IMPLEMENTING CYBERSECURITY POLICIES AND ACCEPTABLE USE

August 2021

AGENDA

- Overview of Security Policies
- Policy vs Process vs Procedure
- Importance of Security Policies
- Policy Topics
- Creating Policies

EideBailly

INFORMATION SECURITY POLICY & ACCEPTABLE USE POLICY

INFORMATION SECURITY POLICIES

- A statement or collection of statements.
- Provide guidance regarding the security of the organization.
- Define the who, what, where and why to organization's overall security posture.

EideBailly

ACCEPTABLE USE POLICY

- **Set of rules when utilizing organizational assets or services.**
- **List of Do's & Don'ts**

The majority of employees (52%) in the US and UK see no security risk in sharing passwords and logins.

-IS Decisions

POLICY VS PROCESS VS PROCEDURE

DIFFERENCES

Policy:

The overall guidelines

Process:

The flows of activity

Procedure:

The detailed instructions of steps

During this unexpected remote work era, more than half (56%) of employees reportedly use their personal computer as their work device.

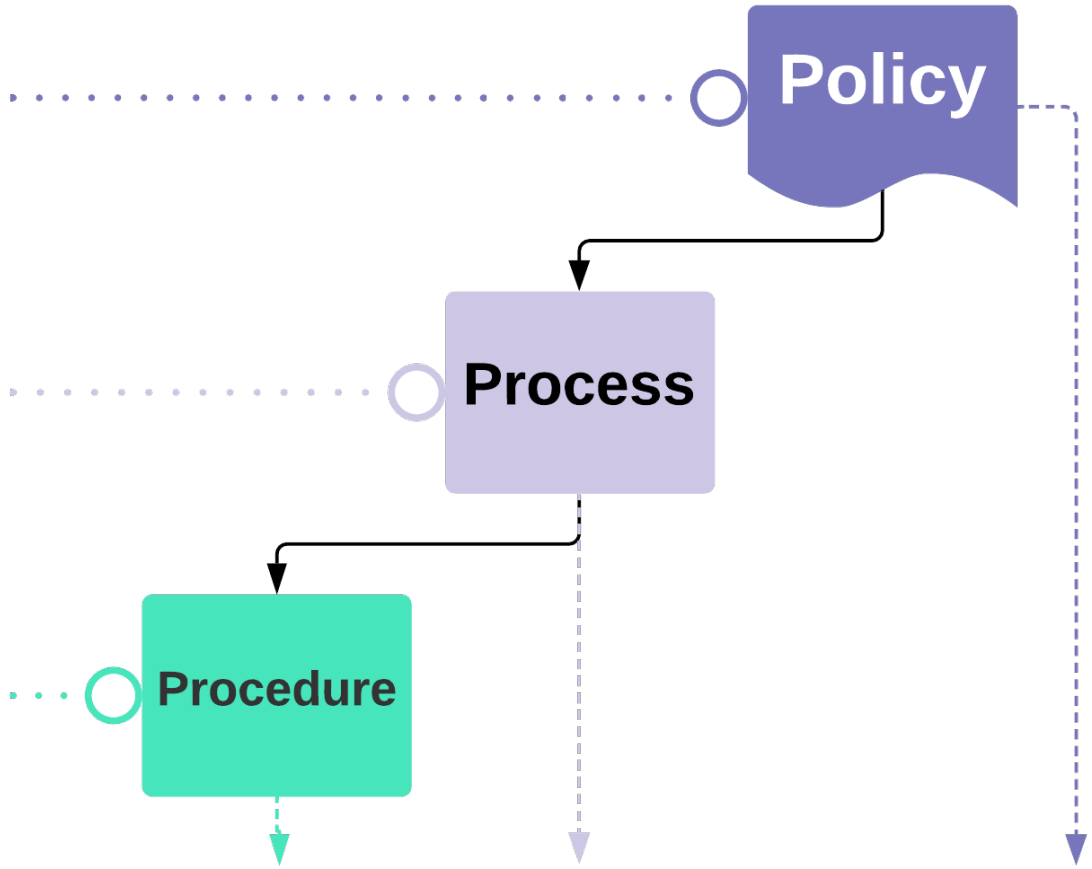
- Morphisec

TYPES OF SERVICE PROVIDERS

A policy is a rule or guideline that helps an organization govern a process.

A process is a series of high-level activities or tasks that produce a specific outcome.

A procedure is a sequence of steps or instructions to complete an activity within a process.



Procedure
Instructions on how to assign online training to this months new hires.

