FINAL-SECURITY ASSIGNMENT

ABSTRACT

Information security: is essentially the practice of preventing unauthorized access, use, disclosure, disruption, modification, examination, recording or destruction of information. Information can be physical or electronic. The information can be anything like your details or we can say your social media profile, your mobile data, your biometrics, etc.

Hasan Alhwietat

Security

CONTENTS

INTERDICTION:

--A successful organization should have multiple layers of security in place: 1- Physical security 2- Personal security 3- Operations security 4- Communications security 5- Network security 6- Information security.

--Three characteristics of information must be protected by information security:

1- Integrity: Assurance that data is not altered or destroyed in an unauthorized manner.

2- Confidentiality: Protection of data from unauthorized disclosure to a third party.

3- Availability: Continuous operation of computing systems.

A.

1- Identify types of security risks:

Risk: The Likelihood of a Threat Exploiting a Vulnerability causing Damage.

- Natural: (example: flood, earthquake, diseases)

1- Spread of the virus covid-19 among employees.

2- A power failure may cause corruption or data loss.

3- The high temperature inside the data center room may cause a fire inside the organization.

- Human benign Intent : (human error)

1- Coffee spilling on the device by mistake.

2- Send an email to someone by mistake.

3- Delete an important file by mistake.

- Human malicious intent Directed: (example: Impersonation, espionage)

1- The data center can be attacked because the door is always open.

2- Data transmitted from employees who work from their homes to the data center can be stolen because of Misconfiguration on VPN.

3- The organization's network can be attacked and disrupted because all devices are connected to the same subnet.

- Human malicious intent Random: (example: malicious code on a public website, phishing)

1- DDOS attack will occur due to misconfiguration of firewalls.

2- When data is transferred from wind farms or solar energy to a data center, data theft can occur.

3- Malware attacks can cause data breaches or data loss because some devices are not secured.

2- Proposing a method to assess them. (Likelihood, impact)

Assess: It is a process through which potential risks are identified and what could happen in the event of a risk and its impact on business.

--Risk Assessments: **Risk = Impact x Likelihood**

Impact Likelihood	Low	Medium	High	Critical
Almost certain		When data is transferred from wind farms or solar energy to a data center, data theft can occur (It will affect the standards that the organization follows in order to protect data because it is possible that information may be stolen for the purposes of sabotage and that the data may be changed or deleted).	DDOS attack will occur due to misconfiguration of firewalls (It will affect all employees working in the organization, causing disruption in traffic and it is possible to send malware or viruses to devices).	The data center can be attacked because the door is always open (It will affect the protection of the database and the devices inside the room, because anyone in the organization can enter the room, which makes the devices vulnerable).
Likely			Data transmitted from employees who work from their homes to the data center can be stolen because of Misconfiguration on VPN (It will affect the policy of the organization because the organization has made a decision about employees working from their homes and it will affect the protection of data when it is transferred to the data center and thus the data may be exposed to theft, change or deletion).	The high temperature inside the data center room may cause a fire inside the organization (It will lead to the destruction of the equipment inside the room and it may cause a fire to the entire building, which leads to data corruption).
Possible	Coffee spilling on the device by mistake (It will affect the device, it may cause damage or malfunction, and	Spread of the virus covid-19 among employees (It will affect the health of employees and thus will affect the continuation of business in the organization, which will affect its profits).	The organization's network can be attacked and disrupted because all devices are connected to the same subnet (It will affect the performance of the	

	therefore the stored data may be lost).		network and slow it down because everyone in the organization uses the same network, and therefore it will become easy for the attackers to destroy or disrupt the network, This causes the business not to continue).	
Unlikely		Malware attacks can cause data breaches or data loss because some devices are not secured (It will affect the performance of the devices or disrupt them because they can be hacked by hackers and spread viruses and malware. Because it is not protected).	Send an email to someone by mistake. (It will affect the confidentiality of the data, which will affect the person who sent the mail to leak information and publish it through the sites).	
Rare	A power failure may cause corruption or data loss (It will lead to the non-continuity of business, which affects the loss of data that was not stored before the power outage).		Delete an important file by mistake. (It will affect the content of the data it has stored inside the file and therefore It will affect business continuity).	

3- Proposing a method to treat them.

It is a process through which risks are addressed by implementing security measures and procedures to avoid risks. These measures include either Avoiding, Mitigation, Transferring or Acceptance risks.

