

Network Security Policy Design and Implementation

Module 04



Network Security Policy Design and Implementation

Module 04



Certified Network Defender

Module 04: Network Security Policy Design and Implementation

Exam 312-38



Module Objectives

C|ND
Certified Network Defender

- Understanding the security policy
- Discussing the need of security policies
- Describing the hierarchy of a security policy
- Describing the characteristics of a good security policy
- Describing the typical content in a security policy
- Understanding the policy statement
- Describing the steps for creating and implementing a security policy

- Understanding how to design a security policy
- Understand the implementation of a security policy
- Describe the various types of a security policy
- Discussing the design of various security policies
- Understand the need to enforce and train on the security policy
- Discussing various information security related standards, laws and acts



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

This module focused on designing and implementing security policies for your organization. The module explains the need and importance of using security policies. It describes the content and the steps involved in designing and implementing security policies. The module also describes the considerations required when designing various security policies, which will guide you on an effective policy design and implementation.

What is a Security Policy

Need for a Security Policy

- A security policy is a **well documented** set of plans, processes, procedures, standards, and guidelines required to establish an ideal information security status for organizations
- The security policy is an **integral** part of an information security management program for any organization

- To provide a consistent application of **security principles** throughout the organization
- To ensure **information security standards** compliance
- To limit the organization's **exposure** to external information threats
- To outline senior management's commitment in maintaining a **secure environment**

- To provide **legal protection**
- To quickly respond to security incidents
- To reduce the **impact** of a security incident
- To minimize the risk of a **data breach**
- To enhance the overall data and network security

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A security policy is a high-level document or set of documents describing the security controls to implement in order to protect the company. It maintains confidentiality, availability, integrity, and asset values. Security policies form the foundation of a security infrastructure. Without them, it is impossible to protect the company from possible lawsuits, lost revenue, and bad publicity, not to mention basic security attacks.

Policies are not technology specific and accomplish three things:

- They reduce or eliminate the legal liability to employees and third parties.
- They protect confidential and proprietary information from theft, misuse, unauthorized disclosure, or modification.
- They prevent computing resource waste.

A security policy comprises objectives, rules for behavior and requirements to secure the organization's network and computer systems. Security policies act as a connecting medium between the objectives and security requirements, as well as to help users, staff, and managers protect technology and information assets. The policy provides a baseline to acquire, configure, and audit computer systems and networks.

A security policy defines a set of security tools for preventing attacks on the entire network in order to keep malicious users away from the organization and provide control over perilous users within the organization.

The security policy should ensure confidentiality, privacy, integrity and availability of the company's assets.

The Need of a Security Policy

- The number of devices used across an organization is increasing and pushing the growth of the information being transferred, networks used and storage space. This growth also increases the likelihood of security threats originating from various vulnerabilities. A security policy enables the organization to combat such threats and protect them from losing information.
- It provides a consistent application of security principles throughout the company to ensure everything functions in a secure manner. Security policies ensure compliance to information security industry standards, building a trust based relationship with clients. It helps limit a company's exposure to external information threats, while it indicates senior management's commitment to maintaining a secure environment.
- It provides legal protection by defining what rules to use on the network, how to handle confidential information and the proper use of encryption, reducing liability and exposure of the organization's data.
- Security policies reduce the risk of damaging security incidents by identifying the vulnerabilities and predicting the threats before they happen.
- They also comprise procedures and techniques to minimize the risk of an organization's data leak or loss by adopting backup and recovery options.

Advantages of Security Policies

- **Enhanced data and network security:** Organizations implement a policy based on their network which enhances their data security. It facilitates protection when sharing information between other systems on a network.
- **Risk mitigation:** The risks involved from external sources is reduced by implementing and deploying security policy. If an employee follows the policy exactly, it becomes nearly impossible for an organization to lose its data and resources.
- **Monitored and controlled device usage and data transfers:** Even though policies are being implemented thoroughly by employees, administrators should regularly monitor the traffic and external devices used in the system. Monitoring and auditing of the incoming and outgoing traffic should always be done on regular intervals.
- **Better network performance:** When security policies are implemented correctly and the network is monitored regularly, no unnecessary loads exist. The data transmission speed in the system increases, providing an overall performance enhancement.
- **Quick response to issues and lower downtime:** Policy deployment and implementation enables faster response rates when resolving network issues.
- **Reduction in Management stress levels:** The role of management becomes less stressful when policies are implemented. Every policy must be followed by every employee in the

organization. If this occurs, management will not need to worry about any malicious attacks on the network.

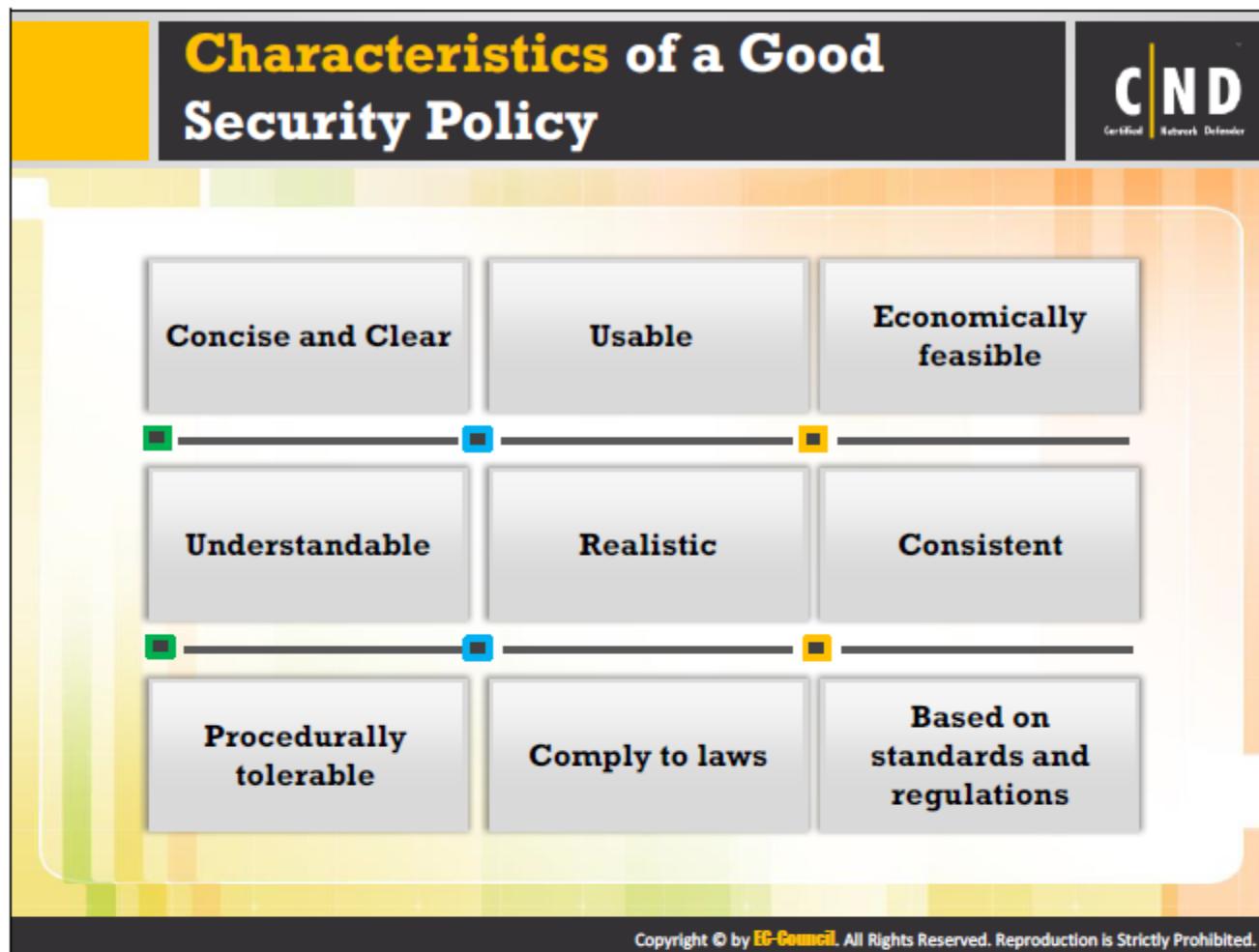
- **Reduced costs:** If employees follow the policies correctly, the cost of each intrusion is reduced as well as the impact on an organization.



Organizations use different terminologies while drafting a security policy. The implementation of these terminologies depends on the severity and the level of the hierarchy they are a part of.

- **Laws:** Placed at the top of the hierarchy. These policies set which laws every individual in the organization must follow. Organizations have the authority to take action against any employee who fails to follow these laws.
- **Regulations:** A regulation is the second component in the hierarchy. Regulations ensure employees follow the law. It is a set of guidelines that depends on the laws of the security policy. Organizations can set either government or social regulations. Social regulations also involve third party regulations.
- **Policies:** With the help of policies, an organization establishes the legal and internal requirements of their network security. Management documents, reviews, and approves these policies. A policy consists of different disciplines and procedures. The documentation of a policy defines the security architecture for the organization. The implementation of these policies set the standard for the organization and improves risk management.
- **Standards:** Standards specify the method of policy implementation. Standards are derived from policies and must be implemented by the organization. They are both voluntary and/or mandatory depending on company policies. They bring consistency to the business functionality. It is not feasible to change the company standards after a certain interval. They also involve security controls related to technology, hardware and software.

- **Practices:** Practices define the strategy to implement an organization's policies and standards. Practices help the organization overcome threats. An organization instructs the employees to execute the practices by deploying, evaluating and assessing certain tasks.
- **Procedures:** A procedure is a set of sequential steps leading up to a process satisfying organizational policies. The implementation of these procedures requires an approval from senior management. Procedures work based on the following questions:
 - Who will do what?
 - What steps will they take?
 - Which forms or documents will they use?Procedures are made up of checklists, instructions and/or flowcharts.
- **Guidelines:** Guidelines are an optional item providing advice which is normally not mandatory to follow. It serves as a reference when there are no specific standards. Guidelines act as a recommendation and organizations should not ignore them. Implementing guidelines mitigate risk. It is advisable to keep guidelines updated as the business requirements change.