Security Awareness Process
Provides high-level guidance on different types of educate such as new user onboarding, working from home, secure coding, etc.

Security Awareness Policy
Outlines training and awareness requirements for all users.

EideBailly

IMPORTANCE OF CYBERSECURITY POLICIES

SET EXPECTATIONS

- **Allow organizations to commit to values and missions.**
- **Provide expectations to end users**
  - **Important of defining expectations for all users including contractors, volunteers, etc.**

If it's not documented…

…it's just a good idea.

EideBailly

ACCOUNTABILITY

- How users should conduct themselves
- Disciplinary actions
- Expectations from co-workers

EideBailly

ADDRESS THREATS

- Never-ending landscape
- Goal of policies and procedures it to address threats
- Implement strategies on how to mitigate threats
- Develop procedures to recover from threats

65%: Security pros who expect to be responding to a major breach in the next year

-Consumers in the Crosshairs (Black Hat USA)

EideBailly

LEGAL

- Due Diligence
- Defend against legal claims
- Legal actions against users who don't follow policy

COMPLIANCE

- **Depending on industry might require specific policy and procedures**

EideBailly

PROVIDE GUIDANCE

- **Above all provide guidance to workforce members.**

The goal when writing an organizational information security policy is to provide relevant direction and value to the individuals within an organization with regard to security.

EideBailly

POLICY TOPICS

NUMBER OF TOPICS

- The number of policies/ size of policy depends on several elements including organization size, compliance/ regulatory, maturity, and organizational structure.

Not all policies are relevant or necessary for all organizations.

EideBailly

POLICY TOPICS

- Acceptable Use
- Asset Management
- Disaster Recovery/ Backup
- Contingency/ Business Continuity
- BYOD
- Change Management
- Data Classification
- Retention
- Data Destruction
- Encryption
- Incident Response
- Access Mgmt.
- Network Security
- Vendor Mgmt.
- Password
- Physical
- Environmental
- Remote Access
- Software Development
- Software life cycle
- Wireless
- Clean Desk
- Patch Mgmt.
- Endpoint Management
- Email policy
- Internet Usage
- Audit and Logging
- Configuration Mgmt.
- Removeable Media
- Risk Management
- Security Awareness
- IT strategy/ Planning
- Vulnerability Mgmt.

EideBailly

NECESSARY TOPICS

- **No matter the size or maturity of an organization they should have the following essential policies/ plans in place.**
- **Incident Response**
  - Being prepared for an incident can significantly limit the amount of damage to the organization.
- **Disaster Recovery**
  - Having a plan to restore operations after an event
- **Contingency/ Business Continuity**
  - Having a plan to keep business operational during an event.
- **Acceptable Use**
  - Demonstrates due diligence
  - Provides guidance

Never expect users to know what is right or wrong, or what to do in an emergency.

EideBailly

CREATING POLICIES

POLICY OUTLINE

- Main Sections of Policy
- Overview
- Objectives/ Purpose
- Scope
- Roles & Responsibilities
- Body
- Exceptions
- Violations/ Sanctions
- References to Relevant Legislation
- Revision History

EideBailly

ACCEPTABLE USE

- Main Sections of Policy
- Overview
- Objectives/ Purpose
- Scope
- General Use/ Acceptable Use
- Unacceptable Use
- Email and Communications/ Internet Use
- Violations/ Sanctions
- References to Relevant Legislation
- Revision History

EideBailly

TIPS

- **Make policies easy to find/ reference for all users**
- **Make them easy to read/ understand**
  - **Limit legalize**
- **Engage employees to see what is/ isn't working**
- **Get executive buy-in**
- **Customize policies, don't just download one from the web**

EDUCATE/ TRAIN

- **Educate users throughout the year on policies and best practices**
- **Don't rely on the old review and sign during onboarding**

95% of cybersecurity breaches are due to human error.

IBM Cyber Security Intelligence Index Report.

EideBailly

EXAMPLES

EXAMPLE REFERENCES

- Check colleges/ universities
  - https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/security-policies/information-security-policy-examples
- SANS
  - https://www.sans.org/information-security-policy/
- Purple Security
  - https://purplesec.us/resources/cyber-security-policy-templates/

Remember using online templates is great, but must customize to your organization.

EideBailly

NEXT STEPS

NEXT STEPS

- Don’t Wait! Its never to late to implement policies and procedures
- There is Help

CPAs & BUSINESS ADVISORS

QUESTIONS?

THANK YOU

Dale Lozo

Cybersecurity Advisory Leader -

Cybersecurity Services

dlozo@eidebailly.com

916.570.1889

eidebailly.com