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

**Security**

**10203280**

**(D/618/7406)**

**Assignment Title**

Warmaksan

Assignment 9

**Submitted to**

Dr. Heba Alawneh

**Submitted by**

Yousef AbuAli

2022/2023(Fall Semester)

**Contents**

**Part1**............................................................................................................................

* Report regarding IT security for Warmaksan:

1. critical assets of the Warmaksan's system……………...…………. page 3.
2. Discuss and assess Warmaksan system's possible risks…………...page 4.
3. Suggest the possible controls/countermeasures initially used by

the company to protect their asset.……………...page 11.

* Security threat risk assessment table……………. page13.

1. ways to improve Warmaksan's IT security:
2. Describing and assessing different security controls………page14.
3. Explaining data protection processes……...page16.
4. Analyzing the IT security audit and its impact…...page18.
5. Reviewing the risk assessment procedures………. Page20.
6. Explaining benefits of risk management………...page20.
7. The impact of misalignment of IT security……. Page23.
8. Warmaksan’s security policy………...page24.
9. Justifing the developed security plan……...page26.
10. Evaluating the tools in the security policy……page27.
11. Roles of stakeholders in the Warmaksan……. Page28.

Student declaration form……………………………………………………. page30.

**References**.......................................................................................................page31.

**Part 1**

1. The purpose of identifying essential assets is to decide how resources should be distributed and to create a suitable security structure that lowers the risks related to a potential breach of these assets. Every important, successful, well-known company makes a huge effort and pays a substantial wage in order to protect their assets, such as their hardware, software, and data in order to maintain the information system’s confidentiality, integrity, and availability. The hardware assets for example such as the servers, laptops, end devices, and all physical devices can be affected by several factors that can cause to lack of availability of this hardware component. Such as, losing the device by theft or damage, or device failure due to an intentional failure or other causes. The company must consider hardware replacement costs, disruption losses, and recovery costs in case of any incidents.

Moving forward to the software assets, that includes applications, operating systems, database management system, and all the company’s system software that are important for the company to keep functioning. Here, the availability is critical because employees need them to be available in order to use what’s inside them of information’s. Another important asset is data and information assets, all the data and information’s in the company has to be protected from any potential risk that might occur, such as the loss of information or the theft and unauthorized access to the company’s important information, because someone could easily use this information for bad purposes or to change this information, and by that violating the confidentiality and the integrity of these data. The company has to consider the confidentiality (no unauthorized party can look at important information), also, they have to consider the integrity (no unauthorized party can make changes on information). And availability (so no one can take the information or delete it from the company’s system) it would be available for anyone who might need it.

Organization assets that do not fit into other categories are included in the business assets category. Human resources, business processes, and physical plant are all included.

|  |  |
| --- | --- |
| Asset Name (including the CIA) | Justification for why it’s critical |
| Confidentiality and reliability of the network | Because data breaches on the network can cause financial losses, and damage of the company’s reputation. |
| costumer’s data (confidentiality) | Maintaining the confidentiality of the customers data is critical to keep the customers trust, to avoid financial losses, as well as to avoid legal penalties. |
| Database information (confidentiality integrity and availability) | To avoid business loss, because the database contains all critical information, such as financial records, customers data. as well as to avoid legal penalties. |
| Transmitted Data (confidentiality and integrity) | To protect sensitive information during the transmission from unauthorized access, and to avoid losing customers. As well as legal penalties. |
| Availability of software applications in employee’s devices | In order for the employees to perform their jobs affectively. To ensure customers satisfaction. |
| servers’ availability and reliability | To avoid servers’ downtime to ensure the customer’s satisfaction. To avoid damaging the company’s reputation. As well as to avoid financial losses |
| Availability and reliability of company’s website | To ensure high levels of customers satisfaction, therefore, it would be a competitive advantage and good reputation for the company. |

1. First of all, it was mentioned before that not all existing office devices (endpoints) are secure. Hackers can create network entrances by using endpoints. And lot of these devices are connected to other important devices for the company that might contain important information’s, such as the company’s servers. After reading some studies about this, around 74.5% of organizations had an attack from an end point. Endpoint attacks impact can include server damages, data loss, or harmful programs downloaded by the attacker that might cause hard disk failure.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset Name (including the CIA)** | **Possible Risks** | **Impact** | **Likelihood** | **Justification for likelihood and impact** |
| Main software failure(availability) and data corruption or stollen (availability and Confidentiality) | - server damages  - data loss  - hard disk failure | (Minor) | (Likely) | Likelihood: because hackers usually target weak end points.  Impact: it depends on the breach type, but it might affect the server. |