OPTION	Risks	TREATMENT
Avoidance	1- When data is transferred from wind farms or solar energy to a data center, data theft can occur.	Data theft will be avoided during its transfer, and this will be done by encrypting the data before transferring it to be secure, and in the event of theft, the content of the data will not be known.
	2- DDOS attack will occur due to misconfiguration of firewalls.	Any attack will be avoided in order to attempt to steal data. We will contact someone who is expert in firewall configurations to avoid any possible threat that affects data security.
	3- The data center can be attacked because the door is always open.	It will be avoided that the door always remains open to protect the servers and devices inside the room by placing a security door that opens via a smart card, password or fingerprint, and installing CCTV cameras to prevent any unauthorized person from entering.
	4- Data transmitted from employees who work from their homes to the data center can be stolen because of Misconfiguration on VPN.	Any attack will be avoided in order to try to steal the data that is transferred from the employee to the data center. We will contact an expert in VPN configurations to suit the requirements of the organization and protect the transmitted data and we can implement data encryption.
	5- The high temperature inside the data center room may cause a fire inside the organization.	Overheating in the data center room will be avoided and therefore we will install cooling systems that will help avoid hardware damage or data loss.
	6- Spread of the virus covid-19 among employees.	The infection of all employees in the company will be avoided, and a rotation system will be implemented between employees to reduce the spread of disease.
	7- The organization's network can be attacked and disrupted because all devices are connected to the same subnet.	Attacks on the network will be avoided and will be avoided by applying DMZ, which will help protect the internal network and prevent hackers from accessing sensitive data. Also, NAT can be implemented, which will help to hide IP addresses, making the network more secure and less vulnerable.
	8- Malware attacks can cause data breaches or data loss because some devices are not secured.	Any malicious attacks will be avoided on the devices by downloading anti-virus software to help prevent any virus from trying to penetrate and destroy some data.

	9-A power failure may cause corruption or data loss	The occurrence of power outages will be avoided by providing machines that generate power for the entire organization to prevent any disruption in work or loss of
	10- Coffee spilling on the device by mistake.	This will be avoided by preventing anyone from bringing any drinks into the workrooms. This can be addressed by allocating a special room for rest, where you can drink drinks and eat food.
	11- Send an email to someone by mistake.	This will be avoided by placing a sign informing employees of the necessity of making sure of the addressee before sending the email.
	12- Delete an important file by mistake.	This will be avoided by making a backup of the data that is deleted in the event that the data is important and was deleted, he can recover it.

B. DISCUSS RISK ASSESSMENT PROCEDURES.

Step assessment risk: Determining the risks that can occur and affect the organization from conducting its work and help to identify risks and take measures and actions to reduce risks

1- Identifying potential risk: It is the first stage in the assessment of risks, which is done by identifying the risks that could negatively affect the work of the organization, and these disasters that are evaluated include natural disasters, electronic attacks, and others.

2- Identifying who might be harmed by those risks: After identifying the risks, it will be determined what are the things that will negatively affect the work of the organization.

3- Evaluating risk (severity and likelihood) and establishing suitable precautions: Risk assessment helps to develop control measures, analyze risks, how the organization will be affected by these risks, how the risks can be reduced or eliminated, the financial losses that may occur in the event that the risk is effective, and the interruption of work in the event of disaster recovery.

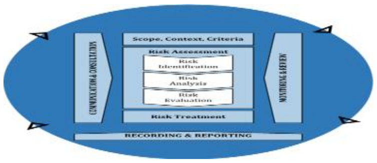
4- Implementing controls and recording your findings: Recording all the results of the risk assessment and submitting them in the form of official documents to the responsible department, which must include details of the risks that may occur and plans to prevent risks.

5- Reviewing your assessment and replay assessing if necessary: There may be a change in the risks that may occur and their impact resulting from the risks, so evaluations must be up-to-date to adapt to developments.

C. EXPLAIN HOW YOU CAN TAKE BENEFIT OF THE ISO RISK MANAGEMENT METHODOLOGY BY SUMMARIZING IT AND HIGHLIGHTING ITS APPLICATION IN IT SECURITY OF THIS PROJECT.

Explanation of ISO 31000: These standards were developed to help organizations manage risks through (International Standards Organization). Risk management: is the structure that is developed and how it can be managed. The structure consists of clear principles and a distinct framework through which the foundations and processes for effective risk management are built. It should consist of a detailed framework within the organization of four main committees, namely design, implementation, review, monitoring and continuous improvement. It does not provide fully detailed standards, instructions and requirements on how to manage risks in a specific way that remains at a general level. Therefore, standard 31000 is innovative in several areas: 1- It presents new definitions of risks with regard to the possibility of achieving the organization's goals, and highlights the importance of setting goals before trying to control risks and emphasizing the role of uncertainty. 2- It presents a controversial idea about the willingness to risk despite the level of risk that the organization accepts in return for the high financial value. 3- It defines a framework for managing all risks with different organizational procedures, responsibilities and roles in managing these risks. 4- Defining the management philosophy where risk management is seen as something unimportant that must be resolved or changed.

