# Lab #6: Define a Remote Access Policy to Support Remote Healthcare Clinics

**Course Name:** Policy Development in Information Assurance (IAP301)
**Student Name:** Nguyễn Trần Vinh – SE160258
**Instructor Name:** Mai Hoàng Đỉnh
**Lab Due Date:** 07/10/2023

## PART A: Elements of a Remote Access Domain Policy

### 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 | Enforce strong password policies, including minimum length, password complexity, and password rotation requirements. |
| Multiple login retries and access control attacks | Implement a lockout policy to limit the number of failed login attempts before an account is locked. |
| Unauthorized remote access to IT systems, applications, and data | Use a virtual private network (VPN) to encrypt all traffic between remote users and the corporate network. |
| Privacy data or confidential data is compromised remotely | Encrypt all sensitive data, both at rest and in transit. |
| Data leakage in violation of existing Data Classification Standards | Implement data classification standards to classify data according to its sensitivity and importance. |
| Mobile worker laptop is stolen | Encrypt all data on mobile devices. |
| Mobile worker token or other lost or stolen authentication device | Implement multi-factor authentication (2FA) to add an extra layer of security to logins. |
| Remote worker requires remote access to medical patient online system through the public Internet | Use a VPN to encrypt all traffic between the remote worker and the medical patient online system. |
| Users and employees are unaware of the risks and threats caused by the public Internet | Conduct security awareness training for all users and employees. |

## PART B: Elements of a Remote Access Domain Policy

### 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 definition to 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**

- ABC Healthcare Provider is committed to protecting the confidentiality, integrity, and availability of its information assets, including protected health information (PHI). This policy establishes the requirements for remote access to ABC Healthcare Provider's information systems, applications, and data by remote workers and medical clinics.

**Purpose/Objectives**

- Establish the rules and responsibilities for remote access to the ABC Healthcare Provider's network and information systems.
- Ensure that remote access is conducted in compliance with the organization's security policies, standards, and regulations.
- Protect the organization's data and resources from unauthorized access, disclosure, modification, or destruction.
- Minimize the risks and potential impacts of remote access incidents.

**Scope**

- All users who are authorized to access the ABC Healthcare Provider's network and information systems remotely, including employees, contractors, vendors, partners, and affiliates.

- All devices that are used to access the ABC Healthcare Provider's network and information systems remotely, including personal computers, laptops, tablets, smartphones, and other mobile devices.
- All remote access methods that are supported by the ABC Healthcare Provider, including Virtual Private Network (VPN), Secure Shell (SSH), Remote Desktop Protocol (RDP), and web-based applications.
- All seven domains of a typical IT infrastructure that are impacted by remote access, including User Domain, Workstation Domain, LAN Domain, LAN-to-WAN Domain, WAN Domain, Remote Access Domain, and System/Application Domain.

## Standards

- Encryption Standards: All remote access connections must use encryption protocols that meet or exceed the industry best practices, such as Advanced Encryption Standard (AES) or Secure Sockets Layer (SSL).
- VPN Standards: All remote access connections must use VPN technology that provides secure tunneling and authentication mechanisms, such as IPsec or SSL VPN.
- SSH Standards: All remote access connections that use SSH must use SSH version 2 or higher and disable password authentication. SSH keys must be generated and managed securely.
- RDP Standards: All remote access connections that use RDP must use RDP version 8 or higher and enable Network Level Authentication (NLA). RDP sessions must be encrypted with TLS or SSL.
- Web-based Application Standards: All web-based applications that support remote access must use HTTPS protocol and enforce strong password policies. Web-based applications must also implement security controls such as session timeout, captcha, and multifactor authentication.

## Procedures

- Remote Access Authorization: All users who need remote access must request and obtain authorization from their managers and the IT department. Users must sign a Remote Access Agreement that acknowledges their understanding and compliance with this policy and other security policies. Users must also provide information about their devices and remote access methods. The IT department will review and approve or deny the requests based on the business needs and security risks. The IT department will also assign appropriate access rights and privileges to the authorized users based on the principle of least privilege.
- Remote Access Configuration: All devices that are used for remote access must be configured in accordance with the organization's security standards. Users must install and update the required software and applications for remote access, such as VPN client, antivirus, firewall, etc. Users must also enable security features such as encryption, password protection, screen lock, etc. Users must not modify or disable any security settings or configurations without prior approval from the IT department.
- Remote Access Usage: All users who access the network and information systems remotely must follow the organization's security policies and best practices. Users must only access the data and resources that are necessary for their work. Users must not share their credentials or devices with anyone else. Users must not store any sensitive or confidential data on their devices unless it is encrypted. Users must not use public or unsecured networks or devices for remote access. Users must report any suspicious or unauthorized activities or incidents to the IT department immediately.
- Remote Access Monitoring: The IT department will monitor and audit all remote access activities and logs regularly. The IT department will also perform periodic vulnerability scans and penetration tests on the devices and systems that support remote access. The IT department will

