Security Management Concepts

**Policies**

Security policies may consist of different types, depending upon the specific need for the policy.

* Organizational or program policy: This policy is issued by a senior management individual, who creates the authority and scope for the security program. The purpose of the program is described, and the assigned responsibility is defined for carrying out the information security mission. The goals of confidentiality, integrity, and availability are addressed in the policy. States how an organisation should be carried out
* Functional, issue-specific policies: While the organizational security policies are broad in scope, the functional or issue-specific policies address areas of particular security concern requiring clarification.
* System-specific policies: Areas where it is desired to have clearer direction or greater control for a specific technical or operational area may have more detailed policies.

Other types of policies may include

* Advisory policy

The job of an advisory policy is to ensure that all employees know the consequences of certain behavior and actions. Here’s an example advisory policy:

Illegal copying: Employees should never download or install any commercial software, shareware, or freeware onto any network drives or disks unless they have written permission from the network administrator. Be prepared to be held accountable for your actions, including the loss of network privileges, written reprimand, probation, or employment termination if the Rules of Appropriate Use are violated.

* Informative policy

This type of policy isn’t designed with enforcement in mind; it is developed for education. Its goal is to inform and enlighten employees. The following is an example informative policy:

In partnership with Human Resources, the employee ombudsman's job is to serve as an advocate for all employees, providing mediation between employees and management. This job is to help investigate complaints and mediate fair settlements when a third party is requested.

* Regulatory policy

These policies are used to make certain that the organization complies with local, state, and federal laws. An example regulatory policy might state:

Because of recent changes to Texas State law, The Company will now retain records of employee inventions and patents for 10 years; all email messages and any backup of such email associated with patents and inventions will be stored for one year.

The more detailed and issue specific the written policy is, the higher the likelihood is that the policy will require more frequent changes.

Policy Checklist

* set out the aim of the policy
* explain why the policy was developed
* list who the policy applies to
* set out what is acceptable or unacceptable behaviour
* set out the consequences of not complying with the policy
* provide a date when the policy was developed or updated.

Common workplace policies

* code of conduct
* recruitment policy
* internet and email policy
* mobile phone policy
* non-smoking policy
* drug and alcohol policy
* health and safety policy
* anti-discrimination and harassment policy
* grievance handling policy
* discipline and termination policy
* using social media

**Code of conduct**

* Attendance and absence
* Employee behaviour
* Company values
* Break and mealtime policies
* Confidentiality
* Use of company property
* Use of social media
* Plagiarism
* Travel policies
* Conflicts of interest
* Client interaction
* Dress code
* Reporting misconduct

**Recruitment Policy**

* Internal and external hiring preferences
* Equal opportunity and anti-discrimination
* Job description and advertisement templates
* Selection process and timeframe
* How to review resumes and cover letters
* The expected amount of short-listed applicants
* How to check references
* How to select a suitable candidate and offer the job

**Internet and Email Policy**

* Internet access rules
* Appropriate online usage
* Controls on misuse of the internet
* Restrictions on web browsing
* A security protocol for online data
* Download rules
* Social networking rules
* Work email usage rules
* How to frame emails to colleagues
* Work email usage at home or outside the office

**Mobile phone policy**

* When you can use your personal mobile phone
* Where you can keep your personal mobile phone during office hours
* Rules surrounding personal phone calls
* How to use your work mobile phone
* What is and isn't acceptable use for you work mobile phone

**Smoking policy**

* Whether smoking is allowed
* Designated smoking areas
* Smoking breaks
* Smoking off-site

**Alcohol and drugs policy**

* A company's tolerance to drug and alcohol use
* Drug testing rules
* Alcohol use rules (i.e., Friday drinks)
* Procedure for dealing with intoxicated individuals

**Health and safety policy**

* Risk assessment
* Employee safety training
* First aid information
* Equipment maintenance
* Safe handling of materials and substances
* Supervision rules
* Delegation of authority
* Accident training
* Physical and mental health information
* Monitoring hazards
* Emergency procedures

**Anti-discrimination and harrassment policy**

* Procedure for employee complaints
* Education and training for employees
* Provide a clear definition of discrimination and harassment
* Guidelines for dealing with discrimination and harassment
* How management expects to respond to complaints
* Confidentiality information

**Grievance handling policy**

* Procedure for submitting a formal grievance
* Company policy regarding response
* Procedure for investigating the grievance
* Time frame
* Confidentiality
* Possible outcomes
* Appeal information

**Discipline and termination policy**

* Procedure for dealing with incidents that go against company policy
* How a company responds to rule breaks
* Your rights to appeal discipline
* Procedure for an investigation into incidents
* Reasons for termination
* Pre-termination procedure
* How to tell an employee they have been let go
* Post-termination procedure

Good policy strikes a balance and is both relevant and understandable. If a policy is too generic, no one will care what it says because it doesn’t apply to the company. If a policy is too complex, no one will read it—or understand, it if they did.

