** Security**

**By: Abdallah Salhab 21110181**

**A. Discuss the most critical assets of the Warmaksan's system, considering their CIA principles in mind.**

-not securing all the end devices can be a threat to the confidentiality and the integrity of the organizations data.

-having one subnet for all the devices and the departments can affect the confidentiality of the data and it may affect the accessibility of the data because it is a big broadcast.

-if the door of the data center was easily opened this can affect the confidentiality and may be the integrity and accessibility of the data.

-having a humid and uncontrolled temperature in the server’s room can lead to data accessibility issues if the servers broke down.

-if third parties have access to the data center via VPN, the confidentiality of the data can be a concern.

-unpatched services and devices can be an accessibility, confidentiality and an integrity problem for these services and data because hackers can benefit from the vulnerability before the patch.

-if the password policy is weak the confidentiality and integrity can be a concern because it’s maybe easy to access one of the organizations devices.

-the data of the should not be transmitted through a published web application because this can affect the confidentiality and integrity of the data.

-storing data on the cloud.

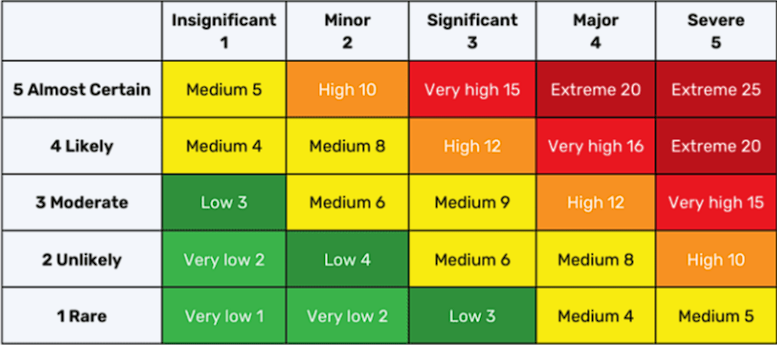
**B. Discuss and assess Warmaksan system's possible risks, their likelihood (rare, unlikely, possible, likely, and almost certain), and exploitation consequences (insignificant, minor, moderate, major, catastrophic, and doomsday).**

**The impact:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Insignificant** | **Minor** | **Significant** | **Major** | **Severe** |
| **1** | **2** | **3** | **4** | **5** |

**The likelihood:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Rare** | **Unlikely** | **Moderate** | **Likely** | **Almost Certain** |
| **1** | **2** | **3** | **4** | **5** |