Secondly, it is mentioned that all devices at all monitoring stations are connected to a single subnet, and this is risky because if an unknown user connects to the same LAN, the network could be hacked. So, I think that they should use subnetting to separate the important network from other networks as subnets prevent devices from accessing the entire network, and corporations can choose which hardware and users have access to sensitive data.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset Name (including the CIA)** | **Possible Risks** | **Impact** | **Likelihood** | **Justification for likelihood and impact** |
| Network connectivity (data breaches)  Confidentiality and reliability of the network | -hacker attack | (Major) | (Unlikely) | Likelihood: because the data is encrypted.  Impact: might include the servers if hacker could reach the whole network |

Thirdly, it is mentioned that the data from each branch using an internet connection will be uploaded to the system (in the cloud). When switching to cloud computing, there are various security risks to consider. Malware is a common threat to cloud security. As cloud usage grows, organizations are more likely to experience data breaches, as cybercriminals are developing their ways of hacking, the company is opening themselves to the possibility of leakage of sensitive data. There is a lot of critical information for important people, which will result in loss or leakage for everyone’s information in there.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset Name (including the CIA)** | **Possible Risks** | **Impact** | **Likelihood** | **Justification for likelihood and impact** |
| Transmitted costumer’s data (confidentiality) | leakage of sensitive data | (Major) | (Unlikely) | Likelihood: because they are transmitting the data over a highly secured web application.  Impact: if it happened all people that have their data in there are going to be affected as it might get stolen, which might result in affecting their business as well. |

Furthermore, it is mentioned that the back door of the data center is easily opened, therefore, it is likely that someone either from outside or inside the company will try to access the network devices to steal information or plant some kind of malware into the devices to harm the system. So, either someone will look through the data(confidentiality), change them(integrity), or disable the devices(availability). Also, the room’s temperature and humidity should be controlled in order to preserve the availability of the devices. It can make a long-term effect in terms of both energy efficiency and cost savings.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset Name (including the CIA)** | **Possible Risks** | **Impact** | **Likelihood** | **Justification for likelihood and impact** |
| Database information (confidentiality integrity and availability)  Web servers’ availability and reliability | -Malware planting  -stealing information or change them  -hardware failure | (Major) | (Likely) | Likelihood: if no action was taken it can easily happen  Impact: because it includes affecting data as well as the affecting servers and other hardware devices. |

Another aspect to consider is the VPN (virtual private network), as mentioned that some staff got VPN access to the data center and can remotely run some apps. Of course, employees having VPN access is important because it helps them to have a safe remote access to the company’s server. Moreover, the massages and information’s sent through the internet are encrypted so no one can access them. But the VPN still have some risks, such as, if the VPN disconnects, the data may be exposed, and the secure channel is no longer available. But this can be managed by having something called a kill switch, it ensures that if a device loses its VPN connection, the internet connection will be stopped. As a result, the internet address is not exposed.

Moreover, it mentioned that some third parties also have VPN access. Allowing a third-party access to an organization’s networks carries a significant security risk. Even if they have no malicious intent, they play a dangerous role in data breaches, which can cost the company millions of dollars. It said that a third party is involved in about half of all the data breaches, because it is the weakest link of network, and if a hacker had access through a third party to the network it allows him to reach a lot of data. A third party could be easily tricked by a hacker somehow and he could give him access to his network, such as by phishing attacks. Therefore, third parties should be granted access to parts of the company that they might need.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset Name (including the CIA)** | **Possible Risks** | **Impact** | **Likelihood** | **Justification for likelihood and impact** |
| Transmitted Data (confidentiality and integrity) | -hacker stealing information or change them | (Moderate) | (Possible) | Likelihood: It can happen considering the misconfiguration.  Impact: hacker can have important information and it might keep going without anyone knowing. |

Next, is the misconfiguration on the security devices such as, the VPN and firewalls. Misconfiguration happens when the security settings are not implemented or contains errors. These kinds of errors are dangerous because they create gaps that makes the data and the company itself exposed to a breach or cyber-attack. It is said that 73 percent of companies have at least one misconfiguration in their system. One of the impacts of misconfiguration is the exposure of private information’s.