The processes that must be developed that make up the risk management process:



1- Communication and consultation:

Communication: It is a two-way process, first by listening to the person who is speaking and thinking about what he says, secondly being the speaker and being listened to. People communicate well and it is easy to discuss important information.

Consultation: It is the process through which the development of systems, policies, important issues and practices must be discussed, and this comes by searching for solutions to problems through the sharing of opinions and information among the members of the organization. Management must make the final decision.

Management must listen to and take into account the views of staff. The organization must consider the impact of this risk on the safety of staff and visitors. It includes structured consultation that takes the opinions of employees into consideration before making a decision. There should be communication between management and employees to exchange information. The consultation should reach an acceptable result that satisfies all parties and move towards a safe environment. Counselling cannot be viewed as a legal thing or matter. But it is a way to improve the organization's decision-making process on safety and health and it is an opportunity to bring about new positive changes.

2- Context: This is the process that most security risk management practitioners fail to understand. Therefore, the internal organizational structure must be fully appreciated and the goals of the organization must be achieved or maintained if they want to build an effective and distinctive plan. The most important thing is the organization’s environment from the outside, and an informed image must be obtained for all stakeholders in the early and final stages, based on which a strong treatment plan can be built and risk criteria are identified that reflect the organization’s goals and requirements.

3- Identification of risks: This step is characterized by showing all sources of risks or threats to the organization and its ability to avoid these risks. It is important to verify the correctness of the information used to prove credibility and that the threat or risks actually exist in the organization, so when this list exists, we can begin to understand it, the possibility of its occurrence and its impact on the organization.

4-risk analysis: After identifying the risks, you must understand the causes of the specific risks. The risks must be analyzed and studied, and the consequences thereof in view of the controls. To determine the level of other risks. Risk analysis is the understanding of the characteristics and nature of risks, consequences, possibilities and events that result from risks.

5- Risk assessment: The risks identified and their likelihood of occurrence should be considered. It is important that we implement a strong systematic and objective analysis of risks, taking into account expert advice and listening to their advice. If the organization fails to apply accurate analysis, either they reduce the impact of risks on the organization's goals and the possibility of these risks occurring.

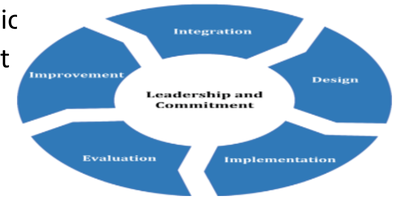
6- Risk evaluation: In this process, we take the results of the risk analysis where maps are drawn to assess the risks against the context. Therefore, the importance of determining the organization's desire and tolerance for risks is important and extremely important during risk assessment, and priorities must be set to address risks if necessary, and that it causes a significant danger to the organization.

7- Risk treatment: the importance of risk treatment to remove or reduce risks to a practical level that protects the organization in the event that the necessary treatment is not achieved. Risks must be re-evaluated in order to avoid or accept, with the importance of balancing cost and effort. Addressing risks is part of any mitigation plan. It can lead to new risks and new risks must be evaluated.

8- Monitoring and review: The importance of monitoring, reviewing and auditing is to improve the quality and effectiveness of the design, execution of orders and their results. Risks should be reviewed and monitored periodically because they are part of risk management. This process includes planning, gathering and analyzing information, and presenting results to management.

9- Recording and reporting:

Any risks, including risk assessment, must be documented and reported using the appropriate mechanism. This aims to: Communicate the results of risk management to the organizatic important information to management for decision-making. Improving risk management Reliable information should be taken, retained and, if possible, processed.



Security risk management can have consequences for an organization if not done properly. Understand the organization's values and goals and use a robust framework for risk assessment and analysis. There are many security risk management practices that hinder the achievement of the business objective through poor management plans.

The framework helps the organization manage risks in critical activities and functions. The effectiveness of risk management depends on its integration into the organization, including its decision-making process. This requires support from the organization, especially the top management.

The organization must evaluate risk management processes and practices, and assess and address any gaps in the framework. The components of the framework and the way in which they operate must be customized by the organization. Components of the framework are:

1- Leadership and Commitment: Management bodies must obtain supreme oversight when there are risks in the organization and all organizational activities. Demonstrate leadership and commitment by implementing the components of the framework and issuing a statement outlining the followed plan or course of action and ensuring the availability of materials necessary to manage risks will help the organization maintain its goals and its cultures.

2- Integration: Risk management requires an understanding of organizational structures and internal and external contexts. The structures differ from each other according to the organization and its goals, and each individual in the organization bears responsibility for managing risks.

