the employee card |
| Employee data  Sensitive customer data | Data breach (it affects Confidentiality and integrity from CIA) | Expired vpn digital certificates | Major | possible | E | Update the vpn / enforce strict access police for any one who use the vpn to be monitored from the company employee dedicated for monitoring people |
| Communication Servers  File servers  Employee data | Physical access to the passwords that cause data leaks (this will affect the Confidentiality)  Some of the data can be altered and this can affect the integrity | Passwords | Major | possible | E | Install security cameras to watch who access that device / enforce police that forbid employee to write down their passwords on nots / conduct awareness training |
| All the employee relevant data | Social engineering attack that may lead to access attack and DDOS attack that could affect Confidentiality, integrity and availability  Phishing attacks to compromise important data either to sell it or change it this will affect the confidentiality and integrity | None  None | Major  Catastrophic | Likely  Likely | E  E | Conduct a training for dealing with social engineering attacks, how to handle data and how to deal with an attack / take the standards of the GDPR and implement it  create awareness training f rom phishing attacks that may be direct or indirect |
| Web servers | DDOS attack that affect the availability of the servers to the users and this could cost a lot of finance problems | None | Doomsday | Likely | E | Create a decoy server that handles the DDos attack and block them from reaching the real servers |
| Database servers | The implementation of malware or getting data breach from the DDoS attack that will affect the confidentiality and integrity of the data | None | Catastrophic | Likely | E | Installing IDS/IPS to have fast response when the attack happen or even stop it / get someone to do penetration test to patch any vulnerability |
| Company data | Unauthorized access to the data and manipulation  That will affect both confidentiality and integrity of the data | None | Major | Likely | E | Implement access controls so that only high ranking employee can reach to the important data/ install CCTV cameras / create survey about the satisfaction of the workers and try to give them what they are missing in reasonable amount |
| The data center | Forced entrance  Unauthorized access  That will lead to destroying the servers and affect the availability of them and could take the data and sell it or even change it and this affect the confidentiality and integrity | Glass doors  Outdated physical key | Catastrophic | possible | E | Add more protective doors on the side of the servers and install barriers outside with new CCTV cameras you also can add biometric device and alarms too  Remove the idea of physical key and go for electronic so it’s harder to duplicate |
| Network security | Unauthorized access to the vpn will lead to data leaks and this will affect the confidentiality | Expired digital certificate/none | moderate | Possible | H | Assign dedicated employee to watch over the third party connections to the company/ get a new digital certificate with good ecnryption |
| Wi-Fi network | Unauthorized access that causes to data leaks and alteration that will affect the confidentiality and integrity of the data | None | Moderate | Possible | H | They should separate guest wi-fi from the employee wife and they should install firewall that block any unwanted traffic and spot early attacks |

# Data protection processes and regulations

## We have three common regulations known around the world

* PCI  
  PCI stands for payment card industry, this regulation ensures that the company processing, storing and transmitting credit card information stay a secure environment to protect the data on the card.

The company could use this regulation to enhance how it handles payments, as if they follow this regulation, it will help them secure the payment data, create a strong access control system, and it will maintain a secure network.

* HIPAA  
  HIPAA stands for health insurance portability and accountability act, the purpose of this regulation is to protect the privacy and security of health information, particularly the electronic information too.

This regulation will be in use if the company is dealing with some health-related data and wants it to be secured.

* GDPR  
  GDPR stands for general data protection regulation, and its European union law, this regulation rules the processing of personal data of individuals within the European union and focus on protecting the privacy and rights of data subjects.  
    
  since the company can work on a global atmosphere its is obligated to use the HDPR regulation on the EU region if its processing any data for the citizens there, this give control to the individuals to give consent to the company to take their data, the processes to handle the personal data must be designed with consideration of the principles and it should provide safeguards to protect the data and they must keep privacy in mind when designing it, for example the dates should not be public and can’t use it to identify a subject.

# Observation on how sofix does its risk assessment and how it take measures

* **Identification**
* For the identification of the risks, they conduct annual risk assessments to check if there are any threats, they also have internal audits and industry reports that help them in the assessment process.
* **Evaluation**
  + For the evaluation of the risk, they are using a qualitative approach as they are not looking at the threats from the financial perspective, and they have the opinion of professionals to act on, and they use the silver star mines risk register to evaluate the likelihood, impact and risk level too as technique to help them.
* **Management**
  + For the management of the risks, the company uses various controls like the firewall, encryption and multi-factor authentication, and those controls help limit the threats and their impact on the company.
* **Frequency**
  + For the frequency, the company has annual risk assessment, and the last update for the risk managing was 6 months ago in that 6 months new advancements and threats were found and to address this problem they will need to do quarterly checkups and updates for their systems as this is the most rational procedure.

