Lab #10 – Assessment Worksheet
Part A – Policy Statement Definitions

Course Name: IAP401
Student Name: Dang Hoang Nguyen

Risk – Threat – Vulnerability	**IT Security Policy Definition**
Unauthorized access from public Internet	**Policy Statement:** It is totally forbidden to gain unauthorized access from the public Internet. All remote access to the IT infrastructure of the company needs to be duly permitted and securely authenticated using techniques that have been approved, like multi-factor authentication VPN connections. **Purpose/Objectives:** • Assure the IT infrastructure of the company is secure and reliable. • Prevent cyber risks and attacks that come from the public Internet. Safeguard confidential information and resources against illegal access and use. **Scope:** This policy applies to all users, employees, contractors, and third parties accessing the organization's IT systems and resources remotely from the public Internet. **Standards**: • Remote access requires the implementation of robust authentication methods, such as multi-factor authentication (MFA). • In order to protect data while it is being transmitted over the open Internet, encryption mechanisms like SSL/TLS need to be enforced. • Firewalls and access control lists need to be set up to prevent

	unwanted access attempts from the public Internet. Protocols: • Consistently examine and modify access control policies and configurations to accommodate new threats and weaknesses. • Perform recurring audits and security assessments to make sure the policy is being followed. • Train staff members on security awareness, emphasizing the need of following security procedures and the dangers of unauthorized access over public WiFi. Guidelines: • Keep an eye on network traffic and log files in case you notice any illegal or suspicious efforts to access data coming from the public Internet. • Use intrusion detection and prevention systems to instantly identify and stop efforts by unauthorized users to gain access.
User destroys data in application and **deletes all files**	Policy Statement: Users are prohibited from intentionally destroying data in applications and deleting files without proper authorization. Any unauthorized modification or deletion of data constitutes a serious violation of IT security policies and may result in disciplinary action. Purpose/Objectives: • Safeguard the integrity and availability of data stored within applications and file systems.

	• Prevent unauthorized data loss or destruction that could impact business operations and continuity. • Establish accountability and deterrence against malicious actions by users. Scope: This policy applies to all users, employees, contractors, and third parties with access to the organization's applications and file systems. Standards: • Role-based access controls must be implemented to restrict users' ability to modify or delete data based on their job responsibilities. • Data backup and recovery procedures must be in place to restore lost or corrupted data in the event of unauthorized deletion or modification. • Logging and monitoring mechanisms must be deployed to track user actions and detect unauthorized data manipulation. Procedures: • Regularly review access permissions and user privileges to ensure they align with business requirements and least privilege principles. • Implement data loss prevention (DLP) solutions to detect and prevent unauthorized data destruction or deletion. • Conduct regular security awareness training to educate users about the importance of data security and the consequences of unauthorized actions.

	Guidelines: • Enforce strong password policies and implement session management controls to prevent unauthorized access to applications and file systems. • Implement file integrity monitoring systems to detect and alert on unauthorized changes to critical files and configurations.
Hacker penetrates your IT infrastructure and gains access to your **internal network**	Policy Statement: • Quick action is required to minimize security breaches, lessen their effects, and resume regular business activities in the event that a hacker breaches the organization's IT infrastructure and gains unauthorized access to the internal network. The coordination of response activities and the execution of corrective actions are within the purview of the incident response team. Purpose/Objectives: • Recognize security breaches and take immediate action to reduce the impact on data integrity and business operations. • Stop the attacker's further illegal access and data espionage. • Maintain the chain of custody and preserve the evidence for forensic examination and court cases. Scope: • This policy applies to all employees, contractors, and third-party service providers involved in incident

	response and security incident management. Standards: • An incident response plan must be developed, documented, and regularly tested to ensure readiness to handle security incidents effectively. • Incident response procedures must include predefined steps for identifying, containing, eradicating, and recovering from security breaches. • Communication protocols must be established to notify stakeholders, including management, IT staff, and legal counsel, of security incidents and response actions. Protocols: • Call in the Incident Response Team and start the incident response process in accordance with the incident response plan that has been previously established. • Work together as a team to control the breach and look into the occurrence, as well as with outside partners and law enforcement. • Keep track of every step you take in the incident response process, such as gathering and analyzing evidence and carrying out cleanup operations. Guidelines: • To restrict the ability of attackers to move laterally within the internal network, implement access limits and network segmentation.