**Standards**

Whereas policies define what an organization needs, standards take this a step further and define the requirements. Standards provide the agreements that provide interoperability within the organization through the use of common protocols. Standards simplify the operation of the security controls within the company and increase efficiency.

Examples of Standards

**ISO 27001 and ISO 27002**

Created by the International Organization for Standardization (ISO), ISO 27001 and ISO 27002 certifications are considered the international standard for validating a cybersecurity program — internally and across third parties. With an ISO certification, companies can demonstrate to the board, customers, partners, and shareholders that they are doing the right things to manage cyber risk. Likewise, if a vendor is ISO 27001/2 certified it’s a good indicator (although not the only one) that they have mature cybersecurity practices and controls in place.

The downside is that the process requires time and resources; organizations should only proceed if there is a true benefit, such as the ability to win new business. The certification is also a point-in-time exercise and could miss evolving risks that continuous monitoring can detect.

ISO standards provide frameworks, guidelines, or requirements that can be followed to help achieve their intended purpose.

**NERC-CIP**

Introduced to mitigate the rise in attacks on U.S. critical infrastructure and growing third-party risk, the North American Electric Reliability Corporation - Critical Infrastructure Protection (NERC CIP) is a set of cybersecurity standards designed to help those in the utility and power sector reduce cyber risk and ensure the reliability of bulk electric systems.

The framework requires impacted organizations to identify and mitigate cyber risks in their supply chain. NERC-SIP stipulates a range of controls including categorizing systems and critical assets, training personnel, incident response and planning, recovery plans for critical cyber assets, vulnerability assessments, and more.

**GDPR**

The General Data Protection Regulation (GDPR) was adopted in 2016 to strengthen data protection procedures and practices for citizens of the European Union (EU). The GDPR impacts all organizations that are established in the EU or any business that collects and stores the private data of EU citizens — including U.S. businesses.

The framework includes 99 articles pertaining to a company’s compliance responsibilities including a consumer’s data access rights, data protection policies and procedures, data breach notification requirements (companies must notify their national regulator within 72 hours of breach discovery), and more.

Fines for non-compliance are high; up to €20,000,000 or 4% of global revenue, and the EU is not shy about enforcing them.

**Baselines**

Baselines provide descriptions of how to implement security packages to ensure that these implementations are consistent throughout the organization. Different software packages, hardware platforms, and networks have different methods of ensuring security. There are many different options and settings that must be determined to provide the desired protection. An analysis of the available configuration settings and subsequent settings desired, forms the basis for future, consistent implementation of the standard.

The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

A baseline is a minimum level of security that a system, network, or device must adhere to. Baselines are usually mapped to industry standards. As an example, an organization might specify that all computer systems comply with a minimum Trusted Computer System Evaluation Criteria (TCSEC) C2 standard. TCSEC standards are discussed in detail in Chapter 5, "System Architecture and Models."

**Guidelines**

Guidelines are discretionary or optional controls used to enable individuals to make judgments with respect to security actions. A good exercise is to replace the word *guideline* with the word *optional.*

Guidelines are also those recommendations, best practices, and templates provided by other organizations such as the Control Objectives for Information and related Technology (COBIT), the Capability Maturity Model (CMM), ISO 17799, and British Standard 7799, security configuration recommendations such as those from the National Institute of Standards and Technology (NIST) or the National Security Agency (NSA), organizational guidelines, or other governmental guidelines.

A guideline points to a statement in a policy or procedure by which to determine a course of action. It’s a recommendation or suggestion of how things should be done. It is meant to be flexible so it can be customized for individual situations.

**Procedures**

Procedures are step-by-step instructions in support of the policies, standards, guidelines, and baselines. The procedure indicates how the policy will be implemented and who does what to accomplish the tasks. The procedure provides clarity and a common understanding to the operation required to effectively support the policy on a consistent basis.