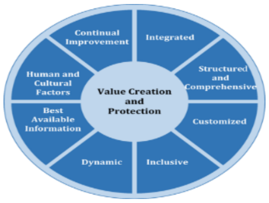
3- Design: When an organization wants a framework for risk management, it must understand its external and internal contexts and examinations, and includes the cultural, social and technological factors of the organization, and it must continue to manage risks and ensure its commitment and that it is responsible for any risks that may occur and allocate appropriate resources to manage the risks.

4- Implementation: The risk management in the organization must implement the framework and identify any issues that may occur and any matter that may be taken. The framework must be implemented correctly in order to be addressed.

5- Evaluation: The organization must evaluate the framework that has been made by the risk management body, measure the framework's performance on an ongoing basis, and determine if something has not been implemented.

6- Improvement: The organization must monitor the risk management framework to address internal and external risks. The organization can expand its goals. The organization must improve the risk management framework and ensure its effectiveness continuously and develop plans and tasks to enhance these improvements. The importance of risk management is to create and protect value. It improves performance, encourages innovation and supports the achievement of goals. The principles shown in the figure provide guidance on the characteristics of effective and effective risk management, clarify its value and clarify its purpose and purpose. Principles are the basis for risk management and must be taken into account when creating a framework for managing risk and operations in an organization. These principles should enable the organization to manage the effects of uncertainty on its objectives.

The principles can be explained as follows:


Continual Improvement
Integrated
Human and Cultural Factors
Value Creation and Protection
Structured and Comprehensive
Best Available Information
Customized
Dynamic
Inclusive

1- Integrated: risk management is part of organizational activities.

2- Structured and comprehensive: structured and comprehensive approaches to risk management must be followed to achieve comparable and most consistent results.

3- Customized: A risk management framework must be allocated to the organization in relation to its special needs, including its objectives and the internal and external context in which the organization operates.

4- Inclusive: Risk management must be more effective and include all sectors of the organization in appropriate ways, and listening to the views and perceptions of all risks leads to improved awareness.

5- Dynamic: risks can appear or disappear with the change of its external and internal course of the organization. Risk management predicts through changes and events, discovers them and solves them in a timely manner.

6- The best available information: Risk management works by looking at new and old information as well as predicting what might happen in the future. Therefore, new and old information must be reliable. Risk management must take into account the limitations related to past and current information.

7- Human and Cultural Factors: Risk management is a human activity and falls within one or more cultures, such as an organizational culture. The risk tool must be fully aware of human and cultural factors and know the effects that occur on these factors by making great efforts.

8- Continual improvement: Risk management must improve themselves through learning, experience, and effort.

ISO 31000 will help manage the risks in the organization, help achieve goals, identify risks and threats, and use them in addressing risks. The reason for using ISO 31000 is because it provides guidance for audit programs and principles for risk management. It will help the organization reduce risks. One of the most important applications of ISO 31000 is to educate employees, provide security instructions that must be adhered to, and explain the importance of following security conditions, including that the office is clean, free of any important information that could harm the organization, and that it is fully responsible for the security of its device, so it must update the antiviruses program daily to prevent Entering any viruses on his device.

D. RECOMMEND WAYS TO IMPROVE IT SECURITY VIA:

1- DESCRIBING DIFFERENT SECURITY PROCEDURES THAT X-POWER COULD APPLY TO PROTECT BUSINESS CRITICAL DATA AND EQUIPMENT.

X-power Security Procedures:

1- Only authorized employees can enter the system and access the information.

2- Permission must be obtained from the administration before going to the data center.

3- Employees must obtain permission from management when they want to modify or delete any information within the database.

4- Installing cooling devices in the data center room to avoid equipment damage or data loss due to high temperatures.

5- Ensure that there are safety tools from fire extinguishers and others.

6- Data must be backed up to protect it.

7- Installing security doors that open with a fingerprint or password for important rooms to prevent anyone from entering them.

8- A security man was placed at the main gate of the organization to conduct an inspection.

9- Create and test a disaster recovery plan before any disaster strikes.

10- Maintaining the safety of employees and making some of them work from their homes to reduce the spread of epidemics.

2- Explaining data protection processes and regulations that might help X-Power to enhance IT security.

Data protection: It is a process by which data is protected from theft or damage and the ability to recover data in the event of loss, inability to access or inability to use the data. Where data is protected, authorized persons must be allowed to access the data, and the data must be available when it is needed and can be used and modified.

Data protection (backup and restore) includes data security and privacy. The organization must protect the data, store the information in the database, and make sure of the people who are allowed to access this data. Principle of data protection when personal data collection occurs it is processed by the organization and it must treat the data in accordance with the protection law. Data privacy is typically applied to personally identifiable information (PII).