identify and remediate any security issues or violations as soon as possible. The IT department will also review and update this policy and other security standards as needed.

**Guidelines**

- User Awareness: The IT department will provide annual or on-going security awareness training for all remote workers and mobile employees. The training will cover topics such as this policy, security standards, security risks, security best practices, security incidents, etc. The IT department will also distribute security newsletters, alerts, and reminders to the users regularly. The IT department will evaluate the effectiveness of the training and communication programs and make improvements as needed.
- User Support: The IT department will provide technical support and assistance for all remote workers and mobile employees. The IT department will maintain a help desk system that allows users to report problems, request services, or ask questions. The IT department will also provide user manuals, guides, and tutorials for the software and applications that are used for remote access. The IT department will strive to resolve any issues or requests in a timely and satisfactory manner.
- User Compliance: The IT department will enforce this policy and other security policies through various means, such as monitoring, auditing, testing, etc. The IT department will also conduct periodic reviews and assessments of the user compliance levels and performance. The IT department will report any non-compliance or violations to the management and take appropriate disciplinary actions, such as warnings, suspensions, revocations, terminations, etc.

# PART C

## 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

## Lab Assessment Questions & Answers

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?

**Answer:**

- **Unauthorized access**: The public Internet is a shared network, which means that anyone can potentially access the data that is transmitted over it. This makes it a prime target for hackers and other malicious actors.
- **Data breaches**: If attackers are able to gain access to your organization's IT infrastructure through the public Internet, they may be able to steal sensitive data, such as customer information, financial data, or intellectual property.
- **Malware attacks**: Attackers can use the public Internet to distribute malware, such as viruses, Trojans, and ransomware. If malware is able to infect a remote device, it could then spread to your organization's internal network.
- **Denial-of-service (DoS) attacks**: DoS attacks can be used to flood your organization's network with traffic, making it unavailable to legitimate users.

- **Man-in-the-middle attacks**: Man-in-the-middle attacks occur when an attacker intercepts communication between two parties. This type of attack could be used to steal data or impersonate one of the parties involved in the communication.

2. Why does this mock healthcare organization need to define a Remote Access Policy to properly implement remote access through the public Internet?

**Answer:**

- To protect patient privacy and security. Healthcare organizations are subject to strict privacy and security regulations, such as HIPAA. A Remote Access Policy can help to ensure that patient data is protected from unauthorized access, disclosure, or modification when accessed remotely.
- To reduce the risk of cyberattacks. The public Internet is a prime target for hackers and other malicious actors. A Remote Access Policy can help to reduce the risk of cyberattacks by implementing security measures such as VPNs, strong passwords, and 2FA.
- To improve compliance. A Remote Access Policy can help healthcare organizations to comply with industry regulations and standards. For example, HIPAA requires healthcare organizations to implement appropriate security measures to protect patient data.
- To ensure consistent implementation of remote access procedures. A Remote Access Policy can help to ensure that all remote workers and medical clinics follow the same procedures when accessing the organization's IT infrastructure.

3. What is the relationship between an Acceptable Use Policy (AUP) and a Security Awareness & Training Policy?

**Answer:**

- The relationship between an AUP and a Security Awareness & Training Policy is that they are both part of the overall information security program of an organization. They complement each other by ensuring that users are aware of their roles and responsibilities in safeguarding the information assets of the organization, as well as the consequences of violating the policies. A Security Awareness & Training Policy helps users understand and comply with the AUP, as well as other information security policies, standards, procedures, laws, regulations, and contractual terms. An AUP helps users avoid behaviors and actions that could compromise the security of the information systems and data, as well as the reputation and legal obligations of the organization.

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?