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ASSETS | THREAT  /VULNERABILITY | IMPACT | LIKELYHOOD | LEVEL OF RISK |
| the data of the customers and organization due to  not securing all the end devices | If the hacker reached the data, he could eater see it, change it or delete it affecting the  CIA | **Major**  (4) | It could be relatively easy to get to an end device especially if the attacker works in the company  (4) **Likely** | (16) **very high** |
| The data of the customers and the organization due to  having one subnet for all the devices | When having one subnet if an attacker get access to a device in the network, he can access all the severs and all the data of the network and he could see it, change it or delete it affecting the  CIA | (5) **Severe** | (4) **Likely** | (20) **extreme** |
| The data center due  to  the door of the data center can be easily opened | If an attacker access get access to the data center, all the data and the devices in it is in danger as he could, see and change and delete the data and he could also destroy the devices them selves affecting  CIA | (5) **Severe** | If the door can be easily opened and they didn’t mention any guards it can happen a lot.  (5) **Almost Certain** | (25) **extreme** |
| The devices in the data center due  to  the humidity and temperature are not controlled in the data center | High humidity and temperature can ruin the devices in the data center but it can only affect the accessibility of the data if the devices get damaged  A | (3) **Significant** | It may happen in the summer and wouldn’t destroy all the devices.  (2) **Unlikely** | (6) **medium** |
| The services and applications due to  unpatched services and applications | Hackers can benefit from a vulnerability that is on the old patch and use it to block those services and applications affecting accessibility.  A | (3) **Significant** | It can only happen if someone is targeting this company and have found this vulnerability.  (2) **Unlikely** | (8) **medium** |
| The data in the data canter due  to  third party can have access to the data canter via VPN | If the third party is not a trustworthy source, he could end up accessing the data and see it, change it, or delete it affecting the  CIA | (5) **Severe** | It is going to happen if the third-party company  (3) **Moderate** | (15) **very high** |
| The organizations devices due  to  the password policy is weak | If the password is too simple the attacker might figure it out but if it is not that obvious, he would use bure-forcing the password, and having weak password make the brute-forcing much faster, and time can help detecting the attacker preventing the attack but if not it can affect the CIA | (4) **Major** | (4) **Likely** | (16) **very high** |
| The data of the application customers due  to  Using a published web application to transmit data | The data can be easily seen and changed by hackers, so it is a worry for confidentiality, integrity and accessibility. | (4) **Major** | It is going to be easy for any hacker to access the important data.  (4) **Likely** | (16) **very high** |
| The organizations data due  to  Storing their data on the cloud | The attacker could attack the data without the organizations knowing so they won’t take any procedure, he can change it or delete it and if there is no internet you can’t access the data, so it can harm the CIA of the data. | (5) **Severe** | The data of the cloud can be poorly encrypted or maybe password policy is weak, which makes the data more accessible to the hackers.  (3) **Moderate** | (15) **very high** |
| The organizations data due  to  Firewall and VPN misconfiguration | Misconfiguration can give the attacker direct access to the data or block authorized people form it  CIA | (5) **Severe** | (4) **Likely** | (20) **extreme** |
| The entire system due  to  The system has auditing issues | Without the auditor the policy might not be implemented correctly especially the security policy, so any thing wrong can be a vulnerability the attacker can benefit from. | (5) **Severe** | (5) **Almost Certain** | (25) **extreme** |

**C. Suggest (given the notes above) the possible controls/countermeasures initially used by the company to protect their asset.**

-they secured some of the end points.

-they used monitoring station on the subnet.

-some employees use VPN to access the data center.

-they have a door on the data center that can be easily opened.

-they have a firewall and VPN but are misconfigured.

-they have password policy but it has some issues.

-the company has an auditor but has issues.

**D. Recommend ways to improve Warmaksan's IT security via:**

**a. Describe and assessing different security controls that could be applied to protect the most critical assets (customers & business-critical data)**

-the company should secure all the end point devices and screen saver and strong password.

-they should divide their network into subnets.

-they have to install TAPs that is connected to a monitoring device that analyze the traffic and detects any intrusions and try to prevent them.

-the data center has to be secured with a door that works with two factor authentications, there has to be guards on the door and there has to be cameras.

-they have to correct the misconfiguration for the firewall and the VPN.

-they have to store their data on premise, or to use the cloud to store unimportant data.

-they have to quit using published web application (HTTP) and use HTTPS instead.

-the data center has to be controlled in the humidity and temperature level.

-they have to patch all the services and applications and install the latest version software on the devices.

-they have to use a strong password policy.

-making sure that the third-party VPN provider is trust worthy and secure.

-the system has to have a good auditor that checks that everything is working up to the standards and everyone is following them.

GDPR regulations:

GDPR is a list of rights for the people who have data that is processed in an organization, to have more control over their private data, like:

-allowing people to delete the processing of their personal data.

-the right to be forgotten.

- the right to take their data and change to another service provider.

**b. Explain data protection processes and regulations that might enhance Warmaksan's IT security.**

Data protecting process that is for the data at rest and in transit consists of making a backup for the data and encrypting the data.

\*Data backup:

It means making a copy of the data to use in the case of the damage of the original data.

There are three types of data backup:

Full back up: the data is completely copied and stored every specific time.

-Differential backup: this backup only copies the data that have changed from the last (full backup).

-Incremental backup: this type copies the data that have changed since the last backup.