	• Keep an eye out for unusual activity and indicators of compromise in network traffic and endpoints to spot intrusions early. • Perform lessons learned sessions and post-event reviews to pinpoint problem areas and strengthen incident response capabilities.
Intra-office employee romance gone bad	• **Standard:** Implement a workplace conduct policy outlining expectations for professional behavior, relationships, and conflict resolution. • **Guideline:** Provide training on workplace ethics and interpersonal relationships to mitigate potential conflicts. • **Procedure:** Establish a process for reporting and addressing workplace conflicts, including mediation and disciplinary actions if necessary. • **Asset Identification:** Identify personnel and human resources as critical assets requiring protection. • **Classification Policy:** Classify personnel-related data as sensitive and restrict access to authorized personnel only.
Fire destroys primary **data center**	• **Standard:** Implement a disaster recovery plan (DRP) to ensure business continuity in the event of a data center outage. • **Guideline:** Conduct regular backups and offsite storage of critical data to facilitate recovery efforts. • **Procedure:** Define roles and responsibilities for executing the DRP, including data restoration and system recovery processes. • **Asset Identification:** Identify data center facilities and infrastructure as critical assets requiring protection.

	• **Classification Policy:** Classify data based on importance and criticality for prioritized recovery efforts.
Communication circuit outages	• **Standard:** Implement redundant communication circuits and failover mechanisms to minimize service disruptions. • **Guideline:** Regularly monitor communication circuits for performance and availability issues. • **Procedure:** Establish protocols for notifying stakeholders and coordinating with service providers to troubleshoot and resolve outages. • **Asset Identification:** Identify communication infrastructure and services as critical assets requiring protection. • **Classification Policy:** Classify communication circuits based on importance and impact on business operations.
Workstation OS has a known **software vulnerability**	• **Standard:** Implement a patch management policy to regularly update and patch operating systems and software. • **Guideline:** Monitor security advisories and vendor announcements for patches and updates. • **Procedure:** Schedule and deploy patches promptly to mitigate vulnerabilities and minimize the risk of exploitation. • **Asset Identification:** Identify workstations as critical assets requiring protection. • **Classification Policy:** Classify vulnerabilities based on severity and prioritize patching accordingly.

Unauthorized access to organization owned **Workstations**	• **Standard:** Implement access control measures, such as user authentication and privilege management, to prevent unauthorized access. • **Guideline:** Enforce strong password policies and implement multi-factor authentication where feasible. • **Procedure:** Monitor and audit user activity on workstations to detect and respond to unauthorized access attempts. • **Asset Identification:** Identify workstations and user accounts as critical assets requiring protection. • **Classification Policy:** Classify sensitive data accessed from workstations and restrict access based on need-to-know.
Loss of production **data**	• **Standard:** Implement data backup and recovery procedures to ensure the integrity and availability of production data. • **Guideline:** Regularly test data backup and recovery processes to verify their effectiveness. • **Procedure:** Establish protocols for data restoration in the event of data loss or corruption. • **Asset Identification:** Identify production data and storage systems as critical assets requiring protection. • **Classification Policy:** Classify production data based on importance and sensitivity for prioritized backup and recovery efforts.
Denial of service attack on organization e-mail Server	• **Standard:** Implement network security measures, such as firewalls and intrusion prevention systems, to detect and mitigate denial of service attacks.

	• **Guideline:** Monitor network traffic for signs of suspicious activity and anomalous patterns indicative of denial of service attacks. • **Procedure:** Activate incident response protocols to mitigate the impact of the attack and restore email services. • **Asset Identification:** Identify email server infrastructure as critical assets requiring protection. • **Classification Policy:** Classify email services as critical for business operations and prioritize their protection against denial of service attacks.
Remote communications from home office	• **Standard:** Implement secure remote access protocols, such as VPN, with strong encryption and authentication. • **Guideline:** Educate remote users on best practices for secure remote communication, including password hygiene and device security. • **Procedure:** Require remote users to use company-provided devices or secure personal devices for remote communication. • **Asset Identification:** Identify remote access infrastructure and endpoints as critical assets requiring protection. • **Classification Policy:** Classify remote communications based on sensitivity and ensure encryption and data protection measures are applied accordingly.
LAN server OS has a **known software vulnerability**	• **Standard:** Implement a patch management policy to regularly update and patch server operating systems and software. • **Guideline:** Monitor security advisories and vendor

