Policies and Procedures

by Sophia

WHAT'S COVERED

In this lesson, you will learn about the difference between policies, procedures, and regulations, examine some examples, and get some tips for distributing policies and procedures to the people they affect.

Specifically, this lesson will cover the following:

1. Policies, Processes, Procedures, and Regulations

Every company should have written policies and procedures to effectively manage their computer networks. Earlier in this unit, you learned about some commonly implemented security policies; now we’ll enlarge the scope of that discussion.

1a. Defining the Terms

Policies, processes, procedures, and regulations all have different purposes, so let’s start by clarifying those terms.

A **regulation** is a rule imposed by outside sources, such as governmental agencies or professional organizations. They're usually completely rigid and immutable. Regulations dictate outcomes; they don't usually specify how something gets done. For example, a company that has servers that store customer credit card data is bound by the Payment Card Industry Data Security Standards (PCI DSS), and it is up to the IT professionals managing those servers to ensure that their policies meet those standards.

A **policy** is a general rule or guideline that explains the plan for achieving or preventing something. For example, there might be a company policy that states that the company must implement certain mandates from the PCI DSS regulations to protect and secure the servers that store customer payment information. A policy explains *what* should happen, and *why* it should happen, but it doesn't explain *how* it should happen. A policy is different from a **guideline**, which is a general recommendation that should mandatorily be followed in all situations.

THINK ABOUT IT

One of the most important aspects of any policy is it's given high-level management support. IT security policies should have the approval of the highest-ranking security or IT officer within the company. This is because a policy cannot be effective if everyone in positions of power doesn't agree that it is mandatory.

A **process** is a high-level checklist or set of steps that outlines *how* something should happen. For our server example, the process might be for administrators to use a certain type of security for customer credit card data at rest (that is, stored on the server), and a certain type of encryption for the data when it is in transit. A process might further specify how often to verify that the protection is in force.

A **procedure** is the next logical step arising from a policy. It explains the how by providing detailed instructions for completing a specific task in support of a policy. Procedures commonly provide step-by-step instructions or checklists and mention who is responsible for making sure the work gets done. In our example, the procedure would specify exactly what should happen—step by step—to implement, verify, and manage the security measures, who is responsible, and what should be done when a breach occurs.

BIG IDEA

It is important that a company has detailed procedures that define the appropriate course of action when there is a security breach. And all network administrators absolutely need to be thoroughly trained on all policies and procedures—no weak links. When a breach occurs, employees will be shaken up from the stress, and being familiar with the step-by-step routine to follow will help them manage. You don't want someone under stress to be trying to make big decisions independently on-the-fly.

As an entry-level network tech, you won't be called upon to create policies and procedures; you'll be handed them and tasked with implementing them. As you progress upward in your career path, however, your duties may include this task.

TERMS TO KNOW

Regulation

A rule imposed by an outside source such as a governmental agency or a professional organization.

Policy

A general rule or guideline that explains the plan for achieving or preventing something.

Guideline

A general recommendation that is not mandatory to follow.

Process

A high-level checklist or set of steps that outlines how something should happen.

Procedure

A detailed instruction for completing a specific task in support of a policy.

1b. More About Regulations

Generally speaking, most IT regulations center around implementing the CIA triad described in the table below.

Confidentiality	Only authorized users have access to the data.
Integrity	The data is accurate and complete.
Availability	Authorized users have access to the data when access is needed.

IN CONTEXT

The question is: what does *confidentiality* mean to your organization, given its industry sector and location? What do *integrity* and *availability* mean? Not just in theoretical terms, but in practical application. How much of each quality is enough?

The answer is that it depends on multiple factors. Different regulations exist for different types of organizations, depending on whether they're corporate, nonprofit, scientific, educational, legal, governmental, and so on. There are also differences based on where the organization is located. U.S. governmental regulations vary by county and state. Federal regulations are piled on top of those. And many other countries have multiple regulatory bodies as well. As a result, it is not always clear which regulations apply to a situation, so those decisions are often left to executive-level IT professionals and corporate lawyers.