General Data Protection Regulation: It is a legal framework that contains guidelines for the collection and processing of personal information from individuals who work in the organization. This is because the regulation does not apply to where websites are located. The GDPR grants visitors to the organization a number of data disclosures. It must take steps to facilitate consumer rights in the organization as timely notification in the event of a personal data breach. The widespread use of sensitive personal data indicates the importance of protecting this data from loss and theft, so global authorities have taken compliance with the General Data Protection Regulation.

These x-power regulations (PII) help protect the data of researchers and not disclose it to anyone because of important data. The work of security cards to enter the important rooms to protect the data and fixing of CCTV cameras be placed to know the people entering the organization. And make back up the data to protect the data from loss, disasters, or the system stops working, protecting it from malicious programs, and the possibility of quickly recovering data.

Six principles of data protection:

1- Fairness, Lawfulness, and Transparency: The organization needs to ensure that the information collected does not violate laws and that it does not conceal any information about data subjects. Specifies the type of data being collected and the reason for it being collected.

2- Purpose limitation: The organization must collect data only for a specific purpose and determine what is the purpose and collect data only for necessity and the data is processed for the purposes of scientific or statistical archiving.

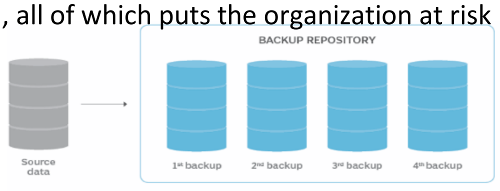
3- Data miniaturization: The organization must process the data they need and carry out the processing. It has two benefits: First, when a data breach occurs, any unauthorized person will not be able to access only a few and limited information. Secondly, when processing the data, the data is reduced and it becomes easier to maintain and update the data accuracy.

4- Accuracy: Data must be accurate to help understand what needs to be protected. The GDPR states that every reasonable step must be taken to correct inaccurate or incomplete data in order to avoid a high risk of data loss.

5- Storage Restrictions: The organization must delete the data when it is no longer necessary to keep it or when the process that the user wants is finished.

6- Integrity and Confidentiality: The GDPR provides that data must be protected and confidential. Therefore, it is processed in a safe manner to protect it from penetration using technical measures. The General Data Protection Regulation deliberately hides the measures that help organizations to take because most technological organizations are constantly changing. The organization must encrypt data to protect it if it is stolen.

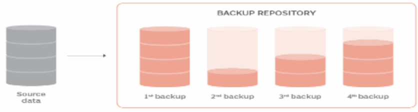
7- Accountability: The organization must take responsibility when using and processing data, as it is responsible for complying with data protection standards and showing the management that the data is properly protected and there is no stolen data or any lost data, all of which puts the organization at risk and exposes it to legal issues.



Type back up:

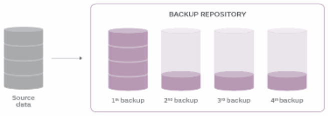
1-**Full backup:**

It is a complete copy of the protected data every time the backup process occurs, the data is completely copied. When performing data recovery, it is characterized by the speed of recovery and simplicity, but it needs a large storage space, and the full backup process takes a long time, and all copies must be protected and data encrypted because if infiltration is done to the version of the data will the full information be obtained



2-**Differential backup:**

It is a backup copy of the data that has changed since the last full backup and is characterized by the speed of creating a backup copy and the storage capacity is not large and helps to reduce the risks due to data loss and reduce the number of backup copies of the records to be restored, but it takes a long time when recovering data and is suitable for a database data.



3-**Incremental backup:**

It is a backup copy of the data that has changed since the last backup and it does not have to be a full backup and is used when the amount of data that must be protected is huge because it saves time to restore data and provides storage space and a small number of backup files, but it takes longer than copies Full back up when restoring data because you must restore the latest full backup and all incremental backups, but when one backup is missing, it will be difficult to recover the data completely.

3- Discussing the benefits of IT security audit and its impact to X-Power IT security.

IT security audit: It is a complete assessment of the security situation of the organization and the information technology infrastructure and helps in conducting audits on the security of the technology in the organization and finding weaknesses within networks, databases and devices connected to the network and evaluating them to fix security holes in the organization.

This is done by examining security vulnerabilities to discover these vulnerabilities or doing a penetration test for unauthorized access to networks and databases. Reports are submitted after the breach and the necessary measures are implemented to protect the organization.

Benefits of an IT security audit: A security audit reveals weaknesses and security risks to the organization, and when identifying risks, it makes it easy and doubly secure.

1- Detection of security vulnerabilities: Upon verification, a vulnerability can be found that was not discovered before it occurred. For example, we have a problem with the firewall configuration, so this is a weak point and must be addressed before hackers discover it. This saves a lot of time and effort and ensures that data is not stolen.

2- Evaluation of training and educational efforts: When the monitors are trained and they receive specialized courses in data protection, they have sufficient experience to deal with risks, so they have sufficient ability to solve the problem and prevent danger, so the organization becomes safe, and the monitors must pursue education and gain the necessary expertise.