\*Data encryption:

It is a way to translate data that is written in plain text to an encrypted text to ensure the integrity and confidentiality of the data and to insure the origin of the data.

How to encrypt data in massages to insure integrity and confidentiality and origin of the data:

The hash function is a mathematical function that is use for encryption, but to insure the integrity and origin authentication to the hashing HMAC is used, HMAC is calculated by using hashing with a secret key the sender creates a secrete key and gives it to the receiver and encrypts the data with the secrete key and send it, when the receiver gets the encrypted data he use the same hash function to decrypt it and use the senders key to re-encrypts it and if it is the same hash function of the original massage the user know that the data was not changed and he knows it’s origin.

And to insure the confidentiality of the data symmetric encryption or asymmetric encryption can be used.

**[E] c. Analyze the IT security audit and its impact on Warmaksan IT security.**

The IT auditor is very important for the security of the company because the auditor compares and evaluates the security of the organization and checks if the system runs on the standard, the protocols and regulations that is determined by the company and the government.

The auditor makes sure that the data is secured up to the standards, he also directs the attention to any vulnerability that might be harmful, he also makes sure that the company follows all the regulations and laws also, the auditor tries to implement the management recommendation of any improvement.

The auditor can help the company from falling into a lot of security problems that might have happened because of human or artificial errors saving time and money.

**E. Review the risk assessment procedures in Warmaksan.**

Firstly, the risks has to found so we had to check all the security assets and if there are any vulnerabilities on the asset and after checking all the system and we noticed that there ware some unsecured endpoints, there was only one subnet, they use cloud storage, the data center’s door can be easily opened and the temperature and humidity was not controlled, works use VPN that is misconfigured and the third party VPN has access to the data center, some applications and servers were not patched to the latest update, their password policy was weak and their auditing has problems also, there is firewall misconfiguration.

Secondly, the assets and everything that might get harmed has to identified and, in this case, it was: the data center and the important data for the organization and the costumers, the applications and services and in one case it was the whole system with its data.

Next, the risks have to be evaluated and recommendations on how the risks can be avoided is presented: all the end points must be secured, the network has to be divided into smaller subnets, they have to install a monitoring system, the data center has to be secured with a door, guards and cameras and its temperature and humidity has to be controlled, reconfigure the firewall and the VPN, use a trusted VPN provider, store their important data on premise, use a secured wed application (HTTPS), use a good auditor, make the password policy stronger and patch all the services and applications.

Then all of these recommendations have to be implemented.

The risk assessment procedure has to be done at least once a year because there might be some changes that happened in a year and some security processes might decrease.

The auditor has a big impact on the risk assessment procedure because he identifies the risks and he could also give recommendation on how to mitigate them and he would insure that they were implemented correctly.

**[B][C] F. Explain how you can benefit from an appropriate risk management approach or ISO risk management methodology by summarizing it and highlighting its application in the IT security of this project**.

The ISO31000 risk management methodology is a global standard that lists important risk management processes, principles and guide lines to rise the success of the project over all.

-the ISO31000 process steps:  
1-identify the risk: point out the risks.

2-analyse the risk: examine the cause or the causes of the risk.

3-evaluate the risk: comparing the risk analysis with the risk criteria to see if the risk is acceptable or not.

4-treat the risk: to implement measures on the risk to reduce, accept, transfer or to avoid the risk.

5-establishing the contents of the risk: defining the scope of the risk management process and defining the internal and external contents of the organization to help the decision making.

6-monitor the risk: to start the managing process and to asses it’s effectiveness and to review it regularly.

7-talk and consult about the risk: to understand the stakeholders interests and to ensure the effectiveness of the risk management process.

-the ISO31000 system principles:

1-the risk management has to be integrated into all the organizations processes.

2-the risk management has to be structured and comprehensive.

3-the risk management has to customizable to suit the organization.

4- the risk management has to fully embrace everything and to be clearly understandable for everyone.

