LAB 3
Assessment Worksheet
Elements of a Remote Access Domain Policy

Course:	**POLICY DEVELOPMENT IN INFORMATION ASSURANCE (IAP301)**
Semester:	**SP24**
Class:	**IA1702**
Name:	**Trần Minh Triết**
(roll numbers):	**SE172241**

Overview

For each of the identified risks and threats within the Remote Access Domain, identify a security control or security countermeasure that can help mitigate the risk or threat. These security controls or security countermeasures will become the basis of the scope of the Remote Access Domain Policy definition to help mitigate the risks and threats commonly found within the Remote Access Domain.

Remote Access Domain Risks & Threats	**Risk Mitigation Tactic/Solution**
Brute force user ID and password attacks	Have users use long IDs and passwords and use numbers and characters
Multiple logins retries and access control attacks.	Limiting login attempts
Unauthorized remote access to IT systems, applications, and data	Lock the user down from the system and secure all data they were after
Privacy data or confidential data is compromised remotely	Data encryption Data loss prevention (DLP) solutions
Data leakage in violation of existing Data Classification Standards	Create a key filtering for content that may contain classified data or use data finger printing
Mobile worker laptop is stolen	Full disk encryption
Mobile worker token or other lost or stolen authentication device	Device deactivation Backup authentication methods

	Lost or stolen device report
Remote worker requires remote access to medical patient online system through the public Internet	Zero Trust Network Access (ZTNA) VPN to accessing sensitive systems Data encryption
Users and employees are unaware of the risks and threats caused by the public Internet	Acceptable Use and Security Policies Remote Access Policy for Remote Workers Medical Clinics

Define a Remote Access Policy to Support Remote Healthcare Clinics

Overview:

In this lab, you are to create an organization-wide Remote Access Policy for a mock organization under a recent compliance law. Here is your scenario:

- Regional ABC Healthcare Provider with multiple remote, healthcare branches and locations throughout the region.
- Online access to patients' medical records through the public Internet is required for remote nurses and hospices providing in-home medical services.
- Online access to patients' medical records from remote clinics is done through SSL VPN secure web application front-end through the public Internet.
- The organization wants to be in compliance with HIPAA and IT security best practices regarding remote access through the public Internet in the Remote Access Domain.
- The organization wants to monitor and control the use of remote access by implementing system logging and VPN connections.
- The organization wants to implement a security awareness & training policy mandating that all new hires and existing employees obtain remote access security training. Policy definitions include HIPAA and ePHI (electronic personal healthcare information) security requirements and a mandate for annual security awareness training for all remote or mobile employees.

Instructions

Using Microsoft Word, create a Remote Access Policy Definition capturing the elements of the policy as defined in the Lab #6 – Assessment Worksheet. Use the following policy template for the creation of your Remote Access Policy definition for a regional healthcare provider with remote medical clinics.

ABC Healthcare Provider

Remote Access Policy for Remote Workers & Medical Clinics

Policy Statement

The remote access policy of [Regional Healthcare Provider] is established to govern the access of employees and authorized personnel to the organization's network resources remotely. This policy outlines the guidelines and procedures necessary to ensure secure and reliable remote access while maintaining the confidentiality, integrity, and availability of sensitive healthcare information.

Purpose/Objectives

The purpose of this policy is to:

- Facilitate secure remote access to organizational resources for employees and authorzed personnel.
- Ensure compliance with regulatory requirements such as HIPAA and HITECH.
- Mitigate the risks associated with unauthorized access to sensitive healthcare data.
- Enhance productivity and efficiency by enabling remote work capabilities for eligible employees.
- Safeguard the organization's network infrastructure from external threats.

Scope

This policy applies to all employees, contractors, vendors, and any other individuals requiring remote access to [Regional Healthcare Provider]'s network resources. The following domains of the IT infrastructure are impacted:

- User Domain
- Workstation Domain
- LAN Domain
- WAN Domain
- Remote Access Domain

Elements within the scope of this policy include but are not limited to:

- Remote access technologies (e.g., VPN, remote desktop services)
- End-user devices used for remote access (e.g., laptops, smartphones)
- Network infrastructure supporting remote access
- Security mechanisms (e.g., encryption standards, authentication methods)

Standards

This policy adheres to the following standards:

- Encryption standards: All remote access connections must utilize strong encryption protocols such as AES for data confidentiality.

- SSL VPN standards: Remote access to internal resources must be conducted through SSL VPN tunnels to ensure secure transmission of data.

- Authentication standards: Multi-factor authentication (MFA) is mandatory for all remote access connections to verify the identity of users.

Procedures

Implementation of this policy will be executed organization-wide through the following procedures:

- Distribution and acknowledgment: All employees and relevant stakeholders will receive a copy of the remote access policy and must acknowledge their understanding and compliance.

- Access provisioning: Remote access accounts will be provisioned only to authorized individuals following the principle of least privilege.

- Security awareness training: Annual security awareness training sessions will be conducted to educate remote workers and mobile employees on best practices for secure remote access and data handling.

Guidelines

To address implementation challenges, the following guidelines will be followed:

- Regular audits: Periodic audits will be conducted to review remote access logs and identify any unauthorized access attempts or anomalies.

- Incident response plan: An incident response plan will be developed and maintained to address security incidents related to remote access breaches promptly.

- Continuous monitoring: Ongoing monitoring of remote access connections will be performed to detect and respond to any security threats in real-time.

By adhering to this remote access policy, [Regional Healthcare Provider] aims to ensure the secure and efficient operation of its remote access infrastructure while safeguarding sensitive healthcare information.

