Security Policy for Panther IT

Prepared by: Nicolas Dauria

Date: March 7, 2025

Table of Contents

Introduction

This security policy is designed to protect the organization's information assets from unauthorized access, disclosure, alteration, or destruction. It outlines the rules and procedures that all employees, contractors, and third-party users must follow to maintain the security and integrity of our systems and data.

Password Management Policy

Policy Statement:

This policy establishes the requirements for managing passwords to protect the confidentiality, integrity, and availability of the organization's information assets.

Scope:

This policy applies to all employees, contractors, and third-party users who have access to the organization's systems and data.

Password Requirements:

1. **Complexity:**
    a. Passwords must be at least 12 characters long.
    b. Passwords must include a combination of uppercase letters, lowercase letters, numbers, and special characters.
    c. Passwords should not contain easily guessable information such as names, dates, or common words.
2. **Expiration:**
    a. Passwords must be changed every 90 days.
    b. Users are encouraged to use password managers to generate and store complex passwords.
3. **Reuse:**
    a. Users cannot reuse the last 5 passwords.

4. **Account Lockout:**
    a. After 5 failed login attempts, the account will be locked for 30 minutes.
5. **Storage:**
    a. Passwords must be stored in a hashed and salted form.
    b. No plain text storage of passwords is allowed.
6. **User Responsibilities:**
    a. Users must not share their passwords with anyone.
    b. Users must report any suspected password compromise immediately.
    c. Users are responsible for the security of their passwords and must not write them down or store them insecurely.

Enforcement:

The IT department will enforce this policy through technical controls and regular auditing.

Exceptions:

Exceptions to this policy must be approved by the Chief Information Officer (CIO) and documented.

Review and Update:

This policy will be reviewed annually or whenever there is a significant change in the organization's security posture.

Incident Response Policy

Policy Statement:

This policy establishes the procedures for responding to security incidents to minimize their impact on the organization's operations and reputation.

Scope:

This policy applies to all employees, contractors, and third-party users who have access to the organization's systems and data.

Definition of a Security Incident:

A security incident is any event that threatens the confidentiality, integrity, or availability of the organization's information assets, including but not limited to:

- Unauthorized access to systems or data
- Malware infections
- Denial of service attacks
- Data breaches or leaks

Reporting Procedure:

All employees are required to report any suspected security incident to the IT department immediately via email or telephone.

Incident Response Team:

The Incident Response Team (IRT) consists of the following members:

- IT Manager (Team Leader)
- Network Administrator
- Security Officer
- Legal Advisor (as needed)

Response Phases:

1. **Preparation:**
    a. The IRT will develop and maintain an incident response plan.
    b. Regular training and drills will be conducted to ensure team readiness.
2. **Detection and Analysis:**
    a. The IRT will use monitoring tools to detect potential incidents.
    b. Upon detection, the IRT will analyze the incident to determine its scope and impact.
3. **Containment, Eradication, and Recovery:**
    a. The IRT will take immediate steps to contain the incident and prevent further damage.
    b. The cause of the incident will be identified and eradicated.
    c. Systems and data will be recovered to their normal state.
4. **Post-Incident Activity:**
    a. The IRT will conduct a thorough review of the incident to identify lessons learned.
    b. The incident response plan will be updated based on the review.

Communication Plan:

- The IRT will notify senior management and affected stakeholders as appropriate.

- Public communications will be handled by the Communications Department in coordination with the IRT.

Documentation:

- All incidents and response activities will be documented in detail.
- Incident reports will be maintained for future reference and auditing.

Review and Update:

This policy will be reviewed annually or whenever there is a significant change in the organization's security posture or in response to a major incident.

Conclusion

By adhering to this security policy, the organization can ensure that its information assets are protected, and that any security incidents are handled efficiently and effectively. It is the responsibility of all personnel to understand and comply with these policies to maintain a secure environment.