5-the risk management has to be responsive to change and repetitive able.

6-the risk management takes into consideration the best available information.

7-human and cultural factors have to be considered in the risk management.

8- the risk management has to improve over time.

-the ISO31000 risk management framework and guide lines:

1-leadership: the leaders of the organization have to make sure that the ISO31000 is implemented and is aligned with the organization culture

2-intigration: they have to make sure that the risk management procedure is integrated in all parts of the organization in a way that is does not affect any operations.

3-design: the organization has o design a risk management plan that works with its needs by understanding their internal and external factors.

4-implimentation: the implementation integrates their plan into their processes and there has to be defined objectives, deadlines and requirements.

5-evaluation: evaluation determines what is working in the design and if it is successful or not.

6-improvement: they have to continually improve their ISO 31000 implementation.

-the ISO31000 risk management benefits:

\*increase the stakeholder’s confidence in the organization.

\*it raises the employees awareness about the risks.

\*customers well be drown into the organization because they follow an international standard.

\*increasing the organizations success rate.

\*to be prepared for the worst scenario.

\*to make the different department work together more effectively.

**[D] G. Discuss, in detail, the security impact of any misalignment of IT security with Warmaksan policy and recommend how to maintain their alignment.**

Misalignment happen in an organization when it has both organization policy and security policy that contradict with each other on some of the organization’s process, and the CISO and the CIO are not coming to an agreement that can be equal to both sides or to give priority to more important policy in that case.

If one of the policies was implemented on the process that had a misalignment the process might become insecure or it might become hard to do so, employees might just not do it or to ignore the policy to make the process easier.

Communication and good understanding of each other’s policies are key answers to the misalignment problem as the CISO and the CIO are aware of the requirements of each policy and build up the process according to the recommendations of each policy, to get the process going securely and efficiently.

**I. Justify the developed security plan, giving reasons for the elements selected.**

The security policy is assessing the security of the network, the web application and the server security.

The network security policy is there to protect the network from any vulnerabilities that is introduced to the network during the working of the organization, and to define the standards that has to be met when connecting to the network or working on the network, policies like remote working to insure the security of both end points and wireless communication to ensure the confidentiality of the data being transmitted.

The application security policy is there to assess the security of the application that is used in the company, the policy defines the assessment procedure to identify any potential misconfigurations, errors, data leakage and their mitigations.

The server security policy is there to ensure the security of the data base and server monitoring guide lines and the guide lines for any software that is going to be on the server, and it is going to discuss the process of disposing any hardware and the guide lines for selling them to ensure that there is no data on them.

There are general policies that is for the password and the emails and those are there to ensure the security of the data that is used and collected and discussed during daily work and there is also CCTV policy to ensure that they are used in a way that will help the security.

The DRP is there to help the organization retrieve the data lost in an incident and to make sure the organization process gets back to work in the fastest time possible.

**J. Evaluate the suitability of the tools used in this policy**

VPN: the VPN is a technical preventive tool that is used to connect to the organizations private network, all the packets that runs through the VPN are encrypted so even if a hacker took them it prevents him from seeing what is inside of them.

CCTV: the CCTV is a physical security tool that is mainly used to detect any unusual behavior and to be a deterrent for any threat actor.

Biometric access door: the door is a physical security tool that is mainly used to prevent any unauthorized people to access important organizational assets.

Firewall: the firewall is a technical security tool that is used to prevent any threat actor to access the private’s organizations network

Antivirus: it is a technical security tool that is used as a deterrent to any malware attacks that happens to the network there for it prevents any attacks that could happen.

**K. A discussion of the roles of stakeholders in the Warmaksan to implement security audit recommendations.**

-the management(c-level):

They have to make sure that the auditor gives them effective recommendation in time and to make sure that the recommendation can be done without affecting any operation.

-the IT officer:

Implementing the security audit recommendation correctly and to make sure they are not interfering with the system.