Unpatched software is one of the main reasons for having a malware. If the software isn’t always updated hackers can use the previous versions to harm the systems. A survey made by (Ponemon Institute) show that 60% of breaches in two years were caused by unpatched software.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset Name (including the CIA)** | **Possible Risks** | **Impact** | **Likelihood** | **Justification for likelihood and impact** |
| Availability of software applications in employee’s devices | -hacker attack | (Minor) | (possible) | Likelihood: hackers can easily attack unpatched software.  Impact: may include sensitive data exposure |

Every company should manage their password policy. And the organization’s employees, customers and third parties should be involved in this policy. Using week password policy will make the company suffer severely. Examples of the risks are, Phishing due to lack of awareness, brute force due to week passwords.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Asset Name (including the CIA)** | **Possible Risks** | **Impact** | **Likelihood** | **Justification for likelihood and impact** |
| - System software availability and reliability  -user’s data confidentiality and integrity | -hacker accessing a device and network | (Almost certain) | (Major) | Likelihood: easy access to devices with week passwords  Impact:  -can result in a system authentication failure and compromise system security.  -Can affect huge parts of the network including data, hardware, software.  -loss of productivity due to system downtime. |

Auditing gives the opportunity to gain valuable insights on how their business is performing. The word audit means to evaluate something. And one of the main reasons to use security audit is to protect the privacy of the customers. Having issues in auditing can put your company in possible danger. Auditing the network access control, encryption mechanisms, and how sensitive activities are being performed ensures that the company is safe, and everything is performed as it is supposed to be. And most importantly is that auditing identifies gaps in your system in order to fix them to insure the protection of your company.

Auditing issues:

|  |  |
| --- | --- |
| Risk likelihood | (Likely) because there might be a lot of vulnerabilities in the company. |
| Risk (impact) | (Catastrophic) major security breaches can happen, might lead to losing customer or even the business. |

1. In the begging it said that they are using one subnet for all devices, but it doesn’t mean that anyone in the network can access any information at any time. They are probably using firewalls in order to give the access for the data for only the people who are permitted to access these data.

Secondly, as they are uploading the data to the system using an internet connection, they are probably using encryption for the data due to the high importance of the data and the customers privacy, and to protect themselves from any law breaking.

Moreover, the private information that the customer place in their profile is probably also encrypted in order to protect their privacy while it is being transported to the cloud.

Also, with VPN access the firewalls might be used to prevent third parties from accessing data they shouldn’t access.

|  |  |
| --- | --- |
| Asset Name (including the CIA) | Controls initially used by the company |
| * Confidentiality of customers data and business sensitive information. * Integrity of business different critical data. * Availability of servers in datacenter. * Reliability and availability of the network. | firewalls |
| * Confidentiality of sensitive information stored in laptops. * Confidentiality of sensitive information stored in servers. * Availability of stored data in the datacenter. | encryption |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Asset | Threat/s | vulnerability | Controls | Impact | Likelihood | Level of Risk | Risk Priority |
| Confidentiality of user’s data/ and the reliability endpoint devices | Malware, unavailability of endpoint device. | Not all endpoints are secure | Firewalls  encryption | Minor | Likely | Medium | 5 |
| Network reliability  software and data (confidentiality, integrity, availability) | Hacking network | Using the same subnet for all devices | Firewalls | Major  (Can affect multiple parts from the network). | Unlikely | High | 7 |
| confidentiality and integrity of the transmitted data | Malware, man-in-the-middle attack | No clear vulnerabilities | encryption | (Major) | (Unlikely) | High | 8 |
| Availability of servers and software in data center | Theft, disabling systems, planting malware | Data center is not well secured | Firewalls | Major to catastrophic | Likely | Extreme | 2 |
| Availability of all hardware devices in the data center | System failure-overheating in data center | Temperature is poorly control | Old or week air conditioner | Moderate | Likely | High | 3 |
| Confidentiality, integrity of data transmitted using VPN | Malware, man-in-the-middle attack | Misconfiguration in VPN | encryption | Moderate | Possible | High | 4 |
| Availability and reliability of company’s website | Denial-of-service-attack (DDOS) | Misconfiguration in firewalls | Firewalls | Insignificant | possible | Low | 9 |
| Availability of software in the employee’s devices | malware | Unpatched software | Firewalls | Minor | possible | Medium | 6 |
| System software availability and reliability, and user’s data confidentiality and integrity | system authentication failure | Password policy issues | Firewalls | compromise system security (Major) | Almost certain | Extreme | 1 |