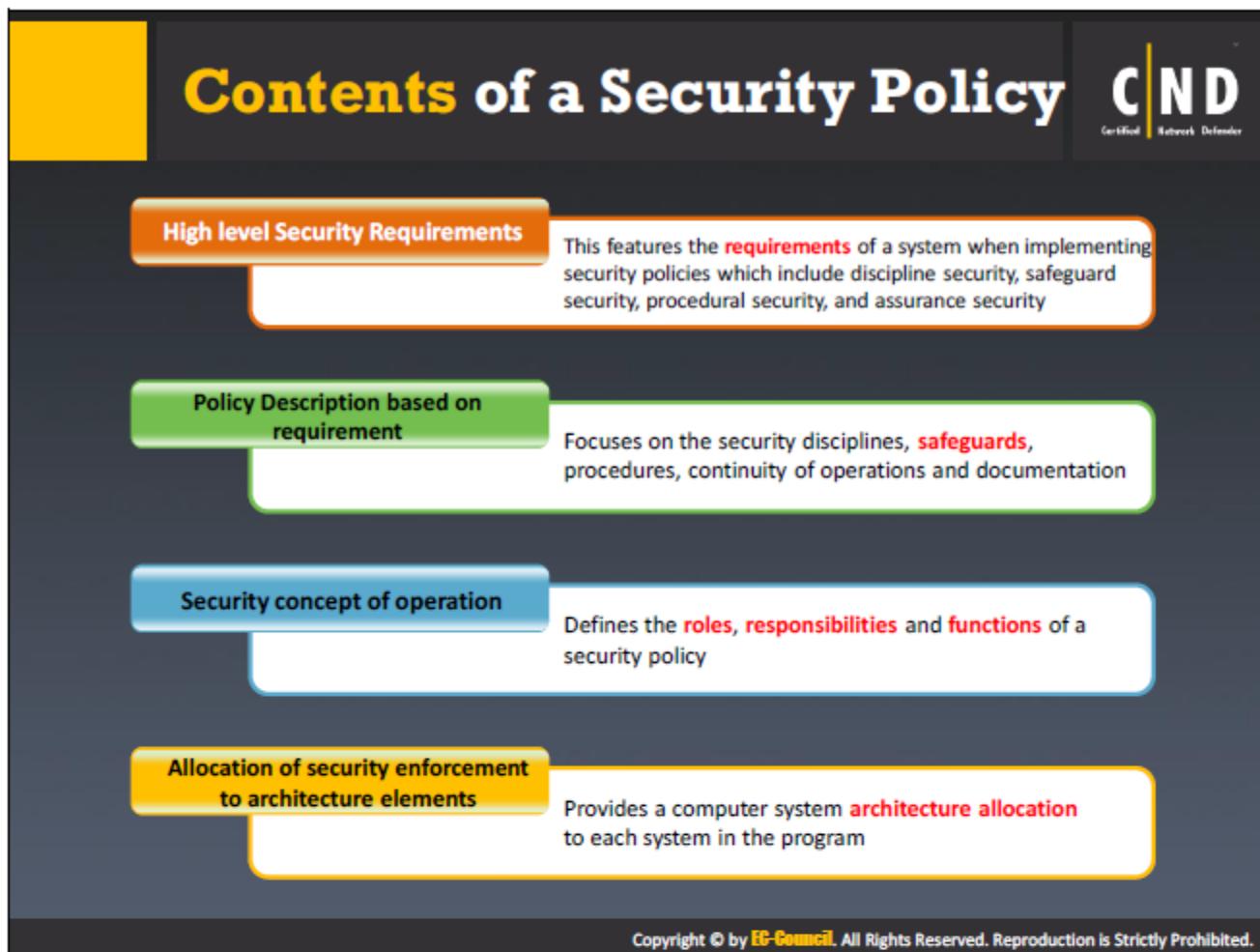
A good security policy has the following features:

1. **Concise and clear:** A security policy needs to be concise and clear. When they are, they are very easy to deploy in the infrastructure. Complex policies become hard to understand and employees may not implement them as a result.
2. **Usable:** Policies must be written and designed so they can be used easily across various sections of the organization. Well-written policies are easy to manage and implement.
3. **Economically feasible:** Organizations must implement policies which are economical and enhance the security of the organization.
4. **Understandable:** Policies must be easy to understand and follow.
5. **Realistic:** Policies must be practical based on reality. Using fictional items in a policy will only hurt the organization.
6. **Consistent:** Organizations must have consistency when implementing their policies.
7. **Procedurally tolerable:** When implementing procedures policies they have to be employer-employee friendly.
8. **Comply with cyber and legal laws, standards, rules and regulations:** Any policy that is implemented must comply with all rules and regulations regarding cyber laws.

Key Elements of Security Policy

Key elements of a good security policy are:

- **Clear Communication:** Pay close attention to any communication gaps. Communication must be clear when designing a security policy. A communication gap leads to undesirable results. A set of policies may be created which are not feasible for the users or the network. Keep communication channels clear.
- **Brief and Clear Information:** Any information provided to developers regarding the creation of the network policy must be clear and understandable. If not the approach to the security of the network will not be as expected.
- **Defined Scope and Applicability:** The scope identifies the items that must be covered, hidden, protected or public and how to secure them. The network policy addresses a wide range of issues from physical security to personal security.
- **Enforceable by Law:** The security policy must be enforceable by law and penalties imposed if there is policy breach. Penalties for a violation must be addressed when the policy is created.
- **Recognizes Areas of Responsibility:** The network policy must recognize various responsibilities for employees, the organization and third parties.
- **Sufficient Guidance:** A good network policy must have proper references to other policies, which help guide and redefine the scope and the objectives of the policy.



The four parts of a security policy implementation are:

1. Security requirements
2. Policy description
3. Security concept of operation
4. Architecture element allocation

Security Requirements

This statement features the requirements for a system to implement security policies. There are four types of security requirements:

- Discipline Security
- Safeguard Security
- Procedural Security
- Assurance Security
- **Discipline Security Requirements**

It involves security policies stating what actions are taken on various components needing to be secured. For example, computer security, operations security, network security, personnel security, physical security, etc.

- **Safeguard Security Requirements**

It involves security policies stating the protective measures required. For example, protective measures for access control, malware protection, audit, availability, confidentiality, integrity, cryptography, identification, and authentication.

- **Procedural Security Requirements**

It involves security policies containing access policies, accountability, continuity of operations, and documentation.

- **Assurance Security Requirements**

It involves security policies used with the compliance of various standards, certifications, and accreditations.

Policy Description

This statement mainly focuses on the security disciplines, safeguards, procedures, continuity of operations, and documentation. Each subset of this policy describes how the system's architecture elements will enforce security.

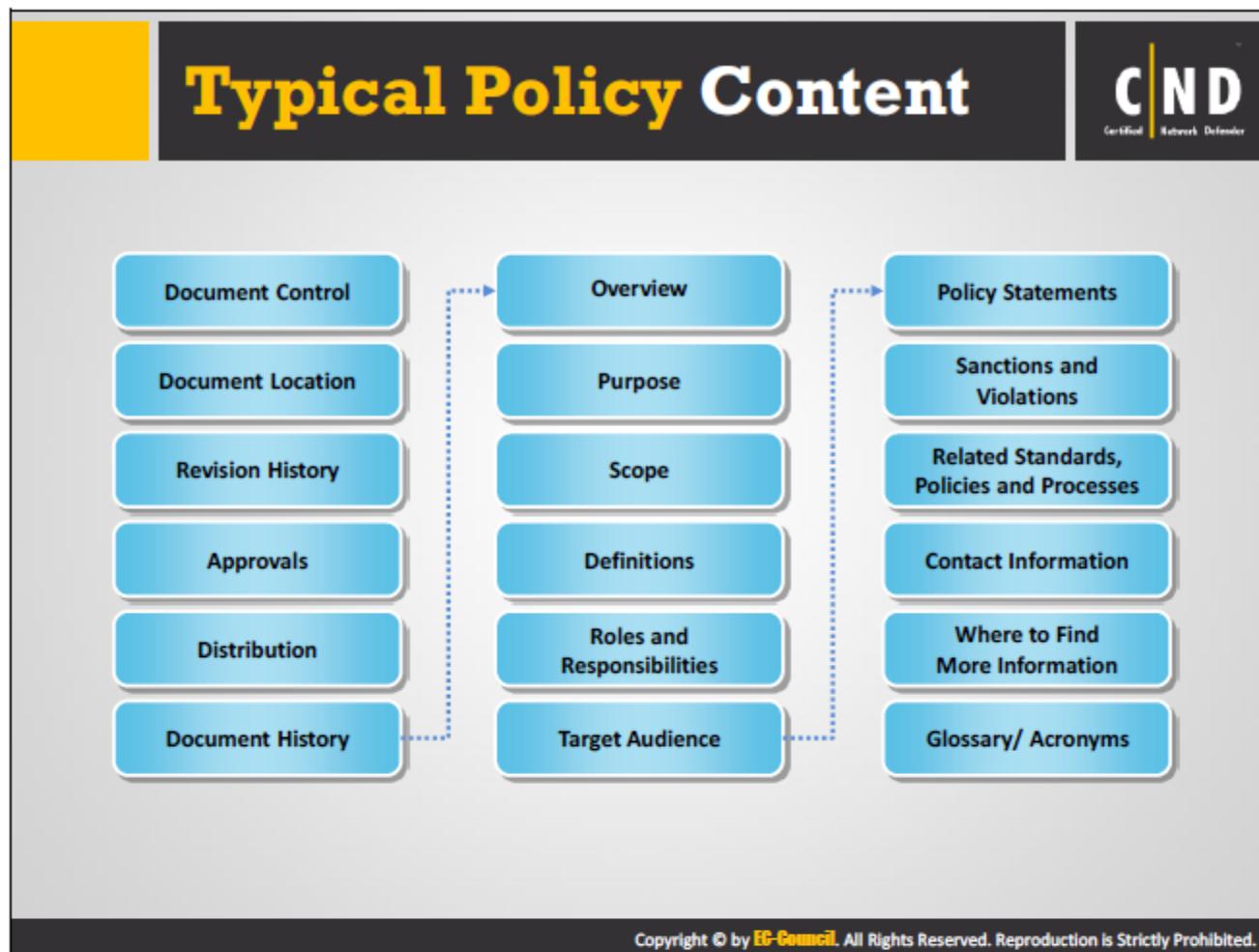
Concept of Operation

This concept defines the roles, responsibilities, and functions of a security policy.

It focuses on the mission, communications, encryption, user and maintenance rules, idle time management, privately owned versus public domain, shareware software rules and a virus protection policy.

Architecture Element Allocation

This policy provides a computer system architecture allocation to each system in the program.



The important policy sections are:

- **Overview** of a security policy provides background information that the policy needs to address.
- **Purpose** is a detailed explanation of why the policy needs to be framed.
- **The scope** includes information about who and what the policy covers.
- **Definitions** are the terms used in the policy.
- **Roles and Responsibilities** are defined for the employees and management.
- **Target Audience** is the users and clients the policy is being created for.
- **Policies** are statements on each aspect of the policy.
- **Sanctions and Violations** defines the allow/deny process clients and users must follow.
- **Contact Information** includes information about who to contact in case there is a policy sanction and/or violation.
- **Version** number ensures all changes/updates to the policy are tracked correctly.
- **Glossary/Acronyms** mention the different terms and abbreviations used in the policy.

Policy Statements



- A policy is only as **effective** as the policy statements it contains. Policy statements must be written in a very **clear** and **formal** style
- Several good examples of a policy statement are:

01

All computers must have **anti-virus protection** activated to provide real-time, continuous protection

02

All servers must have the **minimum services configured** to perform their designated functions

03

All access to data is based on a **valid business need** and subject to a formal approval process

04

All computer software must be purchased by the IT department in accordance with the organization's **procurement policy**

05

A copy of all backup and restoration media must be kept with the **off-site** backup media

06

While using the Internet, nobody is permitted to abuse, defame, stalk, harass, threaten anyone else or violate local and international **cyber laws**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

An organization's security policy is said to be successful, if it consists of clear and concise policy statements. A policy statement is an outline that defines the in-depth structure of the organization's policy. Every policy draft should have a valid policy statement that defines the organization's course of action during the time of a circumstantial situation. The policy statement helps employees understand the preventive measures they are permissible to take.

An example of an ideal policy statement is:

"All access to data will be based on a valid business need and is subject to a formal approval process"

The above policy statement example clearly states employees can access data only on approval from management. It can be concluded that if any employee does not adhere to the policy statement, the organization has the right to take required action.



The steps below are used to create and implement an effective security policy:

1. **Risk Assessment:** An organization needs to perform a risk assessment of their assets before drafting a policy. During a risk assessment, risks are identified and determine its severity and criticality.
2. **Standard Guidelines:** Organizations set up guidelines before drafting their own security policy. A set of standard guidelines drafted in a clear language is helpful to an organization and their employees.
3. **Management Input:** Management is involved in the process of drafting a new policy or adding a policy to the existing one. Employees will only adhere to the drafted policy if management legally sanctions and approves it. Any policy drafted without management consent is illegal and will cause serious consequences.
4. **Penalties:** Certain organizations have very strict policies. If an employee does not follow these policies, severe actions can be taken against them. Organizations should always mention the penalties that an employee will suffer if they do not follow the rules.
5. **Final Draft:** Once management approves the completed policy document, the document is distributed among everyone in the organization.
6. **Accepted by employees:** Employees are required to accept all the policies set by the organization. Employees can give their acceptance by reading the document carefully and then signing it.