-the risk owners:

They have to work with the management and the IT to ensure they mitigated the vulnerabilities identified when auditing and to implement the recommended measures and to ensure that the risks are acceptable.

-facility and security officers:

They need to make sure that the recommended security measures including the physical are in place on primases and on the data center.

-Quality assurance:

The quality assurance and the stake holders are responsible to make sure that the organization is implementing the auditor’s recommendation and is compliant with his recommendations.

[A] <https://www.sans.org/information-security-policy/>

[B] <https://learn31000.com/iso-31000-principles-of-risk-management/>

[C] <https://learn31000.com/iso-31000-principles-of-risk-management/\>

[D] <https://www.enmehr.com/en/blog/7-tips-to-improve-company-alignment/>

<https://www.accessagility.com/blog/benefits-of-subnetting>

<https://www.kaspersky.com/resource-center/definitions/brute-force-attack#:~:text=The%20best%20defense%20against%20password,the%20breach%20to%20be%20worthwhile%E2%80%A6>

[E] <https://panorays.com/blog/what-is-a-security-risk-assessment/#:~:text=The%20auditor%20will%20compile%20a,better%20mitigate%20those%20risks%20further>.

<https://www.prosafetymanagement.co.uk/reviewing-risk-assessments/>

[F] <https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-team>

[G] <https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/#:~:text=The%20GDPR%20lists%20the%20rights,his%20or%20her%20personal%20data>

**[A] H. Design a suitable security policy for Warmaksan, including the main components of an organizational disaster recovery plan.**

\*\*Network security:

\*remote access policy:

- Encryption and a strong password must be used to strictly control secure remote access (VPN).

- Authorized Users must keep their login and password a secrete even from their family members.

- Authorized Users must guarantee that the remote host is not connected to any other network while remotely connecting to the organization's corporate network using an organization-owned computer.

except for personal networks under their total control or the complete control of an Authorized User or Third Party.

- The use of external resources to conduct the organization's operations must be pre-approved by InfoSec and the relevant business unit management.

- All hosts linked to the organization's internal networks via remote access technologies must run the most recent anti-virus software.

  Third-party connections must respect the requirements outlined in the Third-Party Agreement.

- Personal equipment used to connect to the organization's networks must meet the remote access standards specified in the Hardware and Software Configuration.

\*remote access tools policy:

All remote access tools used to interact between the organization's assets and other systems must meet the policy requirements listed below.

- Warmaksan must provide ways for internal users, external partners, and non-organizational systems to collaborate. The organization can provide you with the list of approved software.

Because correct setup is critical for the safe use of these tools, each of the approved tools includes mandatory configuration requirements.

- Multi-factor authentication is required for all remote access tools or systems that allow communication to the organization's resources from the Internet or external partner systems.

- Active Directory or LDAP must be used as the authentication database source, and the authentication mechanism must use a challenge-response protocol that is not vulnerable to replay attacks, such as OAuth 2.0.

Both endpoints of the session must be mutually authenticated by the remote access tool.

- Instead of direct connections through the perimeter firewall, remote access tools must support the organization's application layer proxy.

- As defined in the organization's network encryption protocols policy, remote access tools must provide robust, end-to-end encryption of remote access communication channels.

- All antivirus, data loss prevention, and other security systems in the organization must not be disabled, interfered with, or avoided in any way.

\*wireless communication policy:

All wireless infrastructure devices that stay on the organization's premises and connected to its network, or enable access to confidential data, must:

- Follow the Wireless Communication Standard's specifications.

- An authorized support team must install, support, and maintain the system.

- Use the authentication protocols and infrastructure that have been approved by the organization.

- Use the encryption protocols approved by the organization.

- Keep a hardware address (MAC address) that can be registered and tracked.

- Other support organizations' wireless access deployments should not be interfered with.

\_\* Requirements for Lab and Isolated Wireless Devices:

The section above must apply to any lab wireless infrastructure devices that enable access to the organization's Confidential or higher. Wireless devices in the lab and in isolation that do not provide general network connectivity to the organization's network must:

- To be disconnected from the corporate network and to follow the Lab Security Policy.