➦ EXAMPLE The Sarbanes-Oxley Act of 2002 (SOX) is a regulation system imposed on all publicly traded companies in the United States. Its main goal was to ensure corporate responsibility and sound accounting practices. Although that may not sound like it would have much of an effect on your IT department, it does, because a lot of the provisions in this act target the retention and protection of data. Something as innocent sounding as deleting old emails could get you in trouble. If any of them could've remotely had a material impact on the company's financial disclosures, deleting them could actually be breaking the law. All good to know, so be aware, and be careful!

One of the most commonly applied IT-related regulations is the ISO/IEC 27002 standard for information security. Its official title is *Information technology — Security techniques — Code of practice for information security controls*. Although it's beyond our scope to get into the details of this standard, know that the following items are among the topics it covers:

- Risk assessment
- Security policy
- Organization of information security
- Asset management
- Human-resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business-continuity management
- Compliance

So, what do you take with you from this? Your mission is clear. Know the regulations your company is expected to comply with, and make sure your IT policies and procedures are totally in line with any regulations so it's easy for you to comply with them. No sense getting hauled off to jail because you didn't archive an email, right?

1c. More About Policies

A policy can arise from either a company's necessity to comply with a regulation or its desire to achieve a certain outcome. Either way, the basic structure of a policy is fairly straightforward. A policy should include the following:

- What outcome the policy is intended to achieve
- How that outcome is aligned with the company's underlying values or principles
- The strategies to be implemented to achieve the outcome
- The actions to be taken (in a broad sense, not at the step-by-step level)
- How the policy's success will be measured

1d. More About Procedures

For every policy on your network, there should be a credible related procedure that clearly dictates the steps to take in order to fulfill it. And you know that policies and procedures are as unique as the wide array of companies and organizations that create and employ them. But all this doesn't mean you can't borrow good ideas and plans from others and tweak them a bit to meet your requirements. An example of a network access policy is a time-of-day restriction on logging in to the network.

The following are some examples of details that a procedure might include:

- Disciplinary action to be taken if a policy is broken
- What to do during an audit
- How issues are reported to management
- What to do when someone has locked themselves out of their account

- How to properly install or remove software on servers
- What to do if files on the servers suddenly appear to be “missing” or altered
- How to respond when a network computer has a virus
- Actions to take if it appears that a hacker has broken into the network
- Actions to take if there is a physical emergency like a fire or flood

2. Types of Policies and Procedures

Next, let’s examine a few different types of network-related policies and procedures you may encounter—or may even be asked to help draft.

2a. Employee Access Management

HR will typically make its own policies for employee onboarding and offboarding, but IT must be involved in how HR policies are implemented in network and computer systems to ensure data is stored securely (and in accordance with any applicable regulations). Some topics that may require IT management include the following:

- Creating accounts for new employees
- Training new employees to use IT systems and follow security procedures
- Authorizing employee accounts for an appropriate set of permissions
- Disabling or deleting the accounts of former employees, including the timing of such
- Archiving or deleting the data files of former employees

2b. Change Management

When an organization makes changes (as will be covered later in this course), the employees tasked with implementing the change follow policies and procedures designed to ensure a consistent approach and to leave no important tasks undone.

Some of the topics for which an organization might want change management policies and procedures include the following:

- Disposal of network equipment
- Use of recording equipment
- How passwords are managed (length and complexity required and how often they need to be changed)
- Types of security hardware in place
- How often to save backups and take other fault-tolerant measures
- What to do with user accounts after an employee leaves the company

2c. Security Management

Many IT policies and procedures are designed to prevent end users from doing things that compromise network or workstation security. An IT department may create such policies proactively, but many policies get written because someone did something that caused a problem.