7. **Deployment of policies:** To enforce policies in the organization you may need additional deployment tools.
8. **Training the employees:** Employees should be periodically trained on the organizational policies. Even if the policies in the organization are functional for a long time, there are employees who might be new. Bringing awareness to these employees is a very important task.
9. **View and Update:** Even if an organization is in business for a long time, reviewing their policies is still a requirement. With the introduction of new technologies and new security breaches, updating policies are a necessity. Policies that no longer protect and the current technology and/or scenarios are not useful to the organization.

Considerations Before Designing a Security Policy



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

✓	What is the purpose of the policy? Is it a value addition or a mere formality?
✓	Is the policy in line with the training programs ?
✓	Does the policy comply with the organization's objectives?
✓	Is the policy a guideline for best practices or does it need to be based on a some standard ?
✓	How many people fall under the of the policy? Who are they?
✓	What is the least amount of information each employee must know to do their jobs?
✓	Are all the details required in the policy?
✓	Can the policies be linked ? What is the best method?
✓	What does the staff need to understand from the policies?

Organizations should not deploy a policy without knowing the purpose first.

Before designing a security policy, answer the following questions:

- **What is the purpose of the policy? Is it a value add or a mere formality?**

Organizations or management should be aware of the policy's purpose when deployed in the organization. If management understands the purpose of the policy, it will be easier to make their employees adhere to it.

- **Is the policy in line with any training program?**

Usually, organizations introduce a policy without training or workshops for the employees. It is necessary to deploy only those policies employees have been trained. Policies without training or workshops will serve no good to the organization, as employees will not be aware of its pros and cons.

- **Does the policy comply with the organization's objectives?**

While documenting the policy, it should be noted that they run parallel with the objectives of the organization. Implementation of the policy cannot be termed successful, if it does not meet the organizational objectives.

- **Is the policy a guideline for a better practice or does it needs to be based on a standard?**

The purpose of introducing policies may differ. It is important to know why the policies are being introduced in the first place. Usually certain policies are formed as per the

regulations by the government and some are implemented for the organization's personal security.

- **How many people fall under the purview of this policy? And who are they?**

While designing a policy there are situations where only some employees or a particular group needs to adhere to it. It is important to categorize these types of policies, which leads to simplicity while implementing it in an organization.

- **What is the least every employee needs to know?**

All an employee should know regarding the policy is how the policy should be implemented on a daily basis. The training session conducted for the employees should inform them about the action taken against them in case of compliance.

- **Do I really need all the details written into this policy, or is this better written in System Specific Security Policies (SSSPs) for the IT professional?**

While the policy is documented, it is important to understand the target. It is not necessary that every policy might be part of the same document. **Example** - Document for the security policy will not include the HR policy.

- **How to best link the policies?**

Policies should be documented in a clear and concise language. The document should include all the best practices an organization will undertake and those employees will adhere to.

- **What do the staff need to understand from the policy?**

Management can keep the main objective clear when they write the policy with user friendly language. For example, the policies have to be followed by everyone in the organization. Management should arrange training sessions or workshops to help employees who are not certain of any policy or they are not clear. With the introduction of these policies, an organization makes it very clear to employees on the level of awareness required for securing the data and resources in the network.



The security policy structure provides an overview of the functionalities of security aspects. The security policy structure should ensure that the following is in place:

- The description of the issue the policy is used for.
- Details regarding the status of the policy and the description about the domains where the policy has been applied.
- Employee functions and responsibilities who are involved in the policy.
- The extent to which the policy is compatible with the organization's standards.
- The tasks and procedures involved in the policy and the ones that are not involved.
- End consequences will be encountered if the policy is not compatible with the organization's standards.

The security policy must contain all the information that is required for a successful implementation of the organizational work process.

Consider the following key points while designing security policies:

- **Develop policies that you plan to enforce:** Not enforcing a policy is of no use. Real-time implementation of all statements mentioned in the policy is necessary for limiting network access.
- **Explain the purpose of the policy:** Based on the functions of the organization, develop the policies for a specific network objective.

- **Develop security policies that do not require updates too frequently:** To avoid frequent amendments, the overall network issues are to be pre-estimated.
- **Differentiate between policies, standards and recommendations:** The network policies should be comprehensive and thorough, but should not be too specific.
- **Represent the basic goals of the organization:** Depending on the information, assets of an organization represent the range of network security.
- **Make sure your policies are understood:** Network policies should be straightforward, but not too complicated.
- **Include your policies as part of your security awareness training:** At least one policy has to be included in the security awareness training.
- **Identify the basic risks that can be expected:** The basic risk factors of the network are to be pre-estimated by the network admin.

Some of the measures to develop security policies are as follows:

- Every company and client should identify its roles and responsibilities and its tasks should be described in detail. That means the knowledge of the structure of the organization, the responsibilities of individuals, the tasks performed by everyone in the organization and who tackles the security policies is essential. It is important to make sure the policies address the problems, requirements, and objectives of the organization. The representation of each problem should be to the maximum extent. It should also include data security, legal issues, and human resources. The development and operations of the organization should be represented in the policies.
- The basic goals of the business are represented. Business knowledge is essential to improve security and to build a good security policy. Consider an organization that needs extensive auditing, monitoring and a recovery system that takes regular data backups. This may not be the case for the rest of the company. Therefore, the policies of an organization differ according to their requirements. Some policies may be cost effective, whereas others may be expensive. That means that security policies are specific to each organization.
- The next step in developing policies is to identify the security principles that represent the company's security objectives. These goals are to be checked regularly and introduced into the development process whenever necessary. The aim of security policies is to describe the policies and principles of the organization with less technical details and in a simple way.
- The assets and data that need security are recognized and categorized. The valuable data is made the center of all the security policies. Data that has been identified as more vulnerable to threats is secured. Cataloging the data and assets makes it easy for management to make decisions with respect to its value and use. This helps to effectively control resources.

- As the data is collected and analyzed, it should also be classified. Data is the center of every policy that is developed. Data flow analysis is important to any and all issues related to data. For example, during a transaction, data flows through the browser, the web, and other media such as telephone lines, servers, and firewalls. The data is stored in databases, on disks, tapes, or paper. If the flow of data is tracked through the media, it can be determined where there are potential data vulnerabilities and data corruption locations and control mechanisms can be implemented to prevent the vulnerabilities and corruption.
- The expected risks are identified. Developing a profile for possible threats helps enable a decision-making process for any threats within that area. The chance of risk associated with issues and the amount of money needed to recover from that loss can be recognized. The nature of threats differs depending on different areas. For instance, the result of attacking financial transactions would be very different from an attack on an art website.
- The services that guard the system are to be identified. Once the data resources and flow of data are identified, a risk profile is created. The security services that apply to that particular area will be recognized and identified. The services for security include responsibilities, authentication, accessibility, recognizing, integrity, secrecy, and non-duplication. Knowledge of the security needs of a particular environment is essential for choosing the security policy to be employed over that area.

Policy Implementation Checklist

After the **security policy** has been created, the most difficult part of the process is deploying it throughout the organization

- Make sure the security policy is **approved** by senior management
- Make sure the security policy is officially **adopted** as a company policy
- Review each policy** and decide how it can be enforced within the organization
- Ensure that appropriate tools and techniques **are in place to conform to the policy**
- Develop a policy change plan for both the network and the policy itself
- Coordinate with other departments to **develop procedures based on the policies**
- Provide basic information security **awareness** training to employees

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Implementation of the security policy happens after it is built, revised, and updated. A proper model and outline of the policies must be created. Suggestions from stakeholders must be included to directly correlate it with the interests of the organization. After its completion, the final version must be made available to all staff members so they may understand it. It must be readily available at any time when needed. It must be placed on the internal network and intranet. Proper training of the policies must be given to employees for their prompt understanding and suggestions must always be taken into consideration. For effective implementation, there must be a rotation of jobs, so that different people handle data. This will help employees identify any limitations the security policy has. Company data is very critical. It must not be given to everyone and must not be made public, so proper care must be taken. There must be a proper security awareness program, cooperation and coordination among employees.

Once the security policy is designed and developed, the next step in the process is also the hardest, deployment.

Guidelines for successfully implementing the policy:

- Ensure the security policy is backed by the organization's senior management team and is officially adopted as company policy.
- Go through each policy and think about how it will be applied within the organization.
- Make sure the correct tools are available to conform to the policy.

- Create a plan to make any necessary changes to either the network or the policy.
- Work with the necessary departments within your company (Legal, IT, HR, etc.) to establish procedures to support your policies.
- Provide basic information security awareness training to everyone through a basic Security Awareness Program.
- Make the security policy available to all employees having access to the information assets the policy governs.
- The Information Security Officer or IT Security Program Manager are responsible for implementing and managing the security policy.
- Ensure the organization is well equipped with the technology and tools needed to manage the security policy properly.
- Make sure visitors are provided the Acceptable Use Policy in the event they are allowed to use the company's network.

Types of Information Security Policies

Enterprise Information Security Policy (EISP)

- EISP drives an organization's scope and provides direction to their security policies
- Examples of EISP:
 - Application Policy
 - Network and network device security policy
 - Security policy auditing
 - Back up and restore policy
 - System security policy
 - Policies for servers

Issue Specific Security Policy (ISSP)

- ISSP directs the audience on the usage of technology based systems with the help of **guidelines**
- Examples of ISSP:
 - Remote access and wireless policies
 - Incidence Response plan
 - Password policies
 - Policies for personal devices
 - User account policies
 - Internet and web usage policies

System Specific Security Policy (SSSP)

- SSSP directs users while **configuring or maintaining** a system
- Examples of SSSP:
 - DMZ policy
 - Encryption policy
 - Acceptable use policy(AUP)
 - Policies for secure cloud computing
 - Policies for Intrusion detection and prevention
 - Access control policy

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

In an organization, policies are crucial for information security planning, design and deployment. These policies provide measures to handle issues and the technologies that could help users accomplish their security goals. The policy also explains how the software or equipment functions in the organization.