- Other support organizations' wireless access deployments should not be interfered with.

­\_\* Home Wireless Device Requirements:

- Wireless infrastructure devices that enable direct access to the organization's corporate network must confirm the Home Wireless Device Requirements outlined in the Wireless Communication Standard.

- Wireless infrastructure devices that do not meet the Home Wireless Device Requirements must be installed in such a way that they do not allow direct access to the organization's corporate network. Any device must use standard remote access authentication to connect to the organization's corporate network.

\*\*Application security:

The following factors are used to assess the security of web applications:

- Before the acceptance of the change control documentation and/or release into the live environment, any new or major application release will be subjected to a proper review.

- Third-party or acquired web applications shall be subject to a proper review before being restricted by policy requirements.

- Point Releases - will be subject to a suitable level of assessment based on the risk of changes in application functionality and/or architecture.

- An emergency release will be permitted to skip security evaluations and carry the anticipated risk until a proper assessment can be performed.

- All applications will be subjected to a comprehensive annual evaluation to assess potential risks of functioning and/or architecture.

All security concerns detected during assessments must be mitigated based on the risk levels listed below. The OWASP Risk Rating Methodology is used to determine the Risk Levels. To validate remedy and/or mitigation plans for any found issues with a Medium risk level or higher, remediation validation testing will be necessary.

High, medium, low risk mitigations:

- High - Any high-risk issue must be resolved quickly, or alternative mitigation techniques must be implemented to restrict exposure prior to deployment.

- Medium- risk issues should be examined to identify what mitigation is required and scheduled accordingly. Medium-risk applications may be pulled down or denied release into the live environment depending on the number of issues and whether several concerns raise the risk to an unacceptable degree.

-Low - The issue should be assessed to see what is needed to fix it and scheduled accordingly.

The InfoSec organization or other designated organization that will be undertaking the assessments must create the following security assessment levels.

 A full assessment includes testing for all known web application vulnerabilities using both automated and manual techniques in accordance with the OWASP Testing Guide. A comprehensive assessment will utilize manual penetration testing methodologies to confirm detected vulnerabilities in order to establish the overall risk of any and all discovered vulnerabilities.

A quick evaluation will include an automated scan of an application for the OWASP Top Ten web application security risks.

A targeted assessment is carried out to validate vulnerability repair updates or new application functionality.

\*\*server security:

\_\*Database credentials policy:

General requirements:

Access by software programs must be provided only after authentication using credentials in order to protect the security of the organization's internal databases. The credentials used for this authentication must not be in clear text or easily reversed encryption in the main, running body of the program's source code. Database credentials must not be kept in a location accessible via a web server or by a secured access door that works by an identity check using biometrics. According to the date of implementation, algorithms in use must fulfill the CONSENSUS POLICY RESOURCE COMMUNITY 2022 Institute criteria set for use in NIST publication FIPS 140-2 or any succeeding document. For asymmetric encryption, the RSA and Elliptic Curve Cryptography (ECC) methods are strongly recommended.

Specific requirements (about the storage of data base usernames and passwords):

- Database usernames and passwords can be saved in a file separate from the program's active code. This file cannot be read or written by anyone in the world.

- The database credentials could be stored on the database server. In this situation, a hash function number identifying the credentials may be kept in the program's executing body.

- Database credentials can be stored as part of an authentication server, such as an LDAP server, which is used for user authentication. As part of the user authentication procedure at the authentication server, database authentication may occur on behalf of a program. There is no need to use database credentials programmatically in this scenario.

- Database credentials should not be stored in a web server's documents tree.

- The Password Policy must be followed when creating passwords or passphrases for database access.

Retrieval to database usernames and passwords:

- If database user names and passwords are kept in a file that is not source code, they must be read from the file immediately before usage. The RAM containing the database is immediately cleared after database authentication. Both the user name and the password must be released or cleared.