	announcements for patches and updates. • **Procedure:** Schedule and deploy patches promptly to mitigate vulnerabilities and minimize the risk of exploitation. • **Asset Identification:** Identify LAN servers as critical assets requiring protection. • **Classification Policy:** Classify vulnerabilities based on severity and prioritize patching accordingly.
User downloads an unknown e –mail attachment	• **Standard:** Implement email security controls, such as spam filters and antivirus scanning, to detect and block malicious email attachments. • **Guideline:** Educate users on identifying and avoiding suspicious email attachments and phishing attempts. • **Procedure:** Establish protocols for handling suspicious email attachments, including reporting to IT security for analysis. • **Asset Identification:** Identify email systems and user devices as critical assets requiring protection. • **Classification Policy:** Classify email attachments based on risk and enforce policies for safe handling and execution.
Workstation browser has software vulnerability	• **Standard:** Implement web browser security updates and patches regularly. • **Guideline:** Educate users on safe browsing habits and avoiding potentially malicious websites. • **Procedure:** Configure web browsers to block or warn about potentially harmful content and restrict browser extensions. • **Asset Identification:** Identify workstations and web browsers as critical assets requiring protection.

	• **Classification Policy:** Classify web browsing activities based on risk and enforce policies for safe browsing and content filtering.
Service provider has **a major network** outage	• Standard: Establish service level agreements (SLAs) with service providers to ensure availability and performance requirements. • Guideline: Maintain redundant network connections and failover mechanisms to mitigate the impact of service provider outages. • Procedure: Activate incident response protocols to communicate with the service provider and implement contingency plans to restore services. • Asset Identification: Identify network connections and service provider relationships as critical assets requiring protection. • Classification Policy: Classify network services based on importance and prioritize redundancy and resilience measures accordingly.
Weak ingress/egress traffic filtering degrades **Performance**	• **Standard:** Implement robust traffic filtering mechanisms at ingress and egress points to control and optimize network traffic. • **Guideline:** Regularly monitor network performance and conduct traffic analysis to identify and address performance degradation issues. • **Procedure:** Configure and maintain traffic filtering rules and policies to prioritize critical traffic and block or throttle non-essential traffic. • **Asset Identification:** Identify ingress and egress points, network devices, and traffic filtering tools as critical assets requiring protection.

	• **Classification Policy:** Classify network traffic based on importance and prioritize bandwidth allocation and traffic shaping accordingly.
User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	• **Standard:** Prohibit the use of unauthorized external storage devices on organization-owned computers. • **Guideline:** Educate users on the risks of using unauthorized external storage devices and provide secure alternatives for transferring files. • **Procedure:** Implement endpoint security measures to detect and block unauthorized device connections and enforce compliance with policy. • **Asset Identification:** Identify organization-owned computers and external storage devices as critical assets requiring protection. • **Classification Policy:** Classify data stored on external storage devices based on sensitivity and restrict access and usage accordingly.
VPN tunneling between **remote computer** and **ingress/egress router**	• **Standard:** Implement secure VPN protocols and encryption to protect data transmitted between remote computers and the network. • **Guideline:** Configure VPN clients and routers to use strong authentication methods and encryption algorithms. • **Procedure:** Establish VPN access controls and monitor VPN connections for security compliance and unauthorized access attempts. • **Asset Identification:** Identify VPN endpoints, remote computers, and network infrastructure as critical assets requiring protection. • **Classification Policy:** Classify VPN traffic based on sensitivity and

	apply encryption and access controls accordingly.
WLAN access points are needed for LAN connectivity **within a warehouse**	• **Standard:** Deploy secure WLAN access points with strong encryption and authentication mechanisms to prevent unauthorized access. • **Guideline:** Perform site surveys and RF analysis to optimize WLAN coverage and minimize interference. • **Procedure:** Configure WLAN access points with secure settings, such as SSID hiding, MAC filtering, and WPA2-PSK encryption. • **Asset Identification:** Identify WLAN access points, warehouse LAN infrastructure, and wireless devices as critical assets requiring protection. • **Classification Policy:** Classify WLAN traffic based on importance and sensitivity, and enforce access controls and encryption to protect data transmission.
Need to **prevent rogue users** from unauthorized WLAN access	• **Standard:** Implement network access control (NAC) mechanisms to authenticate and authorize devices before granting access to the WLAN. • **Guideline:** Educate users on the importance of WLAN security and the risks associated with unauthorized access. • **Procedure:** Monitor WLAN traffic for unauthorized devices and behavior, and take action to block or quarantine rogue users. • **Asset Identification:** Identify WLAN infrastructure and devices as critical assets requiring protection. • **Classification Policy:** Classify WLAN access based on user roles and privileges, and enforce access controls and authentication

	mechanisms to prevent unauthorized access

1. Access Control Policy Definition

This policy lays out the rules and processes for controlling who has access to data, applications, and systems that belong to the company. It lays out who is responsible for creating authorization restrictions, maintaining user access permissions, and enforcing authentication procedures. This policy assists in reducing the possibility of illegal access from both internal and external sources by explicitly defining access requirements and limits.