# ISO 31000

It is an enterprise risk management system made by iso (international organization for standardization) and it has three main components:

* The risk management process
* ISO 31000’s risk management principles
* Framework and guidelines

## The risk management process

1. **Risk identification**  
   Identify potential risks that could stop the organization’s objectives.
2. **Risk analysis**Understand the sources and causes of identified risks and evaluate their potential impact.
3. **Risk evaluation**Compare the results of risk analysis against risk criteria to determine the magnitude and acceptability of risks.
4. **Risk treatment**Implement measures to change risk likelihood and impact, aiming to reduce overall risk.
5. **Establishing the context**Define the scope, objectives, and risk evaluation criteria, considering both internal and external factors.
6. **Monitoring and review**Keep a constant watch on risks and the efficiency of risk management procedures and make adjustments as needed.
7. **Communication and consultation**  
   Involve stakeholders at every stage of the risk management procedure to guarantee clarity and well-informed choices.

## risk management principles (ISO 31000)

According to ISO 31000, risk management techniques should be incorporated into every aspect of organizational operations to guarantee a thorough and organized procedure. To enable well-informed decision-making, the framework must be tailored to the goals and culture of the company while also taking stakeholder viewpoints into consideration. It is critical that the risk management strategy continue to be flexible and iterative, adjusting to new situations and depending on the most up-to-date data. Understanding that human and cultural elements have an impact on risk management outcomes, they should be taken into account at every level of the process. Last but not least, maintaining the framework's efficacy requires constant learning and modification, which emphasizes the importance of continual improvement.

## Framework and guidelines

The ISO 31000 framework and guidelines place a strong emphasis on the necessity of securing leadership support and matching risk management with business objectives. All areas of the company should incorporate risk management, and operations should be planned with a thorough grasp of the organization's context. Setting objectives, coming to decisions, and modifying procedures as needed are all part of the execution phase. The performance and efficacy of the risk management system must be regularly assessed. Sustaining the effectiveness and relevance of the risk management framework requires constant monitoring and improvement, which calls for continuous improvement.

## The application in sofix company

We start by identifying risks like outdated software, poor physical security and weak cryptography, after the identification we analyze the impact of the risks like the data breaches, furthermore we assess if the identified risks are acceptable for the company or should be addressed, then the treatment starts by giving recommendations such as updating the software, reenforcing the physical security and rising employee awareness, then we look at the company scop of risk management process by taking into account the objectives of the company and the regulations they use (GDPR, HIPAA,PCI), after that we look regularly into the effectiveness of the security measures, we also look for consultation from stockholders from all types to ensure that they have responsibility and roles to be fullfed in keeping the security of the company and the power of it.

# IT security audit and the impact of it

## What is an IT security audit

First the IT auditor evaluates and compares the security of the organization information system to a list of best practices, policies, standards or regulations for the following 4 things:

* Physical components of organization’s information systems and the environment where its used and stored.
* Application and software, include security patches of the information systems.
* Network vulnerabilities, this includes evaluation of the information when it travels between 2 points.
* The human dimension, include how employees collect, share and store the sensitive information.

## Impact on sofix

Sofix need an IT security audit, so it can ensure that data is protected by creating a routine of auditing network access control, encryption use and transmissions, the audits also have different perspective of observation that can help improve both the cybersecurity and other aspects of there company, farther more they can point out security flaws by creating list of possible flaws and checking it, they also make sure to be UpToDate with the regulations and utilize recommendations to improve the company, lastly they will help saving money for the company.

# The impact of Misalignment and how to fix it

Misalignment happens a lot on the companies, and it may vary from being a big problem to a small one that can be ignored, and there are ways to align back the IT security police and the organizational police, one solution to align them is setting up meetings first they will need to identify what argument point they will ty to fix for example disposing paper documents the organization police said that a scissors can be enough to dispose the documents meanwhile the it security police was to send the documents to the burner were all the sensitive data get destroyed and this is not cost efficient since it cost more money to use it, this mad the employees confused and do not know what to do so in that meeting they will try to find a middle ground were it is safe to dispose the documents and it’s not costing extra budget and they find out a paper shredder can do that job with completely removing the data from the documents and not spending a lot of money on it.