1. ways to improve Warmaksan’s IT security via:
2. security controls that could be applied to protect the most critical assets:

In order to protect the customer and the business-critical assets we need to protect both the network and the data center because if both of these were hundred percent secure there will be nothing to be afraid of.

1. **First of all is the network security**.

This can be done by correctly applying three main parts (Network topology, Security devices, and Security services).

* + - Network topology: which is basically the arrangement of the hardware devices such as a firewall, in order to protect the network’s security.

The firewall’s main job is to protect the network from untrusted traffic based on a set of rules. One of the best topologies is the demilitarized zone (DMZ) which basically a zone between the public and the private network. It’s made to protect and serve the clients while protecting the company and the same time.

* + - Security devices: devices that are made in order to protect the company’s assets and the client’s data at the same time.

There are few types of security devices that can be used:

1. Firewalls: a system made to protect the networks by controlling the access between them. One of the best firewalls applications is the Next-generation firewalls. This type of firewall provides better capabilities beyond the other firewalls. It provides intrusion prevention, controlling and scanning to block untrusted application, methods for dealing with growing security threats.
2. Intrusion detection and prevention devices: both of these technologies can complement each other. Intrusion detection’s main job is to detect any malicious traffic, but Intrusion prevention’s main job is to stop the malicious traffic completely.
   * + Security services: services that provides security for data and information transfer system of an organization.
3. Ipv4: used as an address for each device, it helps to enhance the security by knowing the source of the packet to know wither it is trusted, or it might be a threat for the network. And this can be done with the helping of NAT which translates private address to a public address.
4. VPN: a private network that acts as a tunnel in the internet, and it is better when encryption is used to protect the confidentiality of the data.
5. **Data Center Security: (Physical Security)**

It’s very important to protect data center in order to achieve the availability, integrity, and confidentiality of the customer and business data. this can be achieved through multiple layers or steps:

1. Employees: such as the guard and employees and possible third parties can help in protecting the data center by preventing unauthorized people from accessing any part of the data center.
2. Fences and physical barriers: used as first step of protecting the data center by preventing unauthorized people to enter the data center completely.
3. Doors: have multiple shapes depending on the place it was placed in, but it’s main job is to give access to places in the data center for the allowed people only. Therefore, some might be able to enter a certain room but not another one by having an identity.
4. Badging policies to identify the person that is in the data center.
5. Access control policies that give access to people to the places they are allowed to, and to prevent them from going into another.

|  |  |
| --- | --- |
| Critical Asset Name (including the CIA) | Controls to improve security |
| Sensitive data (confidentiality and integrity) | * Encryption * Access controls, such as passwords. * Data backup * Regular security auditing |
| Data links (availability, reliability) | * Firewalls * Intrusion detection and prevention systems |
| Main Servers (reliability, availability, integrity) | * Regular updates and patches for software * Anti-virus and anti-malware software * Access controls (passwords) |
| Employees devices (availability, integrity, and reliability) | * Anti-virus and anti-malware software * Access controls (passwords) * Regular updates and patches for software * Encryption |
| Company’s website | * Regular audits and updates * Web application firewall |

|  |  |
| --- | --- |
| Recommended controls to protect customers | * Using encryption to protect the customers sensitive data from unauthorized access and theft. * Using strong access control methods. For example, using multi-factor authentication in order to prevent unauthorized people from accessing customers data. * Applying security audits in a regular basis in order to look for any vulnerabilities in the system, to protect the customers data. * Applying data backup by regularly backing up the customers data. as well as having disaster recovery plan to protect the data from loss. |
| Recommended controls to protect business-critical data | * Securing the business data through implementing firewalls, as well as intrusion detection and prevention systems. * Applying Anti-virus and anti-malware software to all devices in the company, such as servers, laptops. * Implementing physical security methods, such as using guard, access control for datacenter, and cameras. * Training employees on the importance of applying all security rules, as well as training them on how to prevent security breaches. |

1. Data protection:

Data protection is critical because it protects an organization’s information against actions such as hacking, phishing, and identity theft. Organizations must protect their data effectively and upgrade their security procedures on a regular basis in order to protect the confidentiality, integrity, and the availability of the data.

