ABC Credit Union

Policy Statement

ABC Credit Union/Bank is committed to ensuring the security, confidentiality, integrity, and availability of its information systems. This Security Management Policy establishes the framework for managing and separating duties within the seven domains of the organization's IT infrastructure. The policy aims to achieve compliance with the Gramm-Leach-Bliley Act (GLBA) and adhere to IT security best practices, with a focus on the critical business function of the customer service department. Additionally, the policy addresses the use of online banking, Internet content filtering, personal use of organization-owned IT assets, and email security controls.

Purpose/Objectives

The purpose of this policy is to:

- Define information systems security responsibilities within each of the seven domains.
- Establish a clear separation of duties to ensure the confidentiality, integrity, and availability of information.
- Achieve compliance with GLBA and IT security best practices.
- Monitor and control Internet use through content filtering.
- Eliminate personal use of organization-owned IT assets.
- Implement email security controls.
- Incorporate policy reviews into the annual security awareness training.

Scope

This policy applies to all employees, contractors, and third-party entities interacting with IT assets owned by ABC Credit Union/Bank. The seven domains impacted by this policy are:

- User Domain: All employees must adhere to security awareness training and refrain from personal use of organization-owned IT assets.
- Workstation Domain: Workstations will comply with established Workstation Configuration Standards.
- Local Area Network (LAN) Domain: Access controls will be implemented to ensure data confidentiality and integrity.
- LAN-to-WAN Domain: Internet usage will be monitored and controlled through content filtering.
- WAN Domain: Secure connections will be established to protect data during transit.
- Remote Access Domain: Access controls and secure connections will be enforced for remote access.
- System/Application Domain: Email security controls will be implemented to monitor and control email system usage

IT assets within the scope of this policy include but are not limited to computers, servers, network devices, software applications, and data repositories.

Standards

This policy references the following standards:

- Workstation Configuration Standards
- Server Configuration Standards
- Network Configuration Standards

These standards define the technical hardware, software, and configuration requirements for IT assets across the seven domains.

Procedures

User Domain:

- Users are responsible for safeguarding their credentials.
- IT administrators manage user account permissions.

Workstation Domain:

- IT administrators ensure the implementation of workstation configuration standards.
- Users adhere to policies regarding personal use and report any security incidents.

LAN Domain:

- Network administrators configure and monitor content filtering solutions.
- IT security personnel enforce policies on personal device use within the LAN.

LAN-to-WAN Domain:

- Network administrators control access between the LAN and WAN.
- IT security personnel monitor and analyze network traffic.

WAN Domain:

- Network administrators secure wide-area network connections.
- IT security personnel implement and monitor intrusion detection/prevention systems.

Remote Access Domain:

- IT administrators control remote access permissions.
- Users follow remote access policies and report any anomalies.

System/Application Domain:

- System administrators manage access controls for critical applications.

- IT security personnel implement and monitor email security controls.

Guidelines

Any disputes or gaps in duties separation will be addressed through regular reviews and updates of this policy. In cases where conflicts arise, the IT Security Officer will act as the mediator and work towards resolution, ensuring the overarching goal of information security is maintained. Implementation roadblocks will be addressed through ongoing training and communication to reinforce the importance of adhering to security policies.

For each of the seven domains of a typical IT infrastructure, summarize what the information systems security responsibilities are within that domain:

1. **User Domain:**
    - **IT Professional:** Ensure user training on security policies.
    - **Security Practitioner:** Enforce user authentication and access controls.
2. **Workstation Domain:**
    - **IT Professional:** Implement and maintain workstation configurations.
    - **Security Practitioner:** Monitor and respond to security incidents on workstations.
3. **LAN Domain:**
    - **IT Professional:** Configure and manage LAN devices.
    - **Security Practitioner:** Implement content filtering and monitor LAN security.
4. **LAN-to-WAN Domain:**
    - **IT Professional:** Control access between LAN and WAN.
    - **Security Practitioner:** Monitor and analyze network traffic.
5. **WAN Domain:**
    - **IT Professional:** Secure WAN connections.
    - **Security Practitioner:** Implement and monitor intrusion detection/prevention.
6. **Remote Access Domain:**
    - **IT Professional:** Control remote access.
    - **Security Practitioner:** Monitor and respond to remote access security.
7. **System/Application Domain:**
    - **IT Professional:** Manage access controls for critical applications.
    - **Security Practitioner:** Implement and monitor email security controls.

Which of the seven domains of a typical IT infrastructure requires personnel and executive management support outside of the IT or information systems security organizations?

- The LAN Domain requires support from executive management and personnel to enforce policies on personal device use within the LAN.

What does separation of duties mean?

- Separation of duties means dividing tasks and responsibilities among different individuals or roles to prevent a single point of failure or abuse of power.

How does separation of duties throughout an IT infrastructure mitigate risk for an organization?

- Separation of duties reduces the risk of unauthorized access, fraud, and errors by ensuring that critical tasks require multiple individuals for completion, preventing any single person from having excessive control.

How would you position a layered security approach with a layered security management approach for an IT infrastructure?

- A layered security approach involves implementing multiple security measures across different layers of the IT infrastructure. A layered security management approach ensures

that responsibilities and access are distributed across various roles, reducing the risk of a single compromise leading to a security breach.

If a system administrator had both the ID and password to a system, would that be a problem?

- If a system administrator has both the ID and password, it poses a significant security risk. Separation of duties dictates that no single individual should possess both credentials to prevent unauthorized access.

When using a layered security approaches to system administration, who would have the highest access privileges?

- In a layered security approach to system administration, the highest access privileges would be granted to a designated security administrator responsible for overseeing and enforcing security policies.

Who would review the organizations layered approach to security?

- The organization's security approach should be regularly reviewed by an independent security audit team or an internal security review board.

Why do you only want to refer to technical standards in a policy definition document?

- Technical standards provide specific, measurable criteria for implementing security controls. Referring to these standards in a policy ensures clarity and consistency in security implementation.

Why is it important to define guidelines in this layered security management policy?

- Guidelines provide instructions for overcoming implementation roadblocks and resolving disputes, ensuring a consistent and effective security posture.

Why is it important to define access control policies that limit or prevent exposing customer privacy data to employees?

- Defining access control policies that limit or prevent exposure of customer privacy data to employees is crucial to protect sensitive information and maintain regulatory compliance.

Explain why the seven domains of a typical IT infrastructure helps organizations align to separation of duties.

- The seven domains help organizations align to separation of duties by delineating specific responsibilities within each domain, preventing conflicts of interest and enhancing security.

Why is it important for an organization to have a policy definition for Business Continuity and Disaster Recovery?

- A policy definition for Business Continuity and Disaster Recovery is essential to ensure that the organization can continue critical operations and recover from disruptions.

Why is it important to prevent users from downloading and installing applications on organization owned laptops and desktop computers?

- Preventing users from downloading and installing applications helps maintain a secure and controlled computing environment, reducing the risk of malware and unauthorized software.

Separation of duties is best defined by policy definition. What is needed to ensure its success?

- To ensure the success of separation of duties, clear policies, ongoing training, periodic audits, and a robust incident response plan are needed. Regular reviews and updates to policies are also crucial.