3- Ensure regulatory compliance: The organization must follow data protection laws and standards and the security audit will ensure that the business remains in compliance.

4- Learn about new technologies and processes: When there are new technologies and processes in such ideal opportunities to learn more about new technologies and developments can be tested and subjected to a safe environment.

5- Reducing costs: When the risks are discovered by the audit, they reduce the risks that may occur and therefore they will be addressed with an amount of money and save the organization the financial losses that may occur because this will prevent potential breaches and violations.

IT security audit impact the reduction of risks in the organization and reveals security holes that were not discovered before or this vulnerability was found when the organization develops and makes data protected and reduces large financial losses that may be caused by risks, so it helps to improve security in the organization.

E. DISCUSS, IN DETAILS, THE SECURITY IMPACT OF ANY MISALIGNMENT OF IT SECURITY WITH X-POWER POLICY.

How does the process of aligning IT security with organizational policy happen?

Since the security measures will comply with the organization’s policies and objectives, and therefore a strong security plan will be formed, and the organization’s security procedures must be updated every period to ensure that the security is advanced, modern and ideal for the organization, and therefore information technology security will comply with the organization’s policies and standers.

Detailing the security impact of any misalignment X-Power policy:

There must be security compatibility with the goals of the organization to become compatible with the needs of the organization, not security is the most important priority for the emerging organization and to develop in its goals. But how does the incompatibility of information technology security with the organization's policy happen? When the organization is exposed to hacking, it contradicts its plans and therefore there will be no development for the organization because it is insecure and in violation of the General Data Protection Law. A security check of the organization must be carried out every period to ensure the integrity of the data and compliance with security standards and regulations for the growth and progress of the organization.

For example, we have misconfigurations of VPN and firewall, so we may a defect occurs in the data protection of employees or researchers, this is not compatible with IT security with the X-power and therefore the organization may be fined because it violates the laws and thus the number of researchers decreases because it does not protect their personal data.

F. DESIGN AND IMPLEMENT A SECURITY POLICY FOR X-POWER.

Organizational Security Policy: It is a set of procedures and rules imposed on an organization to protect sensitive data.

Security policy for X-Power:

1- Accessibility policy: Allow researchers to enter the organization's website by creating a new account by entering the full name, email and password in order to conduct research and allow EDCO and JEPCO to access the organization's website. And allowing employees to work from home to reduce the spread of covid-19 among employees via VPN.

2- Identification and Authentication policy: Each employee of the company must be given an identification card that allows him to enter the organization.

3- password policy: Employees must change the password And that the new password consists of 8-16 characters, numbers, or symbols that were not used in the past, and that it is changed every month or two, making sure that the password is free from the user name, phone number, or any personal information.

4- Encryption data: When data is transmitted from wind and solar farms, all data will be encrypted before being transferred to the data center to avoid any data theft attack.

5- Backup policy: Back up the database to avoid any damage to the devices or loss of dataThe data is copied every week.

6- Server policy: Ensure that the servers are safe from viruses and that they work well every week and that there are no defects.

7- Wi-Fi policy: Ensuring the security of the network on which the organization operates, and making sure that only employees use the organization's network this is done by using (Enterprise mode) when you want to connect to the network it asks for a username and password.

8- Website policy: Ensure that the site works on HTTPs for data security TLS must be purchased for the organization's site in order to increase the protection of sensitive data so that criminals cannot change any information that is transferred to the database.

9- Physical policy: Putting secure doors on the important rooms in the organization so that only people who are allowed to enter can enter these rooms. And Putting CCTV cameras in the organization to monitor any things that may happen inside the building. And Inspection devices can be placed in front of the main doors of the organization to inspect the people who enter the organization and make sure that there are no devices that might affect with the organization.

10- Personnel Policies: All employees must sign and adhere to the organization's policy periodically. Divides tasks between employees. Change roles the employees on a regular basis to forbid continuing with fraud. The employee must clean his area because it reduces the risk of data theft from the data is the password or important paper. When an employee resigns in the organization, all its features must be disabled. And the signing of the non-disclosure of any evil of the secrets of the organization is called the agreement (non-disclosure agreement) and he will be punished if he violates the terms.

11- Putting sensors in firewalls to verify the data that enters the database and preventing the attacker from entering it, and placing sensors when the data leaves the database to verify the data that goes out to the employees who are allowed to access.

12-Vulnerability Scanning should be done for the organization's website and devices to discover security holes and vulnerabilities every six months

13-Every employee must update their antivirus software every day before starting work.