- The scope in which you may store database credentials must be physically segregated from the rest of your code, for example, in a separate source file. The credentials file must contain only the credentials (i.e., the user name and password) and any functions, routines, or methods that will be used to access the credentials.

- For languages that execute from source code, the source file for the credentials must not be in the same browsable or executable file directory tree as the executing body of code.

Access to database usernames and passwords:

- Every software or set of programs that implements a single business function must have its own database credentials. Credential sharing between programs is not permitted.

- Database passwords used by programs are defined as system-level passwords under the Password Policy.

- Developer groups must have a procedure in place to control and change database passwords in compliance with the Password Policy. This procedure must contain a technique for restricting database password knowledge to those who have a need-to-know basis.

-  Any Users or software accessing sensitive data must be subjected to appropriate access control and should not be allowed to undertake privileged activities that are outside the scope of said user and/or software.

\_\*server security policy:  
General requirements:

-All internal servers deployed within the organization must be owned by a system administration operational group. Each operational group must produce and maintain appropriate server configuration guides based on business needs.

-Authorized people may monitor and audit equipment, systems, processes, and network traffic by the Auditor for security, compliance, and maintenance purposes.

Configuration requirements:

-The operating system should be configured in compliance with approved Information security team criteria.

-If possible, services and applications that will not be used must be disabled.

-If possible, access to services should be logged and protected using access control measures such as a web application firewall.

-The most recent security updates must be deployed on the system as soon as possible, with the exception of when immediate application would conflict with business requirements.

-The use of trust relations between systems is a security risk and should be avoided. When another mode of communication is adequate, do not rely on a trust relationship.

-Always follow the standard security principle of requiring the least amount of access to complete a function. Use a non-privileged account instead of root.

-If a secure channel connection approach is available privileged access should be provided over secure channels.

-Servers must be actually located in a secure, access-controlled environment.

-Servers are not permitted to operate from uncontrolled or insecure cubicle areas.

Monitoring:  
-All security-related activities on important or sensitive systems must always be recorded and audit trails saved in the following manner:

• All security logs will be maintained public for at least one week.

• Daily incremental recording backups will be kept for a minimum of one month.

• Weekly full recording log backups will be kept for at least one month.

• Monthly complete backups will be kept for at least two years.

\_\*Software installation policy:

-Employees are not permitted to install software on the organization's computer devices that are connected to the organization's network.

-Software requests first need to be approved by the requester's management before being submitted in writing or through email to the Information technology department or help desk.

-Unless no option on the list fulfills the requester's needs, software must be chosen from an approved software list maintained by the Information technology department.

-The Information technology department will procure and track licenses, test new software for compatibility and conflict, and install it.

\_\*Technology equipment disposal policy:

-When a technology asset has reached the end of its useful life, it should be delivered to the disposal department office for proper disposal.

-All storage mediums will be safely erased by the disposal team in following current industry standards.

-All data, including files and licensed software, must be deleted from equipment using disk deleting software that empties the media by overwriting each disk sector of the computer with zero-filled blocks in accordance with Department of Defense requirements.

-No computer or technological equipment can be sold to anybody other than through the channels outlined in this policy.

-Computer equipment should not be disposed of in skips, dumps, or landfills. Electronic recycling containers should be placed in strategic areas around the organization on a regular basis. These can be used to get rid of unwanted items.

-All electronic drives should always be rewritten with a disk cleaning program that is commercially available. In addition, hard drives can be removed and rendered unreadable.

-Computer equipment includes desktop, laptop, tablet, and netbook computers, printers, copiers, monitors, servers, portable devices, telephones, cell phones, disc drives or any storage device, and network interface cards. Switches, routers, wireless access points, batteries, backup tapes, and other similar devices.

-The equipment will be labeled by the disposal team. The case showing that the disk erase has been completed. The label will indicate the date as well as the technician's initials who performed the disk wipe.

-The memory or storage device in technological equipment with broken memory or storage will be removed and physically destroyed.