How to protect the data?

There are multiple practices that could be applied in order to protect the data:

**1. Encryption**: It is a method in which a normal readable text gets converted into meaningless text usually in order to preserve the integrity of the data.

**2. Data backup**: a procedure that include copying data from one point to another in order secure it in case of a disaster, accident, or criminal action. There are multiple types of data backup that can be applied, such as full backup, differential backup, and incremental backup. And all data backups should be protected from any potential threat.

**3. Fire walls**: Tools (software or hardware) that are used to filter the network’s traffic in order to prevent any malicious traffic from accessing the network.

**4. Data loss prevention**: A group of methods and practices that are used to protect data from theft, loss, deletion, misuse, or other unwanted or illegal kinds of engagement.

Moreover, other strategies can be performed in order to protect the data, such as auditing of sensitive data, assessing the internal and external risks that might affect the data, as well as applying a data protection policy.

**Data protection regulations:**

Data protection regulations are considered as group of laws and guidelines that controls the storage, collection, transfers, and use of personal information. The main idea of these regulations is to protect the privacy of individuals as well as to make sure that these information are handled correctly and in a secure manner. One of the data protection regulations examples includes the European Union's General Data Protection Regulation (GDPR). For example:

* Data storage: define the rules ‘security measure’ on how to store the data to protect personal information.
* Data collection: choosing what data can be collected and how ell they be used.

1. IT security audit:

IT security audit analysis:

|  |  |  |
| --- | --- | --- |
|  | **Issue** | **What can be done** |
| **Physical component** | Not all devices are well secured | -antivirus software  -password policy |
| Door easily opened | -using doors that needs authorized access to open. |
| Humidity and temperature are poorly controlled in the data center | -buy a new air conditioner. |
| **Application and software** | Unpatched services and applications | -Making regular updates and fixes |
| **Network Vulnerabilities** | -Using one subnet | -subnetting the network |
| -Misconfiguration on firewalls and VPN | -know the misconfiguration reason and fix it |
| **Human dimension** | Password policy issues | -Applying new policies and making sure all people are following them |
| Auditing Issues | -making regular scanning on all system components |

**Security audit impact:**

1. Helps in determining the current security status in all possible fields, which means gaining better understanding of how secure the organization is.
2. Help to discover week areas in order to know wither the polices and standards should be changed and updated or not.
3. Helps in protecting the system from attacks by identifying flaws in the system that any hacker might use to gain access to the systems and networks.
4. Make sure that the organization is following polices, and laws to protect themselves.
5. Helps in saving money by showing potential attacks that might happen and preventing them.
6. **Risk assessment procedures:**

|  |  |
| --- | --- |
| Risk assessment approach used | Combined approach:   * Baseline approach * Detailed risk analysis |
| Risk assessment steps taken | 1. Identify the assets in the organization 2. Identifying potential threats, as well as their types and sources. 3. Identifying the vulnerability (flaws and weaknesses) in the system. 4. Knowing the existing controls that are used within the system. 5. Specifying both the impact using (assets and threats). As well as the likelihood based on the (threats, vulnerabilities, and controls). 6. Specifying the level of risk. |
| **Acceptable Risk Level** | **Low** |
| **Risk Assessment Type** | Qualitative |

1. **Risk management approach:**

ISO 31000 risk management is an international standard that was developed in order to offer organizations with risk management principles and guidelines. ISO 31000 was designed to suit any size of organization.