G. EVALUATE THE SUITABILITY OF THE TOOLS USED IN THIS POLICY.

Tools	Suitability	Effectiveness	Where help
1- Firewalls	Very strong and difficult to penetrate and keeps the devices safe from penetration. It acts as a barrier between traffic and external sources	It will monitor all network traffic and prevent any malicious and unwanted traffic or attacks on the system.	It will help prevent attackers from accessing the data and any threats such as Trojan horses.
2- Encryption	No one can decrypt it because it is difficult to obtain the encryption method because it is intricately designed and dedicated to data protection.	The data will remain encrypted until it reaches the database and when it arrives, the system will have a way to encrypt the data and thus the data will be protected.	It will help when transferring data to Database. When any breach occurs, and data will be obtained during the transfer. This data will not be restricted because it has been encrypted.
3- Antiviruses software	It does not protect devices strongly, but it prevents viruses from entering the devices by reviewing the anti-virus program if it knows that this file contains a virus that stops the file.	Antivirus software will not give you 100% effectiveness, but it is a security precaution to remove any viruses present on the device. It is additional protection if there are firewalls.	It will help protect files and devices from malicious software such as spyware and worms.
5- Vulnerability Scanning	It detects vulnerabilities and security breaches that can affect the network and make data vulnerable. It is useful to	It will keep the network secure because it contains important information and work to reduce the	It will help identify the gaps and weaknesses on the network to maintain the security of the network

	know and fix vulnerabilities to increase security.	vulnerabilities that are discovered.	
6- backup	The most important way to preserve and protect data from loss or theft, and the data will be transferred to a safe place and this data will be restored at any time	It works on copying the data in the database. If anything happens to the database, all data will be retrieved because it is kept in a safe place and no data theft will occur.	It will help preserve the data if there is a loss of data and damage to the devices, which leads to the absence of any data.
7- VPN	It protects you from the possibility of the hacker accessing the data and it does this by hiding the traffic that hackers cannot decrypt until they can access it. It also hides all the activities you have done on the network. You can also enter sites that are not accessible in your area and choose the country that you want your site to appear on.	It will benefit the organization in transferring data between employees and transferring it to the data center without the occurrence of any theft or data leakage and encrypting it to connect it to the center.	It helps encrypt your online traffic and hide your identity making it difficult to track your activity by hackers and difficult to steal data.
8- TLS	Since there are many ways to protect data, it is the best way to transfer data without any data theft.	It is useful for the organization when transferring data from wind farms or solar energy to the data center without any theft and it is encrypted purposes from eavesdropping.	It will help encrypt data transmitted over the Internet to prevent hackers from seeing data such as passwords and credit numbers and can be used for email and transfer of important files.
9- Enterprise mode	This is the most secure and complex network security mode because obtaining the user name and password to enter the network requires authentication with the database used to connect to the network and may require great effort as well as additional time.	It is useful in the ease of protection from any unauthorized access from any user, increases the security of the network and improves its performance, as it cannot detect any weaknesses, and it is the most secure way to access the network.	It will help in the security of the network and the inability of any visitor to enter the organization’s network and use it. It is useful in the event of any device being lost. The password can be changed for one user without the need to change all passwords with minimal effort and simplicity.
10-change password	Since devices contain sensitive and important data, maintaining it is one of the main priorities for data protection is to change the password constantly because it helps to avoid risks, including preventing anyone	It will reduce the security risks to the organization and make sure that there is no hacker who wants to access the organization’s data because the password will be changed every period and so the hacker	Changing the password helps in the security of employee accounts and protect their private information because it is sensitive data and harms the organization if any theft happens to it, and the organization will be fined

	from accessing the data. When changing the password, it must be new and not related to any personal information.	cannot penetrate the security because it takes a lot of time to try to hack.	sums of money because of that and make sure that you are the only person who can access your account.
11-non-disclosure agreement	This agreement will fit the organization because all employees will sign this agreement on an ongoing basis in order to ensure continued safety and security, and when the agreement is violated, the violating employees will be punished.	All employees of the organization will sign this agreement in order to protect the secrets of the organization.	It will help to maintain important information and keep it confidential and not divulge it because it will preserve the secrets of the organization.
12- Physical policy	The secured doors will comply with the security standards because they will prevent unrelated people from entering these rooms, as well as surveillance cameras and security inspections will limit intrusion attempts.	This will help to avoid anyone entering the data room, and anyone who may cause risks to the organization will be monitored, and the security inspection will also reduce the attempt of anyone to plant any viruses on the devices.	It will help protect important data because only authorized personnel will be allowed to enter the rooms. Cameras will help in detecting and reporting people who may attack the organization at night, as well as inspections will help in identifying the people entering the organization and knowing if they have anything that might harm the organization.