Information technology enterprises deploy security policies such as:

Enterprise Information Security Policies (EISP)

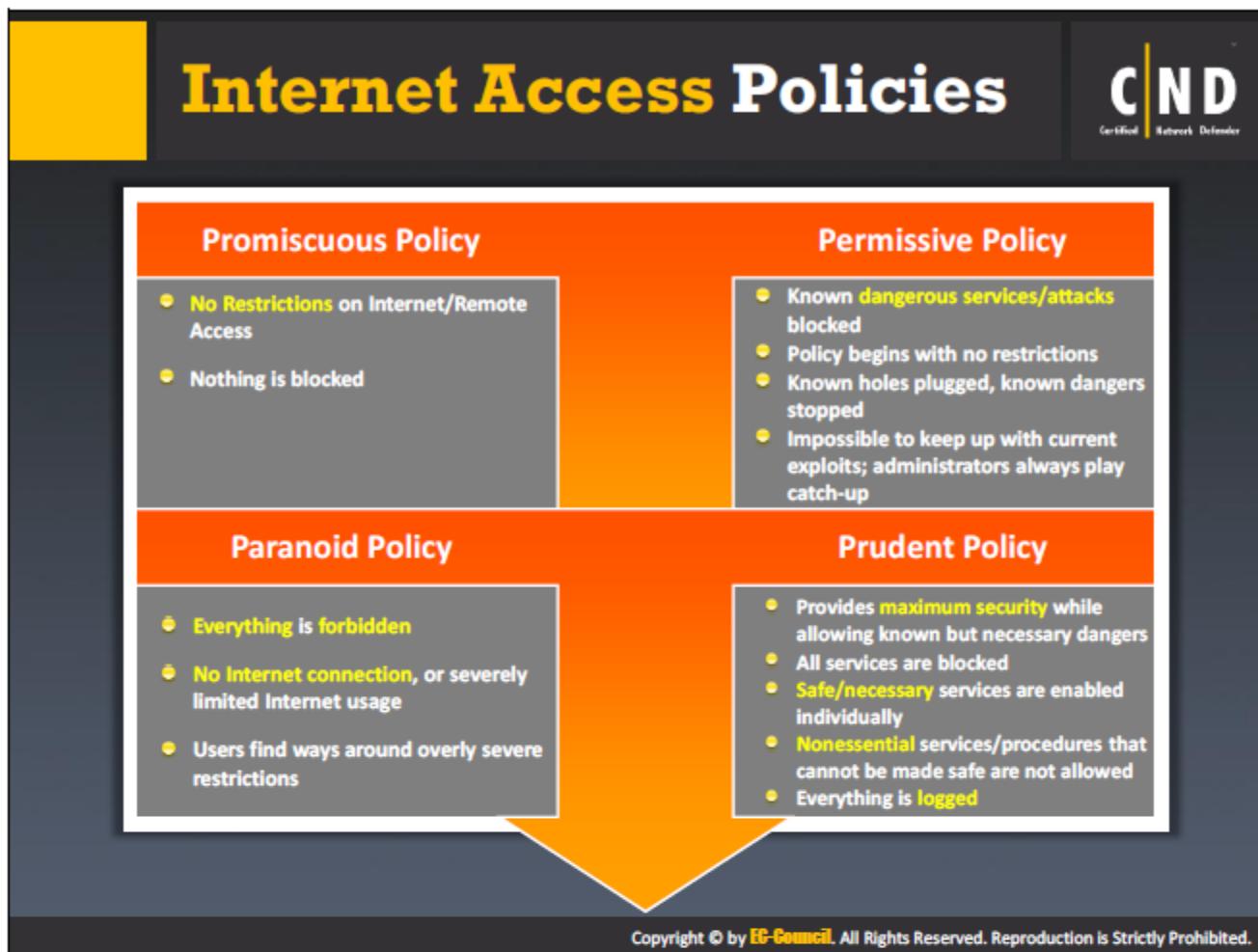
The EISP support organizations by offering ideology, purpose and methods to a secure environment for enterprises. It sets out a method for development, implementation and management of security programs. These policies also ensure the information security framework requirements are proposed and met.

Issue-Specific Security Policies (ISSP)

These policies aim to address specific security issues in an organization. The scope and applicability of these security policies are completely dependent on the type of issue and the methods utilized by them. It specifies the necessary technologies along with preventive measures such as authorization of user access, privacy protection as well as a fair and responsible use of the technologies.

System-Specific Security Policies (SSSP)

The implementation of a System-Specific Security Policy is to focus on the overall security of a particular system in the organization. Organizations develop and manage this type of policy, including procedures and standards in order to maintain the systems. The technologies used by the organization should also be included in system-specific policies. It addresses the implementation and configuration of technology and user behavior.



Internet access policies define the restricted use of the Internet. It is important for employees to know which of their actions is restricted while accessing the Internet. The Internet access policy helps keep employees informed on what they can browse and what they cannot. An internet policy includes guidelines for permissible use of the Internet, system security, network setup, IT service, etc.

Internet access policies broken down into the four categories below:

- Promiscuous Policy:** This policy does not impose any restrictions on the usage of system resources. For example, with a promiscuous Internet policy, there is no restriction on Internet access. A user can access any site, download any application, and access a computer or a network from a remote location. While this can be useful in corporate businesses where people travel or work at branch offices need to access the organizational network, it also opens the computer to threats such as malware, viruses and Trojans. Due to free Internet access, this malware can come in the form of attachments without the knowledge of the user. Network administrators must be extremely alert while choosing this type of policy.
- Permissive Policy:** This policy begins wide-open and only known dangerous services/attacks or behaviors are blocked. For example, in a permissive Internet policy, the majority of Internet traffic is accepted, except for several well-known and dangerous services/attacks. Because only known attacks and exploits are blocked, it is impossible for administrators to keep up with current exploits. They are always playing catch-up with new attacks and exploits.

3. **Paranoid Policy:** A paranoid policy forbids everything. There is a strict restriction on all company computers, whether it is system or network usage. There is either no Internet connection or severely limited Internet usage. Due to these overly severe restrictions, users often try to find ways around them.
4. **Prudent Policy:** A prudent policy starts with all services blocked. The administrator enables safe and necessary services individually. This provides maximum security and logs everything, such as system and network activities.

Acceptable Use Policy

An **acceptable use policy** defines the proper use of an organization's information, electronic computing devices, system accounts, user accounts, and network resources

Design Considerations:

- Should users **read and copy** files that are not their own but are accessible?
- Should users modify files they have write access to but do not own?
- Should users be permitted to use **.rhosts** files? Even though the entries are acceptable?

- Should users be **allowed** to share accounts?
- Should users make **copies** of system configurations for personal use or provide them to other people?
- Should users have the ability to make **duplicates** of copyrighted software?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Acceptable-use policies consist of rules decided by network and website owners. This type of policy defines the proper use of computing resources. It states the responsibilities of users to protect the information available in their accounts. The users must accept the policy restrictions while accessing a computer on the network or the Internet. An AUP (Acceptable Use Policy) covers principles, prohibitions, reviews and penalties and it prohibits the user from using the corporate resources for personal reasons.

An AUP is an integral part of information security policies. Generally, organizations ask their new members to sign an AUP before they are permitted to access the information systems. An AUP should cover all major aspects about what users are permitted to do and what they are not permitted to do in the IT infrastructure.

To ensure the AUP is followed properly, administrators conduct regular security audits.

Example: Many organizations restrict discussions on political or religious topics on sites or in emails.

The majority of AUPs describe the penalties of a policy breach, those penalties range from temporarily disabling the user's account to extreme measures such as legal actions.

User Account Policy

The User Account Policy defines the creation process of **user accounts** and includes user rights and responsibilities

Design Considerations:

- Who has the authority to **approve** account requests?
- Who (employees, spouses, children, company visitors, etc.) are permitted to use the computing resources?
- Can users have **multiple accounts** on a single system?
- Can users **share accounts**?
- What are the rights and responsibilities of the user?
- When should an account be **disabled and archived**?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The User Account Policy is a document specifying the requirements for requesting and maintaining an account on the organization's network. It mentions the processes for creation, deletion and operating user accounts by defining the type of accounts created under a specific network.

The user account policy defines the process of account authorization, user responsibilities as well as Internet services for both internal and external users. In addition, it also defines the creation of a username and password, encryption standards, type of verifications in case the user forgets their password and the devices utilized for accessing or linking to the account.

This policy also defines the necessary user age limit, profession and other criteria for creation or classification of the account such as guest, internal, external, media, etc. It is essential for large sites where users may typically have accounts on many systems. Some sites have users read and sign an account policy. Software applications have users sign an EULA – End User License Agreement as part of the account request process.

Example wording: "Employees shall only request/receive accounts on systems they have a true business need to access. Employees may only have one official account per system and the account ID and login name must follow the established standards. Employees must read and sign the acceptable use policy prior to requesting an account."

Network administrators have responsibilities when implementing a user account policy:

1. **Types of accounts:** As per the organization's policy, administrators are asked to create two types of accounts in the network – Administrator account and Standard account. The

administrator account is for the network administrators only. It may or may not include the top management of the organization. Standard accounts are for employees irrespective of the department in which they are working.

2. **Account Permissions:** Administrators are required to set the level of permissions to every employee in the organization. Even though a team leader may not have access to the administrator privileges, the level of permission will differ with the reporting member of this team. Administrators should assign the permissions according to the designation of the employee. Permissions can also be set for a group. Everyone in the HR group has a standard set of permissions.
3. **Account auto-lock:** An administrator sets a length of time an account will automatically lock. If an employee has not reported to the office for three consecutive days, the auto lock feature will enable and the account will be locked automatically. This feature prevents anyone from forcing the login or attempting to login to the account when the user is not there. This feature is present in mobile phones as well and it prevents others from accessing the device without the log in code.

The User Account Policy should mention certain important characteristics, operations and maintenance. The policy content should state the following:

- Who has the authority to approve account requests?
- Who is allowed to use the resources (e.g., employees or students only)?
- Are there any citizenship/resident requirements?
- Are users allowed to share accounts or are they allowed to have multiple accounts on a single host?
- User's rights and responsibilities.
- When the account should be disabled and archived.
- How long can the account remain inactive before it is disabled?
- Password construction and aging rules.

Remote Access Policy

C|ND
Certified Network Defender

■ Remote Access Policy defines who can have remote access, access mediums, and remote access security controls

Design Considerations:

- ✓ Who is allowed to have **remote access**?
- ✓ What **specific methods** (such as cable modem/DSL or dial-up) does the company support?
- ✓ Are **dial-out modems** allowed on the internal network?
- ✓ Are there any **extra requirements**, such as **mandatory anti-virus** and security software on the remote system?
- ✓ Can other family members of an employee use the **company network**?
- ✓ Do any restrictions exist on the data that can be **accessed remotely**?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Remote Access Policy document defines the acceptable guidelines for remote access to the network and resources. A remote employee should follow the policy when connecting to the internal network. The Remote Access Policy is helpful to organizations having a geographically dispersed network. Implementing the remote access policy helps minimize potential damage that can occur from unauthorized external network traffic. Implementing remote access includes dial-in modems, frame relay, ISDN, DSL, VPN, SSH, Wi-Fi, etc.

Points to consider in the policy:

- **User authentication:** Organizations should have a strict user authentication policy for remote users. The organization has the right to deny access to users having a weak password or user credentials. The policy should also state the action taken against employees if they share their remote credentials with others.
- **Information encryption:** Employees working as a remote user should include encryption of their data while working on a shared infrastructure. This maintains the confidentiality and integrity of the data. The organization must educate remote users on the encryption policy they need to follow.
- **Usage of network and network devices:** The policy should restrict employees from reconfiguring their network devices for the purpose of split-tunneling. This can make the network vulnerable to intrusion. Employees should not perform any third party activities on the organization's network and should not connect to any other third-party network.

- **Antivirus and patches:** The systems used by remote users should meet the organization's requirement. Users should have an up-to-date anti-virus installed on their system. They should proactively install updates for the antivirus and patches for the operating system.
- **Access to data:** Administrators should assign privileges to the remote user according to their roles and responsibilities in the organization. Organizations should restrict users from accessing confidential organization data remotely.

Network administrator's responsibilities in enforcing remote access are:

1. Ensure remote system has specified version of antivirus, firewall and malware
2. Predefine VPN tunnel's connection
3. Enforce an authentication method for the remote VPN
4. Enforce access control on the remote system when connected through remote access
5. List a set of devices which can be used for remote access

Information Protection Policy

C|ND
Certified Network Defender

Information Protection Policy defines guidelines for processing, storing and transmitting sensitive information

Design Considerations:

-  What are the information sensitivity levels?
-  Who can access the sensitive information?
-  How is the sensitive information stored and transmitted?
-  What level of sensitive information can be printed on public printers?
-  What is the process for removing sensitive information from storage media (paper shredding, scrubbing HDDs, degaussing disks, etc.)?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Information-Security policy is a document that guides employees to defend their data or physical devices from unauthorized access. The main aim of the policy ensures the information is not shared or modified by any external sources. The organization should define the level of sensitive information. Organizations should make it a practice to ask new employees to sign the information-security policy.