Another way is to hire someone who monitor both organizational policies and IT security policies and chose what is best and beneficial for the company to work with as this will cut the arguing between the 2 sides and make it more efficient.

## The impact of the misalignment

* The misalignment could create conflict between the 2 sides that leads to exposure in the system and lead to attacks that cost the company time and money, it also confuses the employee as mentioned earlier.
* Misalignment could cost the company its reputation and the trust with the customers and partners.
* Misalignment could lead to regulation violations that leads to big fines.
* Misalignment can cause a loss in the competitive environment, as it will create barriers that restrict the company from advancing.

# Stakeholders

The role of stakeholders to make use of the security audit recommendations are as follows:

* Management (C-level)
* the management make sure that the recommendations are done in short time and in a efficient manner, they also make sure that the necessary resources are allocated to implement the recommendations and does not affect the business.
* IT officers
* They are responsible for installing the technical security measures that the audit recommends, and he ensures that the measures are implemented correctly, and they do not affect the performance of the system.
* Risk owners
* they are responsible for checking if the risk that the audit found is mitigated, and they work with management and IT to take and install the recommended measures to make the risk acceptable.
* Facility and security officers
* they are responsible for the physical security of buildings and data center, and making sure the data center is secure, also they oversee the disaster recovery infrastructure like fire alarms and UPS.
* Compliance officers (quality assurance)
* this role make sure that the hole organization is matched with the security audit recommendations, and they work with the other stakeholders to ensure that recommended measures are implemented.

# Policies

## Password protection policy

1. Overview (importance)  
   Passwords are essential for protecting computer systems. Unauthorized access may result from a weak or compromised password, which could expose private information or permit resource abuse. All employees, including independent contractors and vendors who have access to sofix systems, are in charge of making sure their passwords are created and kept secure by following the instructions below.
2. Purpose (importance)  
   Establishing a uniform method for the safe use and safeguarding of all work-related passwords is the aim of this policy.
3. Scope   
   This policy is applicable to all workers, subcontractors, and suppliers who possess or are accountable for any password-required account (or access) on any system that is housed within sofix buildings, connects to the sofix network, or holds any confidential data pertaining to sofix.
4. Policy

* 4.1 Creating and Utilizing Passwords
  + 4.1.1 The Password Construction Guidelines shall apply to all passwords, both system and user level.   
    4.1.2 Users are required to create distinct passwords for every account they have connected to their jobs. No user may use a password associated with their place of work for a personal account.   
    4.1.3 Employees are permitted to safely keep and manage all of their work-related passwords by using authorized, approved password managers.   
    4.1.4 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges. Furthermore, it is strongly advised that any privileged accounts employ multi-factor authentication.
* 4.2 Changing Passwords
  + 4.2.1 Only in cases where there is a suspicion of compromise or when the password fails to comply to the specified Password Creation Requirements may changes be made to the password.
* 4.3 Security Passwords
  + 4.3.1 No one, not even coworkers or superiors, may obtain your passwords. Every password is regarded as private and sensitive sofix data.   
    4.3.2 Passwords must not be shared over the phone or included in email correspondence or other electronic correspondence.  
    4.3.3 Only password managers authorized by the organization may be used to store passwords.  
    4.3.4 You shouldn't utilize the "Remember Password" function in programs like web browsers.  
    4.3.5 Anyone who believes their password has been compromised has to update all pertinent passwords and report the event right once.
* 4.4 Multi-Factor Authentication
  + 4.4.1 Whenever possible, multi-factor authentication should be utilized for both personal and work-related accounts. It is highly recommended.
* 4.5 Password Encryption
  + 4.5.1 To prevent unwanted access, all passwords must be encrypted while they are in use and while they are in transit.  
    4.5.2 To safeguard the transfer of passwords over networks, data encryption protocols like SSL/TLS must be employed.  
    4.5.3 No password should be kept in clear text or in a format that is easily reversible. All passwords saved on any system must be encrypted using robust encryption techniques.  
    4.5.4 Any software or systems created for sofix must incorporate password encryption into its design and execution, according to application developers.