Purchasing disposed equipment:

-Employees will be able to acquire working equipment that has approached the end of its lifespan for the business.

-To determine who gets the opportunity to purchase available equipment, a random choosing system will be used.

-All purchases of equipment must go through the random draw. Employees cannot directly purchase an office computer. This assures that every employee has an equal opportunity to get equipment.

-Each item's cost will be determined by finance and information technology.

-All sales are final. Any equipment sold will come with no guarantee or support.

-Any equipment that is no longer in functioning order or that is left over from the drawing process shall be given or thrown away in accordance with current environmental regulations. Information.

-Technology has entered into agreements with a number of groups to donate or appropriately dispose of outdated technology.

\*\*General policies:

\_\*Email policy:

-All email usage must adhere to the organization's policies and procedures for ethical behavior, safety, respect for applicable laws, and appropriate business practices.

-The organization's email account should be used primarily for business purposes, but non-organizational commercial applications are prohibited.

-The Data Protection Standard requires that all of the organization's data stored within an email or an attachment be secured.

-Email should be kept only if it is a warmaksan business record. If there is a real and ongoing business reason to maintain the data contained in the email, it is the organization's business record.

-Email identified as an organizational record must be kept in accordance with the organization record retention schedule.

-It is permitted to use a reasonable proportion of the organization's resources for personal emails, however non-work-related emails must be saved in a different folder from work related emails. It is forbidden to send chain letters or humorous emails from the organization's email account.

-Employees of warmaksan have no right to privacy in whatever they keep, transmit, or receive via the company's email system.

-Warmaksan reserves the right to monitor messages at any time. The company is not required to monitor email messages.

\_\*Password construction guide lines:

Strong passwords are lengthy because it is more secure.

All work-related passwords should have at least 16 characters.

Also, we promote the usage of passphrases, which are passwords made up of numerous words.

\_\*password creation:

-all the passwords should conform under the password guidelines.

-the password should be unique and not related to anything.

-the employees can use a secure password managing and storing system.

\_\*changing the password:

Passwords should be changed for a clear reason in such they failed.

\_\*password protection:

-password should not be shared with any one.

-password should not be written in an email, document or shown to anyone.

Password can only be stored on an authorized password manager.

-Don’t use the “remember password” feature on any site.

-if a password is suspected to be compromised it has to be changed.

\_\*multi factor authentication:

-Multi factor authentication is highly encouraged to use whenever possible.

\_\*CCTV policy:

The CCTV system should only be used for the following situations:

-to ensure the safety of the staff and visitors.

-to monitor the organizations doors.

-to ensure the security of the properties.

-to investigate any unacceptable events or situations.

[F][G] \*\*Disaster recovery plan main components:

-DRP team:

A group of individuals that is responsible for planning and documenting and executing the recovery plan, the team should be experienced with IT, emergency management and business continuity, the team should also be able to manage the possible risks and ensuring the security and safety of the physical locations.

-RTO:

Recovery time objective is the time in which a business prosses and information is restored after a disaster or a disruption, the RTO should be realistic and achievable based of the amount of process or information that got destroyed, RTO helps the business recover more quickly in case if anything happened.

-RPO:

Recovery point objective is the maximum acceptable amount of data that can be lost after a disaster or an incident, RPO can be beneficial to the company by preventing the loos of data improve the speed and efficiency of the DRP, and it keeps the DRP under a specific requirement.

-Backups:

Backups are very important after a disaster because they take any of the data that has been destroyed from, backups make the data recovering much easier and faster, the backups should be stored in a safe location that is protected and regulated from all the elements that could harm the data.

-Documentation:

The DRP should be documented so in case of any event happening the instructions can easily be followed, the documentation should include all the components of the DRP, the documentation should always be reviewed and changed to be up to date and be effective.

-Automation:

The automation of the DPR can help implement it much easier and much faster and with less room for mistakes, automation can be used for things such as giving notification in case of an event and the process of making backups.