Lack of an information security policy can lead to vulnerabilities in the network and system. With no information security policy in place, employees can knowingly or unknowingly share the data to external sources.

The information security policy should be drafted based on the following points:

- List of authenticated users who can have access to sensitive information.
- The process and method of saving sensitive information. This can include data that is either archived or encrypted.
- The policy should mention the location where the sensitive information is stored. The authorized users should be asked to save the information in this location. Saving the data at any other location can potentially cause data theft or exposure of information to other sources.

Implementation of information security assures the data will be protected throughout the functioning of the organization.

The slide has a yellow header bar with the title 'Firewall Management Policy' in bold black font. To the right of the title is the 'CND' logo with 'Certified Network Defender' underneath. Below the title is a large text box containing a statement about Firewall Management Policy. Underneath this is a section titled 'Design Considerations:' followed by five numbered items. At the bottom of the slide is a copyright notice.

Firewall Management Policy defines access, management, and monitoring of firewalls in the organization

Design Considerations:

- 1 Who has **access** to the firewall systems?
- 2 Who can receive requests to make changes to the **firewall configuration**?
- 3 Who can **approve** requests to change the firewall configuration?
- 4 Who can see the firewall configuration rules and access lists?
- 5 How often should the firewall configuration be **reviewed**?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A network administrator's responsibilities when configuring firewall security policies are:

- **Authentication of service or application:** Administrators should verify the applications or services before they Allow by default. A service that does not look legitimate should not be added.
- **Setting up a dashboard:** Administrators can set up a dashboard that will include all threats and vulnerabilities the organization's network can encounter. Setting up a dashboard forms a strong rule base.
- **Enable anti-spoofing protection:** To ensure the source IP address is same as the security gateway interface, it is important to enable anti-spoofing protection.
- **Telnet access:** Telnet is insecure by nature. Administrators should not allow Telnet access for the secure functioning of the network.
- **FTP connection:** FTP connections should only be allowed if administrators have to upload error logs for the vendor. In other scenarios, it is advisable to prohibit FTP.
- **Refrain direct connection:** Administrators should avoid setting up a direct connection between an internal client and external service. If the organization needs a connection to be established, it can be done through proxy servers.

Special Access Policy

C|ND
Certified Network Defender

Special Access Policy defines the terms and conditions of granting special access to system resources

Design Considerations:

- Who can **receive requests** for special access?
- Who can **approve requests** for special access?
- What are the **password rules** for special-access accounts?
- How often are **passwords changed**?
- What **reasons or situations** can lead to revocation of special access privileges?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Regulating the special access policy allows certain employees to access the data in the network. Before implementing a special-access policy in the network, an administrator should consider the following items:

- **Authorized users:** Special-access to resources can only be given to privileged users. Usually these users are top-management employees or administrators.
- **Approval:** Employees can be given privileged access only if it is authorized by management or the administrator.
- **Password rules:** The policy should have a policy statement regarding password rules. This may include the strength of the password, the validity of the password, etc.
- **Revoking Privileges:** Users provided with special privileges should be notified of the circumstances under which their privileges can be revoked.

Network Connection Policy

C|ND Certified Network Defender

Network Connection Policy defines the standards for establishing the **connection** for computers, servers, or other devices to the network

Design Considerations:

- 1 Who can **install new resources** on the network?
- 2 Who **approves the installation** of new devices?
- 3 Who must be notified when **new devices** are being added to the network?
- 4 Who **documents network** changes?
- 5 Are there any **security requirements** for the new devices being added to the network?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A network connection policy is drafted to secure the organization's network. The network connection policy defines regulations to be followed and implemented on the systems, servers and other electronic devices used in the organization. An effective network-connection policy involves securing the devices from potential intrusion an organization can experience.

The following points should be included in the network-connection policy:

1. **Connection of devices:** The policy should include the normal rules for connecting their electronic devices, including their personal mobile phones. Employees should be restricted from making any changes in the network through their devices as it may cause network fluctuations or loss of connectivity.
2. **Authenticating:** For a better security service, employees should be asked to authenticate their device every time it is connected to the network. Though it might be a frustrating task for some, the security of the network is the main priority.
3. **Responsibility of employee:** Every employee using their personal devices on the organization's network is responsible for their systems to meet the security standards. The organization will have full authority to deny the device that does not meet their security standards.

Business Partner Policy

C|ND
Certified Network Defender

Business Partner Policy defines agreements, guidelines, and responsibilities for business partners to run business securely

✓	Is it mandatory for a company to have a written security policy ?
✓	Should each company have a firewall or other perimeter security device ?
✓	How will one communicate (virtual private networking or VPN over the Internet, leased line, and so forth)?
✓	How will access to the partner's resources be requested?
✓	Should each partner keep accurate accounts, books, and records relating to the business?

Design Considerations

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Organizations working in partnership follow certain guidelines that are drafted under a business-partner policy. It defines the guidelines partners are required to follow so they can run their business securely. There can be geographical and cultural differences between the two business partners, you need to be careful when drafting policies in these scenarios. Business - Partner policies should address the following questions:

- Need of Policy:** The business partner policy defines the rules and regulations of the respective organizations. Certain policies followed by employees in company A may not necessarily be followed in company B. Organizations should work out a third way for drafting the policy, so it does not affect how both companies function.
- Security:** Getting employees to follow common security rules is the biggest challenge when drafting a business-partner policy. The policy should mention the common security boundaries for both partners and how it will be regulated if employees do not follow it.
- Resource sharing:** Even though both organizations are in a partnership it does not mean the companies will have access to each other's data. The policy should state the amount of data that both parties can share and access. Data breaches either partner will result in legal actions.
- Record maintenance:** In a partnership, an organization should maintain a log for every transaction. This maintains a healthy partnership between each company.

The diagram features a dark blue header bar with the title 'Email Security Policy' in white. A yellow square is positioned to the left of the title. To the right is a logo consisting of the letters 'CND' in white on a dark background, with the text 'Certified Network Defender' underneath. Below the header is a light blue main area containing an orange callout box. The callout box has the text 'An email security policy defines the proper usage of corporate email' at the top. On the left side of the callout box is a large orange arrow pointing right, containing the text 'Design Considerations:'. To the right of the arrow is a black rectangular box listing seven bullet points:

- Define prohibited use
- If personal use is allowed, it needs to be defined
- Employees should know if their emails are reviewed and/or archived
- What types of emails should be kept and for how long
- When to encrypt emails
- Consequences of violating email security policy

At the bottom of the slide, a dark footer bar contains the text 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'

Email security policies are developed to ensure corporate email is used properly. A simple personal email from a corporate account can result in unintended information disclosure.

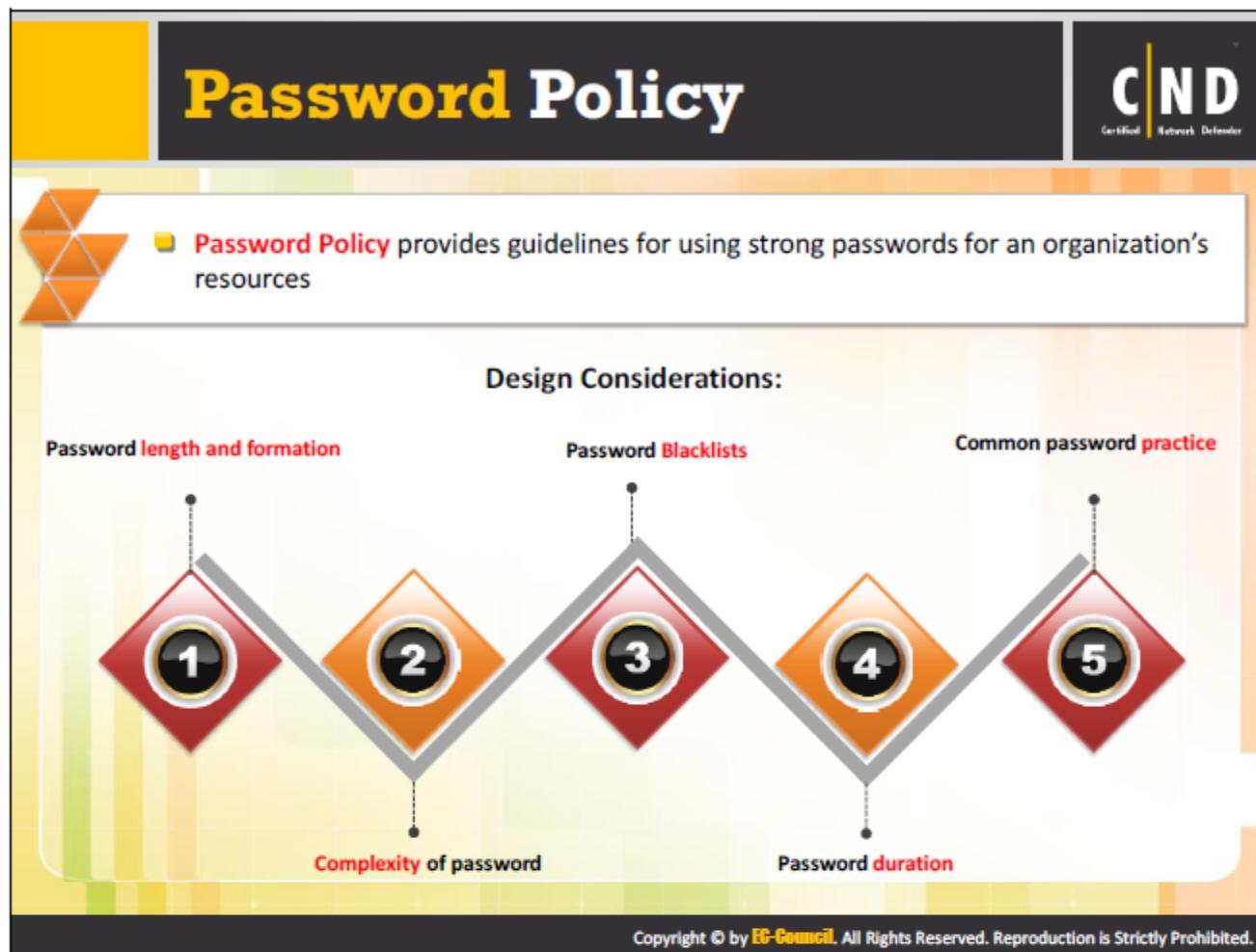
Implementation of an email security policy lets the organization achieve:

1. **Competitive accomplishment:** Through an email security policy, organizations train their employees in email etiquette. Including but not limited to, drafting effective emails, learning about the reply in target duration, etc. This helps the organization maintain its respective competition in the market.
2. **Employee productivity:** Email security policies state what the normal use of corporate email is. This restricts employees from using emails for their personal use, increasing the overall productivity of the organization.
3. **Less employer liability:** Organizations should state the consequences or the actions taken against the employee if the normal use policies are not followed. The liability of the employer is reduced as a result.

Responsibilities of network administrators:

1. **Email Use and Limitations:** The policy should state the scenarios and domains where employees cannot use their corporate email addresses. The email policy should mention; in which scenarios an employee cannot use the corporate email address specifically. The policy should also instruct employees not to open malicious attachments.

2. **Defining extent of personal use:** Policy should set boundaries for employees when using corporate email for their personal use.
3. **Monitoring of emails:** If an organization will be reviewing the emails of all the employees, it should be mentioned in the policy.
4. **Duration of emails:** Employees should be notified about the duration for keeping email in their mailbox. Employees should be informed that the administrators will have the right to archive emails after a certain period of time.
5. **Encryption:** In case of sensitive information being sent or received, employees should be aware of the encryption policy of the organization.
6. **Actions against compliances:** The policy should clearly state the action taken against an employee if they fail to follow the policy set by the organization.



