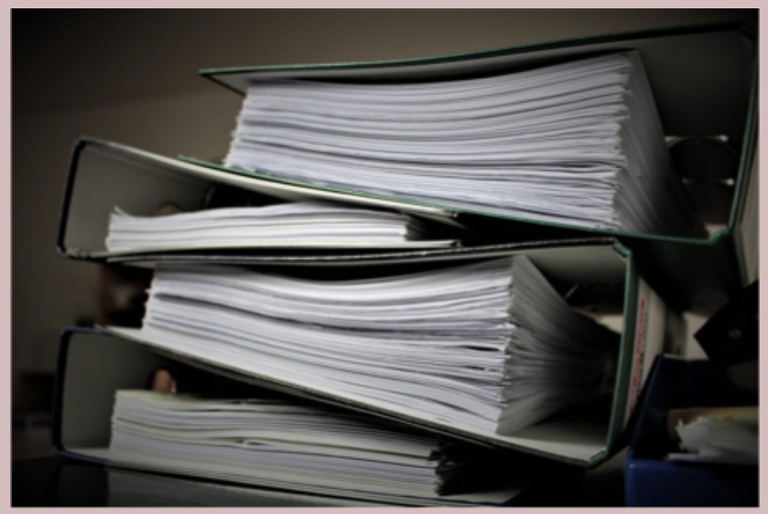
JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Policy Documents

Security Architecture & Tool Sets

Policy Documents

- Information Security Policy Framework
  - Policies
  - Standards
  - Procedures
  - Guidelines



JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Policies

- High-level statements of intent
- Contains broad statements about cybersecurity objectives in the company
- Framework to meet the business goals and to define roles, responsibilities, and terms used in other security documents

Policy Examples

- Information Security
- Acceptable Use
- Data Ownership
- Data Classification
- Data Retention
- Account Management
- Password

Who Approves the Policies?

- The CEO, CISO, CIO, or CSO will approve the policy for the organization
- Without management buy-in, the policy is a waste of your time and effort
- Top-down approach is most effective

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Standards

- Used to implement a policy
- Includes mandatory actions, steps, or rules needed to achieve cybersecurity
- Approved by a lower level than C-Suite, such as Director of Information Systems
- Standards can also exist in industry frameworks (COBIT, ITIL, etc.)

Procedures

- Detailed step-by-step instructions created for people to perform an action
- Actionable steps to create a consistent method for achieving a security objective
- Example:
  - The service desk has a procedure for how to create a new user's account
  - Encompass all the security related policies, standards, and guidelines for action by your front-line employees

Guidelines

- Not required actions, just recommended
- Flexible in nature to allow for exceptions and allowances during a unique situation
- Example:
  - The organization may create a guidelines showing users how to store data files in a cloud service and how to encrypt the files
  - These aren't required, but may be useful to the end user an can be changes quickly

Are the Rules Meant to Be Broken?

- Most of the time, the policies, standards, and procedures should be followed
- How do you get permission to break these established “rules”?
- Your information security framework should include the method for granting any necessary “exceptions”

JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Exceptions

- Specific approval to deviate from a policy, standard, procedure
- Approval authority is specified in policy
- Exception request includes:
  - Policy, standard, or procedure requiring exception
  - Reason for exception request
  - Scope and duration of exception
  - Risks associated
  - Description of compensating controls to lower risk