1. **The Risk management process:**
2. Identify the possible risks that might affect the organization’s progress.
3. Analyzing the risks by understanding the reasons and causes of the threats detected in the organization (likelihood, consequences, level of risk).
4. Evaluating the risks by comparing risk analysis results to risk criteria, you can determine if the risk level is appropriate.
5. Risk treatment: taking advantage of all the existed information and changing them to achieve net grow benefits.
6. Establish the context: understanding the department objectives and defining the external as well as the internal environment of the department.
7. Monitoring and review: monitoring and identifying change from the performance level, then review the effectiveness of the risk management process including the risks, controls, and treatments to achieve goals.
8. Communication and consultation: Help stakeholders in understanding the risks, how decisions are made, and the reasons why certain action are required. Therefore, communications involve promoting awareness and understanding of the risk, whereas consultation involves taking feedbacks and information’s that helps in the decision-making process.
9. **Principles of ISO 31000:**
10. Inclusive: in order to make sure that the risk management is successful, all the stakeholders should be involved.
11. Dynamic: the organization always changes as well as it is risks. Therefore, risk analysis should be performed daily in order for the company to keep functioning.
12. Based on best available information
13. Always consider human and cultural factors (risk related to human error or to organization’s culture).
14. Continues improvement through learning and experience to ensure better risk mitigation overtime.
15. **ISO 31000 framework and guidelines:**
16. Leadership: leaders within the company should make sure that the ISO 31000 is applied to go with the company’s culture and business objectives.
17. Integration: it is essential to reduce risk within as many organizational processes as possible, it is also crucial to avoid negatively impacting the performance of essential business processes.
18. Design: designing the risk management strategy to suit the organization needs.
19. **Benefits of the ISO 31000**:
20. Gives competitive advantage: when a certain company follows a well-known standard, people well have trust in this company, which well make them prefer it on other companies.
21. Protect the company’s profitability by mitigating risks and reducing financial damage.
22. Helps the company to acquire funding easier because of the trust that the banks and investors well have in it.
23. **Misalignment of IT security policy**

Misalignment can happen when there are conflicts between the managers in the company. Or the policies aren’t followed as they are supposed to be. Or else, it is a flaw between the organizational policy rules and the IT security polices and the compatibility between them which would affect the business and its systems negatively.

1. Impact of policy Misalignment:
2. Having misalignment in the company’s policy leads to having errors in the system, which means that the system will have vulnerabilities that could be used by someone to harm the company.
3. Misalignment make employees loss within the company because of the lack of knowledge and misunderstanding what they are supposed to do.
4. Misalignment might destroy the company’s reputation and lead the company to fail.
5. How to avoid misalignment:
6. Understand all the business objectives
7. Regular training for employees and management, and to always have a opened communication between employees and their managers as well as their colleges.
8. The administrators should keep track of their employees and everyone who’s included in the policies to know wither they are following the rules or not.
9. Always make sure that all policies are well understood in order to implement them in the best possible way.
10. Security policy for Warmaksan, including the main components of an organizational disaster recovery plan.

|  |  |
| --- | --- |
| **Included Policies** | **List of sub-policies** |
| 1. Server Policy | * Services and applications must be disabled when not being used. * Access control methods should be used to access services, such as Firewalls, and authentication methods. * The operating system on the server must be regularly updated. * The server must be physically placed in a well secured environment, and the temperature must be controlled. |
| 1. Backup policy | * The frequency of backup depends on the importance of the information. * Any unwanted data copies should be broken and burn. * The backed-up data should be protected from unauthorized access or environment conditions. * The backed-up data must be tested regularly to insure they can be recoverable. |
| 1. Information Security policy,   Ex. (**Email Policy**). | * All Warmaksan data contained in the email must be secured. * Warmaksan email account should only be use for business purposes. * Important emails should be preserved if needed. * Emails received shouldn’t be opened unless it is from a trusted source. |
| 1. Information Security policy,   Ex. (**Clear Screen/Desk Policy**). | * All computers shall be closed and password-protected when unattended * The computer shall be automatically locked when not used for four minutes. * When print sensitive information, the printer should be cleared immediately. * Password should not be in an accessible location in the desk. |
| 1. Network Policy | * All data that are being send through the network should be encrypted * All devices should have software firewalls. * All devices should have antivirus software. * Hardware firewall must be implemented to protect the network. * Patches and updates must be applied regularly on all devices to ensure network security. |