A password policy is a set of rules to increase system security by encouraging users to employ strong passwords when accessing an organization's resources and to keep them secure.

The purpose of the policy is to protect the organizational resources by creating robust protected passwords.

The policy statement should include a standard practice for creating a robust password.

For example,

- The password length should be between 8 and 14 characters
- The password should include both uppercase and lowercase letters, numerical digits and special characters
- Special characters include (@, %, \$, &, ;)
- Passwords are case sensitive while the user name or login ID is not
- Password history: Unique passwords must be used while changing the old password. Passwords cannot be reused.
 - Maximum password age: 60 days
 - Minimum password age: No limit

Some of the components of a password policy include:

▪ Password length and formation

The policy includes the length of the password. The password length varies according to the organization. The formation of a password includes

- One or more numerical digits
- Special characters such as @, #, \$
- Use upper case and lower case letters
- Avoid using personal information
- Use of company name in the password is prohibited

▪ Password duration

The policy suggests users change their passwords regularly usually every 90 or 180 days. Changing a memorized password is hard for the user, but it is necessary to avoid password stealing.

▪ Common password practices

The password policy statement should include guidance or best practices on creating, storing and managing passwords

For example, it should include guidelines such as:

- Do not share your computer user account details.
- Do not keep a common password for all accounts.
- Do not share passwords.
- Never write the password anywhere, instead remember it.
- Employees should not communicate their password through e-mail, phone or IM's even to the administrator.
- Do not leave the machine unattended. Always log off or lock the system when leaving the desk.
- Keep different passwords for the operating system and frequently used applications.

The password policy should include a disclaimer, which should inform everyone on the consequences of not following the guidelines stated in the password policy. The disclaimer should involve all employees, including top management. Disclaimers can include verbal or written warnings or termination.

Physical Security Policy

C|ND
Certified Network Defender

Physical Security Policy defines guidelines to ensure that adequate physical security measures are in place

Design Considerations:

- ⌚ Is the **building protection deficiency** reviewed on a regular basis?
- ⌚ Is there a process to **identify outsiders** such as visitors, contractors, vendors, etc. before giving them access to the premises?
- ⌚ Is there adequate **lighting systems** in place?
- ⌚ Are each of the **entry points** properly blocked?
- ⌚ Are the badges, locks, keys and authentication controls audited on a regular basis?
- ⌚ Is **video surveillance** footage monitored regularly?
- ⌚ Is there a proper **inventory** of an organization's assets maintained regularly?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Physical security is the security provided in terms of physical assets, which can be damaged physically. In IT organizations where there is a huge amount of physical assets present, the assets are prone to damage during installations, during changing the assets from offshore to local locations. Care must be taken in terms of how frequently the risks are being monitored and analyzed, and the training provided to the people handling or working with the physical assets must be monitored.

Designing a physical security policy helps an organization maintain certain norms, which can be followed by the employees, reducing the probability of loss.

Information System Security Policy

C|ND
Certified Network Defender

Information system security policy defines guidelines to **safeguard** an organization's information systems from malicious use

Design Considerations:

- Are the information systems **protected** with anti-malware?
- Is the anti-malware **updated** regularly?
- Is the **operating system** updated and patched regularly?
- Are they **secured** using strong password policies?
- Are they secured with strong **physical security policies**?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The information security policy helps maintain the integrity and confidentiality of the information system.

Information system security policy statements should be focused on:

1. Installation of antivirus
2. Regular updates of software
3. Applying a firewall
4. OS upgrades
5. Password policy
6. Physical security standards

Bring Your Own Devices (BYOD) Policy

A BYOD policy provides a set of guidelines to **maximize business benefits** and **minimize risks** while using an employee's personal device on an organization's network

Design Considerations:

- What **personal devices** are allowed to use under BYOD ?
- Which **resources** can be accessed through BYOD devices?
- What needs to be **disabled** in BYOD devices?
- What are the **Data storage considerations** for BYOD devices?
- What **security measures** are to be put in place for data and BYOD devices?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bring Your Own Device (BYOD) is a terminology used by organizations to motivate employees to bring their own devices. As it is difficult for organizations to keep up with the changing pace of technology, BYOD has been beneficial to employers. BYOD also has a disadvantage, if the device is not fully tested and does not follow the policies it can be a threat to the IT infrastructure.

The existence of a BYOD policy is important. The policy provides a set of guidelines to maximize business benefits and minimize the risks while using employee personal devices on an organization's network.

Aspects of a BYOD policy:

1. **Permissible devices:** The policy should state the name of the devices an employee is allowed to use. The list of devices may differ based on the designation of each employee in the organization.
2. **Permissible resources:** The policy should clearly state the resources an employee can use while using their own device. The policy should mention the actions taken if an employee does not adhere to these policies.
3. **Services to be disabled:** Before an employee connects their device to the corporate network, administrators should verify the services and the applications running on the device. If certain services or applications are a source of vulnerabilities, administrators should disable those services immediately.
4. **Data Storage:** It is necessary to document the location of data storage for BYOD. Administrators should provide a separate location for data on employee devices. Storing

the data in existing drives can be a threat to the data. Administrators must provide a separate drive to employees.

5. **Security measures for data and BYOD device:** Employees should be made aware of threats and vulnerabilities while they use their devices in the corporate network. It is the responsibility of the administrator to monitor these devices along with all corporate devices.

While BYOD is emerging as a new trend in organizations, it is the responsibility of the administrator to enforce the BYOD policy. A few administrator responsibilities associated with a BYOD policy are:

1. **List of devices:** Administrators can prepare a list of devices and software in the BYOD policy document. Items such as these listed below:
 - Smartphones (with model number)
 - Laptops (with model number)
 - OS (with version)
 - Any other process specific software or app
2. **Resources to be accessed:** Depending on the designation of the employee, administrators can allow the following resources on BYOD.
 - E-mail
 - Contact
 - Calendar
 - Process specific documents
3. **Disable the use of the following on BYOD devices:**
 - Storage or transmission of illicit materials
 - Using another company's proprietary information
 - Harassing
 - Engaging in other business activities
4. **Store data on BYOD devices with proper security measures using:**
 - The device
 - Organization server
 - Cloud
5. **To secure data on BYOD devices follow these steps:**
 - Password (BYOD device also) and encryption policies
 - Monitor data transferred

Software/Application Security Policy

 Certified Network Defender

Application security policy mandates proper measures to be set up which **enhance the security of in house and purchased applications**

Design Considerations:		
Configuration Management	Authentication	Error Handling & Exception Management
Data Protection in Storage & Transit	User & Session Management	Logging & Auditing
Authorization	Data Validation	Encryption

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Application security involves securing the inbuilt and purchased applications running on the system. The security policy covers the application throughout its complete life cycle. The threat to an application is caused by software tampering, parameter manipulation, authorization, cryptography, etc.

Drafting the guidelines for application security mandates the proper functioning of the application, further enhancing how the system works.

The key factors in documenting a software/application security policy are:

1. Data validation
2. Session Management
3. Authentication
4. Authorization
5. Encryption

A network administrator's role in enforcing application policies is:

1. **Criteria for data validation:** It is required to set measures to validate data flowing in and out of the application.
2. **Authentication process:** Administrators should set up an authentication policy for all systems. If a user is trying to install a third party application, the system will prompt for an

administrator password. This will restrict users from installing third party applications without administrator rights.

3. **Authorization standards:** Administrators should authorize application use for only those who need it. The authorization can also be limited to certain parts of the application's data.
4. **Encryption policy:** Administrators can encrypt the sensitive application data, preventing users from getting access to it.
5. **Monitoring:** Every employee application session should be monitored.

Data Backup Policy



The backup policy helps an organization **recover and safeguard** their information in the event of a security incident/network failure

Design Considerations:



The location of data backup



Name and contact of authorized personnel who can **access** backups



Backup schedule



Type of backup method used



Hardware and **Software** requirements for taking backups

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Creating a backup policy is one of the most important things you can do for your data security plan. Optimized backup policies and procedures will save your organization time and money. The biggest reason for this is by bringing the backup and recovery process in line with actual requirements. It will also ensure a smooth recovery process in the event of a hard drive failure, virus attack or natural disaster.

Backup policies and procedures vary according to the needs of an organization and industry. There are certain elements of a data backup and restore process that every company should identify:

- **Determining What Files Should Be Backed Up:**

Before implementing a backup policy on a system, administrators should identify the important files for business activity. Data that helps run the business should be backed up. Data that including, financial information, tax information, personal employee information is important and should be backed up.

- **Determine Who Can Access Backups:**

Administrators should assign privileges to access backups to only those employees who work on the data. It is important to keep track of the backup data. Keep the backup logs updated regularly.

- **Determine How Often to Backup:**

An organization backup policy should define the backup schedule employees must use. Informing employees beforehand helps them prioritize their data for this requirement. The schedule should be created, considering the business of the organization and the severity of the data on the machines. It is not necessary to run a backup on everything at the same time. Certain files or databases have to be backed up at a different time. The backup policy should also mention the time the backups should run. Usually an organization prefers to perform backups after business hours. Based on the backup policy, the backup process can be initiated by administrators.

- **What Type of Backup is required?**

While drafting the backup policies and procedures, administrators should also determine the type of backup required. The type of backup depends on the organization's needs. The three basic types of backup include:

- **Full backups:** Performs a backup of all data. The simplest form of backup and a very time consuming process.
- **Incremental backups:** In this type of backup, the backup is created only when the data was changed since the last full backup. It is a less time-consuming process.
- **Differential backups:** It backs up all the selected files that are new and changed since the last full backup.

- **Where to Back Up Data:**

The backup policy should mention the location of the backup data and where it will be stored. Administrators can store the data on a physical external device, cloud or both.

It is important to test and evaluate all backup policies.

Confidential Data Policy

Confidential data policy defines **guidelines** for identifying an organization's confidential data and procedures to handle it

Design Considerations:

<ul style="list-style-type: none">● Treatment of confidential data including data storage, access, transmission, data sharing, disposal, handling and disclosure of data● Use of Confidential Data	<ul style="list-style-type: none">● Security controls for confidential data● Emergency access to the data
---	--

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

A confidential data policy is a set of information that requires a very high level of protection. It may consist of salary details, product details, organization structure details, etc. It is the responsibility of administrators to ensure the confidential data is secured from non-authorized access.

Drafting of a confidential data policy will help the organization protect the information, important to the existence of the business. The presence of a confidential data policy ensures users maintain the integrity and confidentiality of the business which will further help the overall growth of the business.

The slide has a yellow header bar with the title "Data Classification Policy" in white. In the top right corner is the CND logo (C|ND Certified Network Defender). The main content area is divided into two sections: a blue box on the left and a yellow box on the right. The blue box contains two bullet points about data classification policy. The yellow box is titled "Design Considerations:" and lists four items. At the bottom of the slide is a black footer bar with the copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

Data Classification Policy

Design Considerations:

- A data classification policy establishes a **framework** for classifying organizational data based on its level of sensitivity, value and criticality within the IT security policy
- The organization's data is classified into one of three sensitivity levels or classifications which are restricted, private and public

- Appropriate data classification by data owners
- Protecting data at rest
- Protecting data in transit
- Data labeling

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The data classification policy document aims to classify sensitive data and secure it as per its class. The implementation of a data classification policy helps the organization maintain and secure their data and resources. The classification of data and prioritizing its risk level depends on the organization. They can classify their data according to the user-requirement, security requirement or managerial requirement. The prioritization of the risk level can be restricted, confidential or public. The data classification policy should also include a list of users who can have access to the information.