1. Policy Compliance

* 5.1 Compliance Measurement
  + - The Information Security (Infosec) team will use a variety of tools, such as business tool reports, internal and external audits, and input to the policy owner, to ensure adherence to this policy.
* 5.2 exceptions
  + - The Infosec team must first approve any deviations to this policy.
* 5.3 Failure to Comply
  + - If an employee is found to be in violation of this policy, they may be subject to disciplinary action, which may include losing their job.

1. Evaluation of the tools

* Password managers  
  For safely storing and organizing numerous passwords, authorized password managers are very useful tools. Employees can keep complicated, one-of-a-kind passwords for every account without having to learn them by using password managers, which improves security overall. However, it is essential to make sure that only verified and certified password managers are utilized, since if compromised, these technologies themselves turn into a single point of failure.
* Multi-factor authentication (MFA)  
  By requiring a second form of verification in addition to a password (such as a code given to a mobile device), MFA offers an extra degree of protection. This considerably lowers the possibility of unwanted access even in the event that a password is stolen. It is highly recommended by the policy to use MFA for personal and work-related accounts.
* Encryption  
  Passwords must be encrypted both in transit and at rest in order to prevent interception. Strong encryption techniques guarantee that password security even in the event that data is accessed by unauthorized parties. Compulsory use of encryption protocols such as SSL/TLS for network communication provides an additional layer of defense against eavesdropping and man-in-the-middle attacks. To prevent potential vulnerabilities like poor encryption algorithms or incorrect key management, encryption implementation must be carefully maintained.

## Remote Access Policy

1. Overview (importance)  
   For the team to remain productive, remote access to our corporate network is essential. Nevertheless, in contrast to our corporate setting, such access frequently comes from external networks that may already be compromised or have weaker security controls. Hypergolic Reactions, LLC has no control over these external networks, but we must take all reasonable precautions to reduce the hazards involved.
2. Purpose (importance)  
   Establishing the policies and procedures for connecting from any external device to the network of sofix is the aim of this policy. This policy is meant to reduce the risks that may face from improper usage of its resources. The company's reputation could be harmed, sensitive data could be lost, private company information could be revealed, vital internal systems could be interfered with, and these problems could result in financial obligations for the company.
3. Scope  
   All workers, independent contractors, suppliers, and representatives who connect to the sofix network using personal or company-owned devices are subject to this policy. It covers all remote access utilized for work-related activities, like sending and receiving emails and gaining access to intranet resources. All technical applications of remote access to sofix networks are covered under this policy.
4. Policy

Only workers, independent contractors, suppliers, and agents are permitted to access the general internet for personal use over the sofix network. Authorized Users are responsible for making sure that no unauthorized users have access to sofix resources or data when using a personal device to access the sofix network. It is strictly forbidden to engage in unlawful activities over the sofix network, and authorized users are responsible for any misuse of their access credentials.  
Sofix networks must not be used by Authorized Users for outside commercial purposes.

* + 4.1 Requirements
    - 4.1.1 The use of strong passphrases and VPNs, among other encryption techniques, is required to guarantee secure remote access. For further information, see the Password Policy and the Acceptable Encryption Policy.
    - 4.1.2 Authorized Users must keep their passwords and login information private, even from their relatives.
    - 4.1.3 Authorized Users must make sure the remote device is not concurrently connected to another network when using a company-owned device to remotely connect to the sofix network, with the exception of personal networks that are entirely under their control or the management of a third party.
    - 4.1.4 The most recent version of antivirus software needs to be installed on all devices, including personal ones, that are remotely linked to Sofix internal networks. The conditions outlined in the Third-Party Agreement must be followed by third-party connections.
    - 4.1.5 As stated in the Hardware and Software Configuration Standards for Remote Access, personal devices connecting to sofix's networks have to meet the same remote access standards as equipment owned by the company.

1. Policy Compliance

* 5.1 Compliance Measurement
  + The team responsible for information security (Infosec) will use a variety of techniques to make sure that this policy is followed, such as business tool reports, internal and external audits, and feedback sent to the policy owner.
* 5.2 Exceptions
  + The Infosec team must first approve any deviations to this policy.
* 5.3 Failure to Comply
  + Workers who disobey this policy could be disciplined, up to and including having their jobs terminated.