1. Justifying and reasoning for the selected elements.

|  |  |
| --- | --- |
| **Policy Introduction** | |
| **Included Policies** | **Justification for the Included Policies** |
| 1. Server Policy | * Implementation of this policy insures secure access to data. * It highlights the rights of server users. |
| 1. Backup policy | * Insures the availability of data in case of a hardware/software failure or physical disaster. * Provide protection for data in case of human error or the accidental deleting of crucial data. |
| 1. Information Security policy,   Ex. (**Email Policy**). | * Insure the proper use of Warmaksan email system for users. * Making users aware of the possible attacks from untrusted emails. |
| 1. Information Security policy,   Ex. (**Clear Screen/Desk Policy**). | * Reduce risk of unauthorized access. * Reduce risk of stolen, losing or damaging information during and outside work hours. |
| 1. Network Policy | * Ensuring the security of the network. * Helps the network to operate in the best way. |

1. Evaluating the tools in this policy.

|  |  |
| --- | --- |
| **Tools used within the policy** | **The Evaluation of the Tool** |
| 1. Software and hardware firewalls | They are used to prevent unauthorized access to network and devices, by blocking malicious or unwanted traffic from accessing the network. |
| 1. Antivirus software | Used to detect and prevent malicious traffic from accessing the network. |
| 1. Access control method | Used to allow only trusted people to access a certain information or network. And prevent unauthorized users.  Also, prevent unauthorized people from accessing physical places in the business. |
| 1. Data backup software | Used to store critical information, so in case of an emergency the data well be preserved from any potential loss. And using the software well help in accessing the data faster. It also provides antivirus protection to protect data from any potential attack. |

1. **Stakeholder’s roles to implement security audit recommendations.**
2. Management:
3. Making sure that all recommendations of security audit are applied effectively and on time
4. Making sure that all necessary resources where organized to come up with recommendations. And the implementations have no bad effect on the company’s operations.
5. IT officers:
6. They are responsible of knowing the measures of technical security that were recommended by the security audit and implement them.
7. Making sure that all measures are correctly implemented, and they have no negative affect on the system’s performance.
8. Risk owners:
9. Making sure that risks that are related to the security vulnerabilities that are shown by security audit are reduced.
10. Working hand by hand with management and IT to apply the measures that were suggested and ensure that the risks are manageable.
11. Facility and security officers:
12. Making sure that the datacenter and all buildings are physically secured.
13. Making sure that the security measure that were recommended are applied and ensure the security of the data center.
14. Compliance officers:
15. Make sure that the company is following the suggestion of the security audit.
16. Working with other stakeholders in order to make sure that all measures recommended are applied and the organization is complying.

|  |  |  |
| --- | --- | --- |
| **Student name:** Yousef Abu Ali  **Student ID: 21110294**  **Is the student repeating this unit? YES NO** | | **Assessor name:**  Eng. Sami Al-Mashaqbeh  Dr. Heba Alawneh  Dr. Safaa Hriez  Eng. Asma Lafi |
| **Issue date:**  06/11/2022 | **Submission date:**  31/01/2023 | **Submitted on:**  **30/01/2023** |
| **Programme:** Computing | | |
| **HTU Course Name:** Security  **BTEC Course name:** Security  **HTU Course Code:** 10203280 **BTEC Course Code:** Unit 5 (D/618/7406) | | |
| **Assignment number and title:**  Assignment 9: Warmaksan | | |

**Plagiarism**

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalised. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

|  |
| --- |
| **Student declaration**  I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.  **Student signature: Date: 30/01/2023** |

**References**...................................................................................................................

www.linkedin.com. (n.d.). *Identifying Critical Assets*. By Endro SUNARSO [online] Available at:

<https://www.linkedin.com/pulse/identifying-critical-assets-endro-sunarso->

www.fieldengineer.com. (n.d.). *What is Subnetting, Benefits, and How does it Work?* [online] Available at: <https://www.fieldengineer.com/skills/subnetting>.

SecurityScorecard. (n.d.). *Top 5 Security Risks of Cloud Computing*. [online] Available at: <https://securityscorecard.com/blog/top-security-risks-of-cloud-computing#:~:text=What%20are%20the%20security%20risks%20of%20cloud%20computing%3F,data%20...%205%205.%20Inadequate%20due%20diligence%20>

www.vertiv.com. (n.d.). *Why is monitoring server room temperature important?* [online] Available at: <https://www.vertiv.com/en-us/about/news-and-insights/articles/educational-articles/why-is-monitoring-server-room-temperature-important/>