Define a Remote Access Policy to Support Remote Healthcare Clinics

What are the biggest risks when using the public Internet as a WAN or transport for remote access to your organization's IT infrastructure?

Overview:

This lab presents the risks and threats commonly found in the Remote Access Domain and how the use of the public Internet introduces new challenges regarding security and compliance for organizations. The students created a Remote Access Policy definition specific to a healthcare organization requiring remote access to patients' medical records systems from remote clinics and patient homes from mobile nurses and healthcare providers in the field.

1. What are the biggest risks when using the public Internet as a WAN or transport for remote access to your organization's IT infrastructure?
    - ***Unauthenticated access****: Public networks are vulnerable to eavesdropping and attacks.*
    - ***Malware attacks****: Malicious software can be downloaded unknowingly.*
    - ***Data breaches****: Sensitive information can be intercepted or stolen.*
    - ***Compliance violations****: Improper access can violate HIPAA and other regulations.*

2. Why does this mock healthcare organization need to define a Remote Access Policy to properly implement remote access through the public Internet?
    - *Defines secure access procedures to comply with regulations.*
    - *Minimizes risks associated with public internet use.*
    - *Provides clear guidelines for authorized users.*

3. What is the relationship between an Acceptable Use Policy (AUP) and a Security Awareness & Training Policy?
    - ***AUP****: Defines acceptable and unacceptable uses of IT resources.*
    - ***Security Awareness Training****: Educates users on security risks and best practices to mitigate them.*
    - ***Relationship****: AUP provides the rules, while training equips users to follow them.*

4. One of the major prerequisites for this scenario was the requirement to support nurses and healthcare professionals that are mobile and who visit patients in their homes. Another requirement was for remote clinics to access a shared patient medical records

system via a web browser. Which type of secure remote VPN solution is recommended for these two types of remote access?

- ***SSL VPN****: Provides secure access through a web browser, suitable for both remote clinics and mobile nurses accessing patient records.*

5. When trying to combat unauthorized access and login attempts to IT systems and applications, what is needed within the LAN-to-WAN Domain to monitor and alarm on unauthorized login attempts to the organization's IT infrastructure?
    - ***Intrusion Detection/Prevention Systems (IDS/IPS)****: Monitors network traffic for suspicious activity and alerts administrators.*
    - ***Log aggregation and analysis****: Centralizes and analyzes logs from various sources to detect unauthorized login attempts.*

6. Why is it important to mobile workers and users about the risks, threats, and vulnerabilities when conducting remote access through the public Internet?
    - *Empowers users to identify and avoid threats.*
    - *Reduces risk of accidental data breaches.*
    - *Enhances compliance with security policies.*

7. Why should social engineering be included in security awareness training?
    - *Users often fall victim to social engineering attacks.*
    - *Training helps them recognize and resist such tactics.*
    - *Protects sensitive patient information.*

8. Which domain (not the Remote Access Domain) throughout the seven domains of a typical IT infrastructure supports remote access connectivity for users and mobile workers needing to connect to the organization's IT infrastructure?
    - ***WAN Domain****: Provides the connection between remote users and the organization's network.*

9. Where are the implementation instructions defined in a Remote Access Policy definition? Does this section describe how to support the two different remote access users and requirements as described in this scenario?
    - ***Procedures section****: Defines how to request, provision, manage, and use remote access.*
    - ***Guidelines section****: Addresses potential roadblocks and implementation challenges.*
    - *Both sections may need adaptation to support specific user needs.*

10. A remote clinic has a requirement to upload ePHI data from the clinic to the organization's IT infrastructure on a daily basis in a batch-processing format. How

should this remote access requirement be handled within or outside of this Remote Access Policy definition?

- ***Dedicated secure file transfer solution****: More secure than standard remote access for large data volumes.*
- *Consider additional controls like encryption and access restrictions.*
- *May require separate policy or procedures outside the Remote Access Policy.*

11. Why is a remote access policy definition a best practice for handling remote employees and authorized users that require remote access from home or on business trips?
    - ***Reduced security risks****: Clear guidelines and controls minimize vulnerabilities.*
    - ***Improved compliance****: Demonstrates adherence to regulatory requirements.*
    - ***Increased user accountability****: Ensures responsible use of remote access privileges.*

12. Why is it best practice of a remote access policy definition to require employees and users to fill in a separate VPN remote access authorization form?
    - *Tracks who have access and for what purpose.*
    - *Helps ensure legitimate use and prevent unauthorized access.*
    - *Can be used for risk assessments and access reviews.*

13. Why is it important to align standards, procedures, and guidelines for a remote access policy definition?
    - *Creates a cohesive set of rules for secure remote access.*
    - *Ensures consistency in implementing security measures across all users and devices.*
    - *Minimizes confusion and simplifies enforcement of the policy.*

14. What security controls, monitoring, and logging should be enabled for remote VPN access and users?
    - ***Multi-factor authentication (MFA)****: Adds an extra layer of security to logins.*
    - ***Strong password policies****: Enforces complex passwords that are difficult to crack.*
    - ***Encryption****: Protects data transmissions from eavesdropping.*
    - ***Device security****: Requires antivirus, security updates, and endpoint protection on remote devices.*
    - ***Logging and monitoring****: Tracks access activity for security analysis and incident detection.*

15. Should an organization mention that they will be monitoring and logging remote access use in their Remote Access Policy Definition?
    - *Transparency builds trust and encourages responsible behavior.*

- *Deters malicious activity by informing users they are monitored.*
- *Important for compliance with certain regulations.*