Here are a few examples of IT policies and procedures that a department might create to help strengthen its security posture. Some of these may also involve **agreements**, which are statements that employees are required to sign to indicate that they have been informed of them and they agree to comply with them as a condition for their employment.

Clean-desk policies	These policies are designed to prevent users from leaving sensitive documents on unattended desks.
Network access (who, what, and how)	These policies control which users can access which portions of the network. They should be designed around job responsibilities.
Acceptable-use policies (AUP)	These policies should be as comprehensive as possible and should outline every action that is allowed in addition to those that are not allowed. They should also specify which devices are allowed, which websites are allowed, and the proper use of company equipment.
Consent to monitoring	These policies are designed to constantly remind users that their activities are subject to monitoring as they are using company equipment and as such they should have no expectation of privacy.
Privileged user agreement	Whenever a user is given some right normally possessed by the administrator, they thus possess a privileged user account. In this agreement, they agree to use these rights responsibly.
Password policy	This policy defines the requirements for all passwords, including length, complexity, and age.
Licensing restrictions	These restrictions define the procedures used to ensure that all software license agreements are not violated.
International export controls	In accordance with all agreements between countries in which the organization does business, all allowable export destinations and import sources are defined.
Data loss prevention	This policy defines all procedures for preventing the egress of sensitive data from the network and may include references to the use of Data Loss Prevention (DLP) software.
Remote access policies	These policies define the requirements for all remote access connections to the enterprise. This may cover VPN, dial-up, and wireless access methods.
Incident response policies	These policies define a scripted and repeatable process for responding to incidents and responsibilities of various roles in the network in this process.
Nondisclosure agreement (NDA)	All scenarios in which contractors and other third parties must execute a nondisclosure agreement are defined.

System life cycle	The steps in the asset life cycle are defined, including acquisition, implementation, maintenance, and decommissioning. It specifies certain due-diligence activities to be performed in each phase.
Asset disposal:	This is usually a subset of the system life cycle and prescribes methods of ensuring that sensitive data is removed from devices before disposal.

TERM TO KNOW

Agreement

A statement signed to indicate that the signer has been informed and agrees to comply.

2d. Distributing Policies and Procedures

A policy or procedure is of limited use if it's not made available to the people who must follow it. When deciding how to disseminate (that is, distribute) policies and procedures to employees, consider the following factors:

- Reach: In what formats and media are the affected people most likely to see this information? How can we ensure maximum reach—not only in who receives it but in who actually reads it?
- Security: If the policy or procedure is sensitive in nature or contains information we would prefer the public not have, how do we restrict its reach appropriately?

Distributing the information via multiple platforms or formats may be helpful in maximizing reach. For example, if there is a new password policy that will require all employees to change their passwords by a certain date, you might post a notice about it in public areas and break rooms, send an email about it to every employee, and display a splash screen message reminding employees to change their passwords when they log in. In contrast, if the policy is narrow in the scope of people it affects, or sensitive in nature, you might discuss it in a staff meeting where only those people are in attendance, and you might follow up by sending attendees a copy of the policy via email.

Making sure that people actually read the policy is a different matter and may require extra effort. For example, you might request a read receipt on an email containing the policy, or you might require affected employees to sign an agreement stating they have read and understood it.

SUMMARY

In this lesson, you learned about the difference between **policies, processes, procedures, and regulations**. You learned about **defining terms**, **more about regulations**, **more about policies**, and **more about procedures**. You also learned about types of policies and procedures. These included **employee access management**, **change management**, **security management**, and **distributing policies and procedures**.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor**

Companion Site (wiley.com)

TERMS TO KNOW

Agreement

A statement signed to indicate that the signer has been informed and agrees to comply.

Guideline

A general recommendation that is not mandatory to follow.

Policy

A general rule or guideline that explains the plan for achieving or preventing something.

Procedure

A detailed instruction for completing a specific task in support of a policy.

Process

A high-level checklist or set of steps that outlines how something should happen.

Regulation

A rule imposed by an outside source such as a governmental agency or a professional organization.