Top VPN Deals For All Devices. (2021). *What are Advantages and Disadvantages of VPN?- Benefits & Risk*. [online] Available at: <https://www.vpnblade.com/vpn-advantages-and-disadvantages/>

eSecurityPlanet. (2020). *VPN Security: How VPNs Work in 2021 | eSecurity Planet*. [online] Available at:<https://www.esecurityplanet.com/networks/vpn-security/>

www.kaspersky.com. (2022). *What is endpoint security and how does it work?* [online] Available at: <https://www.kaspersky.com/resource-center/definitions/what-is-endpoint-security>

<https://reciprocity.com/blog/security-misconfigurations-how-to-avoid-them/>

SearchSecurity. (n.d.). *6 reasons unpatched software persists in the enterprise*. [online] Available at:<https://www.techtarget.com/searchsecurity/feature/6-reasons-unpatched-software-persists-in-the-enterprise>

*The 5 biggest dangers of unpatched and unused software*. Available at: <https://www.1e.com/blogs/5-biggest-dangers-of-unpatched-and-unused-software/#:~:text=Unpatched%20software%20is%20an%20open,versions%20to%20infiltrate%20your%20system.&text=According%20to%20the%20SANS%20Institute,offenders%20for%20not%20being%20patched>.

Cypress Data Defense (2020). *6 Password Security Risks and How to Avoid Them*. www.cypressdatadefense.com. Available at:<https://www.cypressdatadefense.com/blog/password-security-risks/>

SailPoint. (n.d.). *Benefits of a Cybersecurity Audit*. Available at: <https://www.sailpoint.com/identity-library/benefits-of-a-cybersecurity-audit/>

HowStuffWorks. (2011). *5 Ways to Keep Your Information Secure in the Cloud*. [online] Available at: <https://computer.howstuffworks.com/cloud-computing/5-ways-to-keep-your-information-secure-in-the-cloud.htm#:~:text=5%20Ways%20to%20Keep%20Your%20Information%20Secure%20in,...%205%205%3A%20Play%20Smart%20with%20Passwords%20>

www.ijser.org. (n.d.). *Cloud Computing Security threats and Countermeasures*. [online] Available at: https://www.ijser.org/paper/Cloud-Computing-Security-threats-and-Countermeasures.html

https://www.conceptdraw.com. (n.d.). *Network Security Devices*. [online] Available at: https://www.conceptdraw.com/How-To-Guide/network-security-devices

PECB (2021). *Why is Data Protection Important?* [online] pecb.com. Available at: <https://pecb.com/article/why-is-data-protection-important>

OmniCyber Security. (2022). *The Importance of Data Protection*. Available at: <https://www.omnicybersecurity.com/importance-data-protection/>

Learning Center. (n.d.). *What is Data Protection | Principles, Strategies & Policies | Imperva*. [online] Available at: <https://www.imperva.com/learn/data-security/data-protection/>

ZEVENET. (2021). *10 Importance of Information Security Audit*. [online] Available at: <https://www.zevenet.com/blog/10-importance-of-information-security-audit/>

Trainer, P.R. (2021). *ISO31000 risk management process*. [online] Practical Risk Training. Available at: <https://practicalrisktraining.com/iso-31000-risk-process?utm_source=rss&utm_medium=rss&utm_campaign=iso-31000-risk-process>

Server Security Policy. (n.d.). [online] Available at: <https://www.cpcstech.com/pdf/server_security_policy.pdf>

EDUCBA. (2019). *Security Policies | Learn List of 6 Most Useful Security Policies*. [online] Available at: <https://www.educba.com/security-policies/>

Biswas, P. (2020). *Example of Backup Policy*. [online] PRETESH BISWAS. Available at: <https://preteshbiswas.com/2020/01/30/backup-policy/>

Ochieng, J. (2019). *Network Security Policy - A Complete Guide - Cyber Experts %*. [online] Cyber Experts. Available at: <https://cyberexperts.com/network-security-policy/>

[General Data Protection Regulation - Wikipedia](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation#:~:text=The%20General%20Data%20Protection%20Regulation%20%28EU%29%20%28%20GDPR%29,Charter%20of%20Fundamental%20Rights%20of%20the%20European%20Union.): <https://en.wikipedia.org/wiki/General_Data_Protection_Regulation#:~:text=The%20General%20Data%20Protection%20Regulation%20%28EU%29%20%28%20GDPR%29,Charter%20of%20Fundamental%20Rights%20of%20the%20European%20Union>.