H. A DISCUSSION OF THE ROLES OF STAKEHOLDERS IN THE X-POWER TO IMPLEMENT SECURITY AUDIT RECOMMENDATIONS.

Stakeholders:-

1- CEO: He is the person with the highest rank in the organization who can sign security agreements or treaties with companies in order to provide the necessary protection and take decisions regarding the purchase of the latest security devices and servers and punish anyone who violates laws and regulations and can dismiss and promote employees.

2- Chief Information Security Officer: He is the chief data security officer who can build security strategies and is responsible for protecting the organization. He directs employees and defines instructions and processes, develops and implements them, and maintains systems to reduce risks. He fully supervises the employee at work and is responsible for protecting the organization’s information and responsible for its growth, development, business continuity and disaster recovery.

3- Audit committee: Its purpose is to audit and review the processes that have occurred within the organization, prepare reports and comply with the laws of security regulations, and it searches for any possible impact that affects the security of information. It makes reports on whether this affects the integrity of the data. It analyzes and audits and informs the management of any weaknesses that they have discovered.

4- Security analysis: Analyzes the organization's security systems in order to protect data and help maintain security standards and must identify flaws in the organization Installs firewalls and encryption programs to protect data from unauthorized persons Can check for weaknesses within the network and inform technology personnel to take security measures and must Update security programs and prevent any electronic attacks.

5- Security officer: He must provide a safe environment for the organization, monitor employees, inspect visitors to prevent any security breaches that may occur, protect equipment, and alert employees to follow and abide by laws.

6- Information security: It must prevent unauthorized access, be able to protect data stored or used, protect technology systems, stop malicious programs and hack attacks, prevent any threat to the organization, comply with the GDPR, identify and address risks.

7- Network Security: It protects the network from any intrusion and vulnerabilities found by addressing them and performs network-related configurations, accessibility and network analytics Responsible for endpoint and web security and VPN and firewalls configurations Responsible for network performance and email security.

I. LIST THE MAIN COMPONENTS OF AN ORGANIZATIONAL DISASTER RECOVERY PLAN, JUSTIFYING THE REASONS FOR INCLUSION.

DRP: It is a series of steps and measures that will be taken for the organization to resume business after disaster strikes.

1- Documentation: The disaster list for the IT infrastructure should contain both hardware, software and a disaster team and contain a list of team members and their contact information and take action to resume business operations Documents should be kept up-to-date to comply with IT changes and are well-designed and meticulously designed documents To take a shorter recovery time and when any accidents occur, he must follow these procedures, evaluate the impact on the business, and back up these documents to restore them.

2- Scope and Dependencies: When a disaster occurs, it is not possible to recover all the information that has been lost because not all data is of the same importance in order to ensure business continuity. Select the most important devices in the organization to ensure recovery as soon as possible because they contain important applications, systems and information.

3- Responsible Team and Staff Training: The disaster recovery plan should have employees and officials to coordinate the recovery plan who communicate the plan to all staff in order to eliminate risks and in the event of any disaster they will work to recover data and start the recovery plan in a timely manner.

4- Secondary Location Configuration: You must have another site that does not share with the main site to avoid the site being exposed to the same disasters, which is to ensure the protection of resources and data from loss and loss. To carry the work transferred to the secondary site.

5- Setting (RTO) and (RPO) (Specify backup and off-site storage procedures): Recovery time and recovery goals are a measure associated with recovery documents. The RTO determines the length of time that can take without operating the system or equipment. The RPO determines the amount of data that can be lost in the work of the organization. Both RPO and RTO should be as close to zero as possible. But it is very expensive, but as much as it is expensive, it makes the devices non-stop for long periods.

6- Testing and Optimization: A disaster recovery plan that has not been tested cannot be considered effective because it is not enough to have a plan only because when it is tested, weaknesses will be discovered and some inconsistencies in the plan will be identified because the disaster recovery plan is a critical step that helps to gain confidence that No failure will occur in the attempt to retrieve the data. Also, optimization is an important part of the success of the plan. These improvements and upgrades to the IT infrastructure occur regularly.

7- Automation: Disaster recovery plan allows from disaster recovery to reboots, and automation frees IT managers from reducing the burden and complexity, making the recovery process take less time and is not at risk. Thus, automation saves time and money to reduce downtime.

REFERENCES:-

1- https://www.360factors.com/blog/five-steps-of-risk-management-process/

2- https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:en

3- https://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018

4- https://www.theupcoming.co.uk/2020/11/23/the-benefits-of-getting-an-it-security-audit/

5- 13_Implementing Policies to Mitigate Risks.pdf

6- https://info.knowledgeleader.com/what-is-organizational-alignment-risk

7- https://www.techtarget.com/searchsecurity/definition/security-policy

8- https://www.investopedia.com/terms/s/stakeholder.asp

9- 12_Audits and testing procedures_Risk Management.pdf