**Answer:**

- The best type of secure remote VPN solution for mobile nurses and healthcare professionals and remote clinics to access a shared patient medical records system via a web browser is a cloud-based VPN.
- Cloud-based VPNs are easy to set up and use, and they can be accessed from anywhere with an internet connection. This makes them ideal for mobile users and remote clinics. Cloud-based VPNs also offer a high level of security, using the latest encryption technologies to protect data in transit.

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?

**Answer:**

- Log management system: A log management system collects and stores logs from all IT systems and devices. This allows organizations to monitor for suspicious activity, such as failed login attempts and unusual access patterns.
- Security information and event management (SIEM) system: A SIEM system analyzes log data from a variety of sources to identify and alert on security threats. SIEM systems can be used to detect unauthorized login attempts, as well as other types of attacks, such as malware infections and data breaches.
- Intrusion detection system (IDS): An IDS monitors network traffic for suspicious activity, such as unauthorized login attempts and port scans. IDS systems can be used to detect unauthorized login attempts at the network level, before they reach the target IT system or application.
- Intrusion prevention system (IPS): An IPS is similar to an IDS, but it can also block suspicious traffic. This can be useful for preventing unauthorized login attempts from reaching the target IT system or application.

6. Why is it important to mobile workers and users about the risks, threats, and vulnerabilities when conducting remote access through the public Internet?

**Answer:**

- It is important to educate mobile workers and users about the risks, threats, and vulnerabilities when conducting remote access through the public Internet because they are more vulnerable to these risks than users who are connected to the organization's internal network.
- The public Internet is a shared network, which means that anyone can potentially access the data that is transmitted over it. This makes it a prime target for hackers and other malicious actors. Additionally, mobile workers and users may be using their own devices to connect to the organization's network, which may not be as secure as the organization's own devices.

7. Why should social engineering be included in security awareness training?

**Answer:**

- Social engineering is a type of cyberattack that relies on human psychology to manipulate people into revealing confidential information or performing actions that compromise security. Social engineering attacks can be very effective, even against people who are aware of the risks.
- That is why it is important to include social engineering in security awareness training. Security awareness training can help employees to identify and avoid social engineering attacks by teaching them about the different types of attacks and how they work.

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?

**Answer:**

- The domain that supports remote access connectivity for users and mobile workers needing to connect to the organization’s IT infrastructure, besides the Remote Access Domain, is the WAN Domain. The WAN Domain is the domain that connects the organization’s LANs to external networks, such as the Internet, other branches, or business partners. The WAN Domain provides the network infrastructure and services that enable remote access connectivity for users and mobile workers who are outside the physical boundaries of the organization. The WAN Domain can use various technologies and protocols to support remote access connectivity, such as VPNs, MPLS, SD-WAN, or cellular networks. The WAN Domain also requires proper security controls and measures to protect the data and devices that traverse the external networks, such as encryption, authentication, firewall, IDS/IPS, or SIEM.

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?

**Answer:**

- The implementation instructions are usually defined in a separate section of the remote access policy document, where the specific steps and procedures for setting up and using the remote access services are explained. This section may also include the technical requirements, such as the hardware, software, and network configurations, that the remote users and devices must meet to access the organization's network. The implementation instructions may vary depending on the type of remote access service, such as VPN, web portal, or remote desktop, that the organization provides.
- The implementation instructions should describe how to support the two different remote access users and requirements as described in this scenario. For example, the implementation instructions should specify how to install and configure the VPN client software for mobile healthcare professionals who need to access patient records and other back office services while visiting patients in their homes. The implementation instructions should also specify how to access the web portal for remote clinics that need to access a shared patient medical records system via a web browser. The implementation instructions should also provide guidance on how to troubleshoot common issues and contact technical support if needed.

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?

**Answer:**

**Handling the requirement within the Remote Access Policy definition**

- If the organization chooses to handle the requirement within the Remote Access Policy definition, it should include the following provisions:
    - The policy should define what constitutes ePHI data and how it should be protected.
    - The policy should specify the batch-processing format that the remote clinic must use to upload the ePHI data.
    - The policy should specify the frequency with which the remote clinic must upload the ePHI data.
    - The policy should specify the security measures that the remote clinic must take to protect the ePHI data during transit and at rest.

**Handling the requirement outside of the Remote Access Policy definition**

- If the organization chooses to handle the requirement outside of the Remote Access Policy definition, it should create a separate policy or procedure that addresses the specific requirements for uploading ePHI data. This policy or procedure should be referenced in the Remote Access Policy definition to ensure that remote clinics are aware of their responsibilities.
- Regardless of whether the requirement is handled within or outside of the Remote Access Policy definition, it is important to ensure that the organization has adequate security controls in place to protect the ePHI data. This includes implementing data encryption, strong passwords, and two-factor authentication.