2. Business Continuity – Business Impact Analysis (BIA) Policy Definition

In order to prioritize recovery efforts, identify essential business operations, and evaluate potential implications of disruptions, this policy describes the steps and standards for completing a Business Impact Analysis (BIA). This policy guarantees that the company can efficiently detect and mitigate risks to its operations, hence boosting its resilience and ability to sustain continuity in the event of interruptions. It does this by outlining roles, responsibilities, and processes for BIA.

3. Business Continuity & Disaster Recovery Policy Definition

The organization's general framework and protocols for guaranteeing business continuity and catastrophe recovery capabilities are laid forth in this policy. In addition to outlining the tactics and procedures for minimizing disruptions, it also specifies the roles and duties of important staff and requires the creation and upkeep of thorough continuity and recovery plans. This policy assures the organization's ability to quickly recover from disruptions, reduces downtime, and protects important assets by offering direction on proactive planning, response processes, and recovery techniques.

4. Data Classification Standard & Encryption Policy Definition

This policy lays out the standards and methods for grouping data according to how sensitive and important it is, as well as the steps involved in encrypting it to safeguard privacy. It defines the encryption protocols and procedures to be used for protecting data in transit and at rest, as well as the duties of data owners, custodians, and users while handling classified material. This policy assists in preventing violations of regulatory compliance, data breaches, and unauthorized access by putting in place explicit classification rules and encryption procedures.

5. Internet Ingress/Egress Traffic & Web Content Filter Policy Definition

To reduce security risks and uphold acceptable usage norms, this policy sets rules and controls for handling both incoming and outgoing internet traffic as well as web content screening. It outlines the standards for web content filtering tool configuration and management, as well as the protocols for examining and screening network traffic at entry and egress points. This policy helps defend against viruses, phishing attempts, and unauthorized access to unsuitable or hazardous content by putting in place efficient traffic filtering and web content filters.

6. Production Data Back-up Policy Definition

In the case of data loss or corruption, this policy specifies the conditions and steps for backing up important production data to guarantee its availability and integrity. It details the frequency, duration of retention, and places of storage for data backups in addition to the procedures for testing and verifying backup integrity. This policy's establishment of strong backup procedures and guidelines lessens the effects of data loss events and makes prompt recovery operations easier.

7. Remote Access VPN Policy Definition

Through the use of virtual private network (VPN) connections, this policy establishes the guidelines and practices for safely accessing organizational resources from remote locations. It describes the prerequisites for setting up VPN client software and network equipment, encrypting data transfers, and authenticating remote users. This policy assists in defending against cyberthreats that target remote connections, illegal access, and data interception by enforcing secure remote access procedures.

8. WAN Service Availability Policy Definition

The standards and procedures for guaranteeing the dependability and accessibility of wide area network (WAN) services that are essential to organizational operations are outlined in this policy. In order to handle service disruptions or degradations, it sets up performance monitoring standards, escalation protocols, and service level agreements (SLAs). This policy supports proactive WAN infrastructure monitoring and repair, which reduces downtime, improves network performance, and raises overall service availability.

9. Internet Ingress/Egress Availability (DoS/DDoS) Policy Definition

The tactics and precautions against denial-of-service (DoS) and distributed denial-of-service (DDoS) assaults that target the organization's internet entry and egress points are described in this policy. It outlines the procedures for working with internet service providers (ISPs) and law enforcement organizations, as well as the roles and duties for identifying, minimizing, and responding to DoS/DDoS occurrences. This policy helps reduce the impact of DoS/DDoS attacks and sustain internet connectivity by putting proactive defense mechanisms and response protocols into place.

10. Wireless LAN Access Control & Authentication Policy Definition

This policy defines standards and procedures for controlling user authentication on wireless networks and safeguarding wireless local area network (WLAN) access points. It outlines the steps for setting up authentication methods, encryption protocols, and WLAN access controls. It also describes how to monitor and manage wireless network access. This policy assists in preventing network intrusions, illegal WLAN access, and data breaches by implementing stringent access controls and authentication procedures.