1. Evaluation of the tools

* Virtual Private Networks (VPNs)  
  it is used to create a secure connection between employees and sofix network to make sure that the data is protected, the vpn is important in remote access to protect against compromised networks if some employees conected from there.
* Anti-Virus Software  
  anti-virus is a vital layer of defense it protect form malicious software that try to take control of the remote connection and leak the information.

## Disaster recovery plan

1. Overview  
   Even though they happen rarely, disasters can significantly affect how businesses operate. Because disasters are uncommon, management frequently undervalues the significance of disaster recovery planning. However, sofix has a strategic advantage because they have a thorough contingency plan in place. This policy requires management to provide both operational and financial support for catastrophe recovery operations. Disasters are not just natural occurrences; any event that has the potential to result in extended service disruptions must to be taken into account. A crucial part of the entire business continuity plan is the disaster recovery plan.
2. Purpose   
   This policy's objective is to make it clear that Sofix needs a basic disaster recovery strategy. The steps for restoring IT systems, apps, and data in the case of a calamity that causes a sizable outage will be described in this plan. The plan will also define key metrics such as Recovery Time Objective (RTO) and Recovery Point Objective (RPO) and describe the backup documentation process, along with the different types of disaster recovery sites.
3. Scope  
   The sofix IT Management Staff, who oversee creating, testing, and maintaining the disaster recovery plan, are covered by this policy. The policy stipulates that backup plans must be established, RTO and RPO must be specified, and the utilization of hot, warm, and cold sites for disaster recovery must be documented.
4. Policy
   * 4.1 Contingency Plans
     + 4.1.1 Establish who should be alerted, when, and how in the event of a specific issue using your computer emergency response plan. List the urgent steps that must be taken in each of the scenarios.  
       Establish the chain of command in the event that normal employees are unable to carry out their duties.  
       Data analysis: Document the criticality and confidentiality of the data kept in systems.  
       List of Critical Services: Outline all services offered by Sofix and arrange them according to priority. The recovery order for both the short-term and long-term scenarios should be included in this list.  
       Plan for Data Backup and Restoration: Specify which data has to be backed up, what kind of media to use, where to store it, and how often to perform backups. Add the data recovery processes.  
       Backup Documentation: Keep complete records of all backup procedures, including timetables, guidelines for preservation, locations for storage, and the individuals in charge. To ensure accuracy, this documentation needs to be periodically checked and updated.  
       Equipment Replacement Plan: List the equipment required to get back into service, the equipment replacement priorities, and your recommended suppliers or vendors.
   * 4.2 Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
     + 4.2.1 Recovery Time Objective (RTO): To guarantee business continuity following a disaster, specify the longest period of time that can be given for the restoration of crucial systems, apps, and data. IT management and business stakeholders should determine and agree upon this timeline based on how vital each system is.  
       4.2.3 Recovery Point Objective (RPO): Define the longest period of time that can be tolerated before data loss occurs as a result of a significant occurrence. To establish acceptable data loss thresholds for each system, business units and the RPO should work together to set the parameters.
   * 4.3 Types of Disaster Recovery Sites
     + 4.3.1 HotSite**:** A fully operational off-site data center with real-time data replication and the ability to assume full production workloads almost immediately. This site will be maintained to mirror the production environment and is designed for quick recovery with minimal downtime.
     + 4.3.2 WarmSite**:** A partially equipped site that has hardware and connectivity established, but not live data. This site can be brought online more quickly than a cold site but requires additional time to restore data and services to full operation.
     + 4.3.3 ColdSite**:** A basic recovery site with minimal infrastructure. It lacks the equipment or data needed for immediate operation and requires extensive time to install hardware, restore data, and bring services online. This site is used for non-critical systems where recovery time is not as urgent.
5. Policy Compliance  
   5.1 Compliance Measurement  
   Through a variety of techniques, including regular walkthroughs, video monitoring, business tool reports, internal and external audits, and reporting to the policy owner, the Information Security (Infosec) team at sofix will make sure that this policy is followed.  
     
   5.2 Exceptions  
   The Infosec team must first approve any exception to this policy.  
     
   5.3 Failure to Comply  
   If an employee is discovered to be in breach of this policy, they may be disciplined or even have their employment terminated.
6. Evaluation of the tools

* Back up servers  
  this ensures that data loss is minimized and recovery is efficient and will help reduce the costs.