Points to consider when developing a data classification policy:

- Employees should avoid distribution of any restricted or confidential data internally and externally.
- Authorized employees dealing with confidential data should send it only in an encrypted format through email.
- Administrators should have a secure backup of the data and monitor the backups regularly. The backups should have strong user credentials.
- After receiving the confidential data, an employee should scan the device or the file to avoid any malicious activity.
- If the authorized employee finds confidential data that is public, they should immediately delete the data (if possible).

- The document should mention the action taken against employees if they do not adhere to the policy.
- The organization should perform regular audits to ensure authorized employees are following the required measures.

Internet Usage Policy

Internet usage policy governs the way the organization's **internet connection** is used by every device on the network.

- Internet **usage limit** for official as well as personal use
- **Time frame** for personal use
- Method adoption for web usage **monitoring**
- **Levels of privacy** for employees
- **Restricted Content**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

An Internet usage policy informs employees about the rules which have to be followed while accessing the corporate Internet network. The implementation of such policies helps the organization maintain a secure network. Using an Internet policy keeps the systems secure and helps the user understand the types of risks a network can encounter. The policy should make employees aware that browsing prohibited sites or downloading files from unreliable sources can land them in trouble.

A small negligence from an employee or administrator end can lead to a major vulnerability in the network. The Internet usage policy must be accepted by all employees and it must be signed by them to acknowledge their understanding. Network administrators should (in consultation with top management) ensure the following facts:

1. **Limited usage:** Employees should be aware that the corporate Internet is used for official use only. Employees should refrain from using the Internet for their personal use. Example, downloading movies should not be allowed.
2. **Setting a timeframe for personal use:** If an organization plans to allow employees to use the Internet for personal purposes, it can set a timeframe for the use.
3. **The method to be adopted for monitoring web use:** Administrators should set monitoring standards to keep track of user activities on the Internet. These monitoring standards should follow the policies drafted in the document.
4. **Discuss and decide what content should be never allowed:** Administrators should discuss with top management and decide on a list of sites that should be denied or can be added to a list of non-trusted sites.

The infographic is titled "Server Policy" in large yellow text. It features a "Design Considerations:" section with three items: "Location and protection consideration for servers", "Configuration of servers", and "Monitoring of servers". Each item has a grey arrow pointing right next to it. The background has a decorative gradient bar at the bottom.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

- Server policy establishes a **standard** for the base configuration of an organization's server
- An effective server policy restricts unauthorized access to an organization's data and technology

Design Considerations:

- Location and protection consideration for servers
- Configuration of servers
- Monitoring of servers

A server policy is an internal organizational policy that defines the handling of server issues. It includes the details of installation, configuration, services required, etc. for the server. The policy document authorizes only its target audience - network/system administrators to have access to read it. The policy states administrators have the rights to perform deletions or modifications in a server. Following the policy, if any changes are made administrators are required to inform management or the users that will be affected by the changes.

The policy should cover the points that can help administrators rebuild the network or servers during a time of a disaster or calamity. With many troubleshooters available, the document reduces the troubleshooting time of the administrators.

For every server on a secure network, there are lists of items that must be documented and reviewed on a regular basis to keep a private network secure. The server list of information must be updated as new servers are added to the network and updated regularly.

1. Server name
2. Server location
3. The function or purpose of the server
4. Hardware components of the system, including the make and model of each part in the system
5. List of all software running on the server including the operating system, programs, and services

6. Configuration information about the server including:

- Event log settings
- A comprehensive list of services that are running
- Configuration of any security lockdown tool or setting
- Account settings

Responsibilities in enforcing general server policies are:

1. **User restriction:** Servers are the foundation of a functioning organization, administrators should not allow server access privileges to anyone in the organization except those who have been given permission by them.
2. **Configuration compliance:** At times, administrators may have to make changes to the configuration settings of a server. Such exceptions should be permissible. The changes should be monitored.
3. **Server registration:** Server registration should follow the corporate enterprise management system.
4. **Updating the corporate enterprise management system:** It is the responsibility of the administrator to update the corporate enterprise management system on a regular basis, this keeps the network and machines running smoothly.
5. **Parallelism in modifications:** Administrators should make sure that the configuration changes made on the server comply with the change management procedure.

The slide has a yellow header bar with the title "Wireless Network Policy". In the top right corner is the CND logo (C|ND Certified Network Defender). Below the title is a text box containing the definition of a wireless network policy. A blue callout box titled "Design Consideration" lists five items related to wireless network policy design. At the bottom of the slide is a copyright notice.

A wireless network policy states the **rule and regulations** for accessing an organization's wireless network resources

Design Consideration

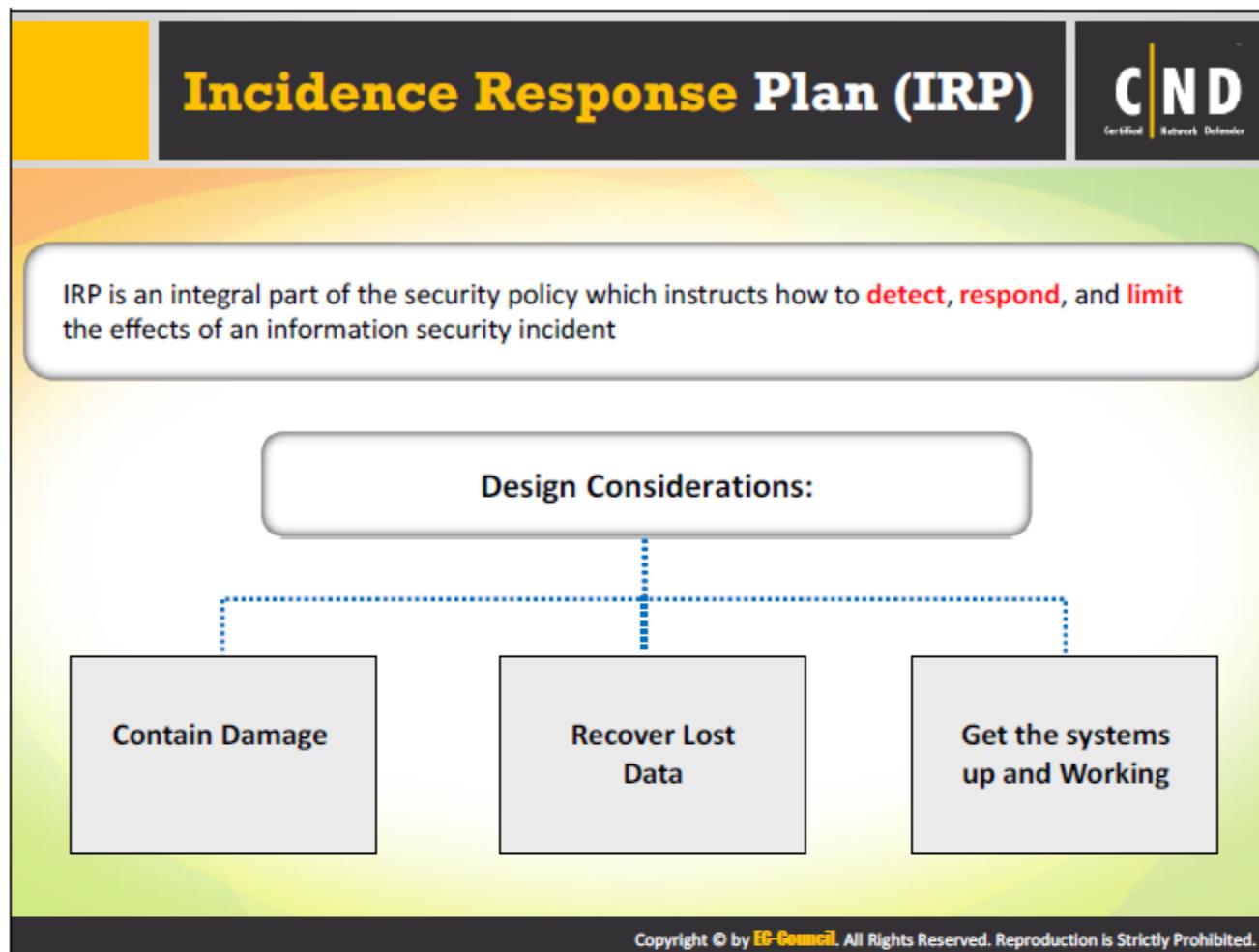
- ➊ Defining an **access point** for a WLAN
- ➋ **Placement** of an access point
- ➌ Technologies used for **wireless connectivity**
- ➍ Procedure **for integration** of a new system into the wireless environment
- ➎ Procedure for **monitoring** the network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Wireless Network policy is designed to protect organizational resources against intrusion from a wireless network. It applies to all wireless devices in use by the organization or those that connect through a wireless device to any organization network.

A network administrator's responsibilities in enforcing Wireless policies are:

1. **Access Point:** Administrator should provide a clear description of new established access points in the network. All access points must be registered and approved. They should be connected to the organizational network.
2. **Configuration:** Administrators should configure the SSID on all wireless devices so they do not reveal any information about the organization.
3. **Permissible devices:** The policy document should mention the type of devices that can be used to connect to the corporate wireless network. Only those devices that are approved by management should be connected to the network.
4. **Permissible technologies:** Administrators should define what technologies can be accessed through the wireless network.



An incident response plan (IRP) is a set of written instructions for detecting, responding to and limiting the effects of an information security event. Incident response plans provide instructions for responding to a number of potential scenarios, including data breaches, denial of service/distributed denial of service attacks, firewall breaches, virus or malware outbreaks or insider threats. Without an incident response plan in place, organizations may not detect the attack in the first place, or not follow proper protocol to contain the threat and quickly recover from it.

The design process of an IRP should concentrate on these aspects:

- To limit the ill effects of damage
- Recover lost data
- Get the systems up and working

Network administrator's responsibilities in designing an IRP are:

- Prepare an IRP as a preventive measure.
- Scan all log files on a daily basis to discover an attack in the earliest stage.
- After you detect an attack incident, immediately debrief your top officials.
- Follow the IRP steps and take appropriate actions to minimize the damage.
- Ensure the organization fully recovers from the attack.
- Take appropriate steps to prevent a similar kind of attack in the future.

The slide has a dark blue header with a yellow square on the left. The title "User Access Control Policy" is in white text on the right. In the top right corner is the "CND" logo with "Certified Network Defender" underneath. A callout box in the upper left contains the text: "User Access control policy gives an organization the ability to control, restrict, monitor, and protect corporate resource availability, integrity, and confidentiality". Below the title is a section titled "Design Considerations:" followed by a numbered list from 1 to 5. The numbers are in yellow boxes on the left, and the questions are in orange boxes on the right.

User Access Control Policy

Design Considerations:

- 1** Who can access (people, process, machines)?
- 2** What system resources can be accessed?
- 3** What files can be read?
- 4** What programs can be executed?
- 5** How to share data with other entities?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The access control policy provides a way to control the interaction between users, systems and resources. An access control policy helps an organization control, constrain and defend the resource availability of an organization.

The access control policy should define:

- Who can access (people, process, machines)?
- What system resources can be accessed?
- What files can be read?
- What programs can be executed?
- How to share data with other entities?

The policy should address the typical Access Control Practices such as:

- Undefined user or unknown account logins should be prohibited.
- Powerful accounts such as an administrator account must be monitored continuously.
- Lock access to accounts after crossing a limited number of unsuccessful login attempts.
- Remove unused accounts.
- Administer strict access criteria.
- Enforce the need-to-know and least-privilege practices.
- Disable unrequired system features and unused ports.
- Restrict global access rules.