11. Internet & E-Mail Acceptable Use Policy Definition

This policy outlines the authorized use of email and the internet within the company, along with best practices for security, content limits, and acceptable usage rules. It describes what users must do to follow acceptable use guidelines, report security issues, and safeguard private information when communicating via email. This policy assists in reducing the risks associated with malware, phishing, data leaks, and compliance violations by encouraging the prudent and secure use of email and internet resources.

12. Asset Protection Policy Definition

This policy lays out how to protect organizational assets against theft, loss, or illegal access. These assets include information assets, intellectual property, and physical assets. It delineates the duties and responsibilities pertaining to asset protection, details the security mechanisms and controls that are in place to safeguard assets, and delineates the protocols for reporting and looking into occurrences involving assets. This policy helps reduce risks to vital resources and maintain the integrity and confidentiality of organizational assets by encouraging a proactive approach to asset protection.

13. Audit & Monitoring Policy Definition

This policy describes the standards and processes for carrying out audits and keeping an eye on things in order to find and stop security lapses, noncompliance, and inefficiencies in operations. It outlines the duties of those engaged in audit operations as well as the goals and purview of the monitoring and auditing procedures. This policy assists in identifying security vulnerabilities, ensuring regulatory compliance, and improving overall governance and accountability by instituting a methodical approach to auditing and monitoring.

14. Computer Security Incident Response Team (CSIRT) Policy Definition

The organization's Computer Security Incident Response Team (CSIRT) is responsible for managing and responding to security issues. This policy outlines their roles, responsibilities, and processes. It describes the communication channels and escalation mechanisms for coordinating incident response activities, as well as the protocols for incident detection, analysis, containment, eradication, and recovery. This policy aims to reduce impact, maintain the integrity and confidentiality of organizational assets, and enable a timely and effective response to security incidents by defining clear principles and response methods.

15. Security Awareness Training Policy Definition

This policy specifies the conditions and methods for educating workers, outside contractors, and other organization stakeholders about security awareness. It specifies the subjects and curricula for courses on security awareness, as well as the frequency and mode of instruction. This policy lessens human error, cultivates a workforce that is security-conscious, and strengthens the organization's resistance to security threats by fostering a culture of security awareness and education.

Lab #10 – Assessment Worksheet
Part B – Craft an IT Security Policy Definition

Course Name: IAP401
Student Name: Dang Hoang Nguyen

ABC Credit Union

Email Security Controls Policy

Policy Statement:

In order to reduce the risks related to malware threats, unauthorized access, and data breaches, the organization's email system is secured by following the rules and procedures set forth in the Email Security Controls Policy. In order to protect the privacy, availability, and integrity of email communications, this policy sets forth guidelines for using email-related technology and controls.

Purpose/Objectives:

- Make sure that private information sent by email is kept private.
- Stop illegal access to data and email accounts.
- Defend against phishing and viruses spread through emails.
- Encourage adherence to legal and regulatory obligations, such as GLBA.
- Address the requirement for thorough email security measures to close the found gap in the IT security policy framework.
- Reduce the dangers, hazards, and weaknesses that come with email correspondence, such as virus infections, illegal access, and data loss.

Scope:

All workers, subcontractors, and outside parties with access to the company's email system are subject to this policy. It affects email servers, client apps, and related network equipment within the IT infrastructure's Communication Domain. All email-related actions and conversations carried out through systems and resources owned by the organization are covered by the policy.

Standards:

- standards for encryption that protect critical email correspondence.
- methods of authentication for confirming email senders' and receivers' identities.
- requirements for anti-malware software to scan and filter email attachments and content.
- email server configuration guidelines, such as audit logging, filtering rules, and access controls.

Procedures:

- Use email encryption techniques to safeguard private data sent over the internet.

- Set up email servers to impose multi-factor authentication and other robust authentication methods.
- Use anti-malware software to scan and filter email correspondence for links and attachments that could be harmful.
- Update and patch email servers and client software often to fix vulnerabilities that are known to exist.
- Keep an eye out for security problems and questionable activities in the email traffic and access records.
- To teach staff members about phishing awareness and recommended practices for email security, offer training and awareness campaigns.

Guidelines:

- Make sure that, in order to handle new threats and vulnerabilities, email security controls are routinely examined and updated.
- Work together with pertinent stakeholders and the IT security team to continuously improve email security posture.
- Through awareness campaigns and training programs, convey to all employees the significance of email security and compliance.
- To determine what needs to be improved and to gauge how well email security safeguards are working, do audits and assessments on a regular basis.