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?

**Answer:**

- Protect the organization's IT infrastructure and data from unauthorized access: A remote access policy can help to protect the organization's IT infrastructure and data from unauthorized access by requiring remote users to use strong passwords, two-factor authentication, and a VPN to connect to the organization's network.
- Reduce the risk of security breaches: A remote access policy can help to reduce the risk of security breaches by requiring remote users to follow security best practices, such as keeping their devices up to date with the latest security patches and being careful about what emails they open and what links they click on.
- Improve compliance: A remote access policy can help organizations to comply with industry regulations and standards that require remote access security.
- Ensure consistent implementation of remote access procedures: A remote access policy can help to ensure that all remote users follow the same procedures when accessing the organization's network.

12. Why is it a best practice of a remote access policy definition to require employees and users to fill in a separate VPN remote access authorization form?

**Answer:**

- To verify the identity of the user: The authorization form can require users to provide their name, employee ID, department, and other identifying information. This helps to ensure that only authorized users are granted access to the VPN.
- To assess the user's needs: The authorization form can ask users to explain why they need remote access and what applications and resources they need to access. This helps the organization to assess the user's needs and to grant them the appropriate level of access.
- To obtain the user's consent: The authorization form can require users to consent to the organization's remote access policy and to agree to comply with the terms of the policy. This helps to protect the organization in the event of a security breach or other incident.
- To track VPN usage: The authorization form can be used to track who is using the VPN, when they are using it, and what resources they are accessing. This information can be used to identify and investigate suspicious activity.

13. Why is it important to align standards, procedures, and guidelines for a remote access policy definition?

**Answer:**

- Ensure that the policy is consistent and enforceable. When standards, procedures, and guidelines are aligned, it is easier to ensure that the policy is applied consistently to all remote users. This makes it easier to enforce the policy and to identify and investigate any violations.
- Reduce the risk of confusion and errors. When standards, procedures, and guidelines are aligned, it is less likely that remote users will become confused or make errors when trying to comply with the policy. This can help to reduce the risk of security incidents.
- Improve the overall security posture of the organization. By aligning standards, procedures, and guidelines, organizations can help to improve their overall security posture. This is because a well-aligned remote access policy can help to protect the organization's IT infrastructure and data from unauthorized access, reduce the risk of security breaches, and improve compliance.

14. What security controls, monitoring, and logging should be enabled for remote VPN access and users?

**Answer:**

**Security controls:**

- Strong authentication: All remote users should be required to use strong passwords and two-factor authentication (2FA) to access the VPN.

- VPN encryption: The VPN should use strong encryption to protect data in transit between the remote device and the organization's network.
- Authorization: Remote users should only be granted access to the resources that they need.
- Firewalls: Firewalls should be used to restrict access to the organization's network and to protect it from unauthorized access.
- Intrusion detection systems (IDS) and intrusion prevention systems (IPS): IDS/IPS systems can be used to detect and prevent malicious traffic from entering the organization's network.

**Monitoring:**

- VPN usage: VPN usage should be monitored to identify any suspicious activity, such as unusual access patterns or failed login attempts.
- Network traffic: Network traffic should be monitored to identify any suspicious activity, such as malware infections or data breaches.
- Security logs: Security logs should be monitored to identify any suspicious activity, such as failed login attempts, unauthorized access to resources, or malware infections.

**Logging:**

- VPN logins: All VPN logins should be logged to track who is accessing the VPN and when.
- Network traffic: Network traffic should be logged to track what traffic is entering and leaving the organization's network.
- Security events: All security events, such as failed login attempts, unauthorized access to resources, and malware infections, should be logged.

15. Should an organization mention that they will be monitoring and logging remote access use in their Remote Access Policy Definition?

**Answer:**

- Yes, an organization should mention that they will be monitoring and logging remote access use in their Remote Access Policy Definition. This is important for transparency, accountability, and compliance purposes. By informing the remote users of the monitoring and logging activities, the organization can ensure that they are aware of the security risks and best practices when connecting to the network from outside the office. The organization can also use the monitoring and logging data to audit the remote access usage, identify and resolve any issues, and generate reports for management or regulatory bodies.