Switch Security Policy

C|ND Certified Network Defender

Switch security policy describes a required **minimal security** configuration for the switches in the network

Design Considerations:

- Is the switch data **monitored** regularly?
- Are unnecessary **services** and **applications** blocked?
- Is all the stored passwords and sensitive data **encrypted** ?
- Is the switch located in a **restricted area**?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Switch security policy should be based on the following aspects:

1. **Monitor regularly:** The data in the switch should be monitored regularly for smooth network function.
2. **Services and applications:** It is not necessary to block all the services and applications of the switch device. Block the items which are not required and those which are known to be vulnerable.
3. **Encryption:** Administrators should encrypt all the stored data and passwords.
4. **Restricted area:** Physical storage of the switch should be in a restricted area.
5. **Configuring a L3 switch:** If an organization is using a L3 switch, it should be configured identical to the router policy.

A network administrator's switch policy responsibilities are:

1. **Enable Password:** You should always maintain the 'enable password' option. This helps to keep the switch in a secure encrypted form.
2. **Timeout periods:** Setting session timeout periods on the switch will not keep the switch busy, until the time a packet does not reach its destination.
3. **Privileges:** Privileges should be enabled on all levels of the switch.
4. **SSH:** Administrators should avoid using Telnet as a communication channel. SSH has proven to be more secure than Telnet. Use SSH with a strong password.

5. **Port security:** Port security limits the MAC based access. Enhancing the security of the switch. Limit MAC based access by implementing port security.
6. **Disable ports:** Ports that are not used by the switch should be disabled. Administrators can assign these ports to an unused VLAN number.
7. **Configure trunk ports:** Trunk ports carry traffic for all VLANs. A VLAN number that is not in use should handle the configuration of trunk ports.
8. **VLAN restrictions:** Use a static VLAN and limit the number of VLANs that can be transported over the trunk.
9. **AAA framework:** The Authentication, Authorization and Accounting framework includes the access of computer resources, implementation of policies, and provides information about services. AAA provides local and remote access to the switch.
10. **Switch Logs:** Set the switch to log data and then transfer it to a secure log host
11. **Disable the following if not in use:**
 - Cisco discovery protocol
 - Dynamic trunking
 - Scripting environments like TCL shell
12. **Encryption:** Enable Password-encryption and NTP configuration following the corporate standard.
13. **ACL:** ACL's to be configured following the organization hierarchy and requirements.
14. **Disable VTP:** If you are unable to disable VTP, then set VTP to management domain, password, and pruning. After performing the above steps set VTP to transparent mode.

Intrusion Detection and Prevention (IDS/IPS) Policy



The IDS and IPS policy facilitates **detection** and **prevention** of intrusion into the organization's network

Design Considerations:

- **Deployment** of a standard IDS system
- **Monitor** log files of an IDS continuously
- Regularly **update** the intruder's definition in the IDS logic for all evolving threats

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The policy of an IDS/IPS should facilitate the detection and prevention of intrusions in the organization's network.

The IDS and IPS policy design should include the following components:

1. **Deployment of a standard IDS system:** For a successful working IPS, administrators should deploy a standard IDS system across the network. The successful deployment of an IDS ensures threats will be detected and then prevented using the IPS standards.
2. **Monitor log files of an IDS continuously:** For monitoring the activity on a network continuously, administrators should actively audit and monitor the IDS.
3. **Regular update:** It is important for administrators to perform regular updates for the intruder's definitions in IDS logic as per evolving threats.
4. **Need of IPS:** It is advisable to deploy an IPS for large organizations. Deployment and implementation of an IPS ensures threats are detected using the same software as an IDS and prevents the networking using these prevention tools.

Encryption Policy



The encryption policy defines an **acceptable use and management** of encryption methods, techniques, and tools throughout an enterprise

The policy is **applicable to all enterprise network resources**, users(staff, stake holders etc.), internal network (LAN, Wi-Fi) and remote(WAN) connections

Design Considerations: It should define encryption standards that need to be used in an enterprise wired/wireless data communication, servers, desktops, laptops, smart phones, removable storage devices, USB memory sticks, VPN, Wi-Fi, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The encryption policy sets universal standards for organizations to facilitate data protection. It involves establishing business and technical strategies for accomplishing data security. The encryption policy determines the need for data encryption and the process of encrypting it.

The encryption policy is applicable to large and small organizations. It is applicable to but not limited to employees, partners, vendors, stakeholders, etc. It is necessary to understand every aspect of the policy to implement it further across the organization. The encryption policy defines the standards which can be deployed and implemented in electronic devices like servers, laptops, smart phones, removable devices, etc.

Encryption policies should be designed based on the following points:

- Encryption algorithm:** Once the encryption policy is approved by management, administrators should research the encryption algorithm which can be implemented in the infrastructure.
- Changes in hash functions:** You should change the hash functions of the selected algorithm, if required.
- Type of key:** As per the organization's requirement, administrators can use a symmetric or asymmetric key for encrypting the data.
- Verified certificates:** Before installing any certificate on the server, administrators should verify the authenticity of the certificates and its provider.
- SSL and TLS certificate:** Ensure the servers are using SSL and TLS and that both of these have a trusted certificate.

Router Policy

C|ND
Certified Network Defender

Router policy describes a required minimal security configuration for all routers in the network	Design Considerations: User authentication Access rules Placement Password management Services required/disallowed/blocked
---	--

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

An organization should establish router policies for the smooth functioning of the IT infrastructure.

The router policies should be designed based on following points:

- No local user account:** Routers must use TACACS user authentication. Administrators should not create local user accounts on the router.
- Encryption:** The security of the router can be done by setting up the 'enable secret password' on the router in a secure encrypted form.
- Corporate Management System:** All routers should be included in the corporate enterprise management system with a designated point of contact.
- Do not touch:** Administrators should place warnings such as, 'Do not touch' on the routers to avoid any mishandling by employees.
- Maintain standards:** Routers should comply with the standards outlined in the Router IOS Template.
- Non-usage of SNMP:** Administrators should use standardized corporate SNMP strings. They should avoid using public and private SNMP community strings.
- Login information:** Administrators should ensure every router saves system logging information to a local RAM buffer. The information should also be stored on "syslog" server.

8. **Configuration of VTY:** Virtual terminal (VTY) should be configured so it accepts connections for the required set of protocols only.
9. **Administrators should consider blocking the following services:**
 - Incoming packets with an invalid source address
 - Incoming packets with spoofed source addresses (i.e. company names)
 - TCP and UDP small services
 - Source routing
 - Web services running on the router
 - IP directed broadcasts
 - Cisco discovery protocol on all third party interfaces

Security Policy Training and Awareness



Advantages:

- Security Policy Training teaches employees how to **perform** their duties and to comply with the security policy
- Organizations should train new employees before granting them access to the network or provide limited access until the completion of their **training**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The security policy training and procedures are required to ensure the security and effective network management.

- The security policy training program helps employees appropriately recognize and respond to security threats in real time. The training teaches employees understand the importance of data on their devices or systems. Employees adapt themselves to secure computing habits.
- The security policy training provides new updates to employees with the awareness of probable vulnerabilities that can occur if they do not follow the policies.
- Security policy training and awareness helps minimize security breaches in the organization. Early identification of a breach decreases the cost to the organization.
- Security policy awareness among users helps notify them about new security policies, by publishing policy documentation and by developing descriptive security documentation for users, etc.
- Employees following the security policy correctly reduces potential fines or legal actions.
- An effective training program will help an employee monitor their computing behavior and inform their security concerns to management. The training will enhance the overall compliance with the company's security policies and procedures.

ISO Information Security Standards



Sr. No.	Standards	Objective
1	ISO/IEC 27001	Formal ISMS specification
2	ISO/IEC 27002	Information security controls
3	ISO/IEC 27003	ISMS implementation guide
4	ISO/IEC 27004	Information security metrics
5	ISO/IEC 27005	Information security risk management
6	ISO/IEC 27006	ISMS certification guide
7	ISO/IEC 27007	Management system auditing
8	ISO/IEC TR 27008	Technical auditing
9	ISO/IEC 27010	For inter-organisation communication
10	ISO/IEC 27011	Iso27k in telecoms

<http://www.iso27001security.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ISO Information Security Standards (Cont'd)



Sr. No.	Standards	Objective
11	ISO/IEC 27013	ISMS & ITIL/service management
12	ISO/IEC 27013	ISMS & ITIL/service management
13	ISO/IEC 27014	Information security governance
14	ISO/IEC TR27015	Iso27k in financial services
15	ISO/IEC TR 27016	Information security economics
16	ISO/IEC 27017	Cloud security controls
17	ISO/IEC 27018	Cloud privacy
18	ISO/IEC TR 27019	Process control in energy
19	ISO/IEC 27031	ICT business continuity
20	ISO/IEC 27032	Cybersecurity

<http://www.iso27001security.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ISO Information Security Standards (Cont'd)



Sr. No.	Standards	Objective
21	ISO/IEC 27033-1 to -5	Network security
22	ISO/IEC 27034-1 & -2	Application security
23	ISO/IEC 27035	Incident management
24	ISO/IEC 27036-1 -2 & -3	ICT supply chain
25	ISO/IEC 27037	Digital evidence [forensics]
26	ISO/IEC 27038	Document reduction
27	ISO/IEC 27039	Intrusion prevention
28	ISO/IEC 27040	Storage security
29	ISO/IEC 27041	Investigation assurance
30	ISO/IEC 27042	Analyzing digital evidence
31	ISO/IEC 27043	Incident investigation
32	ISO 27799 ISO27k	In healthcare

<http://www.iso27001security.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ISO/IEC 27001

Source: <http://www.iso27001security.com>

ISO/IEC 27001 formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks. The ISMS is an overarching management framework through which the organization identifies, analyzes and addresses its information security risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts - an important aspect in such a dynamic field, and a key advantage of ISO27k's flexible risk-driven approach as compared to, say, PCI-DSS.

ISO/IEC 27002

Source: <http://www.iso27001security.com>

ISO/IEC 27002, is relevant to all types of organizations, including commercial enterprises of all sizes (from one-man-bands up to multinational giants), not-for-profits, charities, government departments and quasi-autonomous bodies - in fact any organization that handles and depends on information. The specific information security risk and control requirements may differ in detail, but there is a lot of common ground, for instance, most organizations need to address the information security risks relating to their employees plus contractors, consultants and the external suppliers of information services.

ISO/IEC 27003

Source: <http://www.iso27001security.com>

ISO/IEC 27003 guides the design of an ISO/IEC 27001-compliant ISMS, leading up to the initiation of an ISMS implementation project. It describes the process of ISMS specification and design from inception to the production of implementation project plans, covering the preparation and planning activities *prior* to the actual implementation.

ISO/IEC 27004

Source: <http://www.iso27001security.com>

ISO/IEC 27004 concerns the measurements relating to information security management: these are commonly known as 'security metrics'.

ISO/IEC 27005

Source: <http://www.iso27001security.com>

The standard provides guidelines for information security risk management and supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

ISO/IEC 27006

Source: <http://www.iso27001security.com>

ISO/IEC 27006 is the **accreditation standard** that guides certification bodies on the formal processes they must follow when auditing their client's Information Security Management Systems (ISMSs) against ISO/IEC 27001 in order to certify or register them compliant. The accreditation processes laid out in the standard give assurance that ISO/IEC 27001 certificates issued by accredited organizations are valid.

ISO/IEC 27007

Source: <http://www.iso27001security.com>

ISO/IEC 27007 provides guidance for accredited certification bodies, internal auditors, external/third party auditors and others auditing ISMSs against ISO/IEC 27001 (*i.e.* auditing the *management system* for compliance with the standard).

ISO/IEC 27007 reflects and largely refers to ISO 19011, the ISO standard for auditing quality and environmental management systems - "management systems" of course being the common factor linking it to the ISO27k standards. It provides additional ISMS-specific guidance.

ISO/IEC TR 27008

Source: <http://www.iso27001security.com>

This standard provides guidance for all auditors regarding “information security management system controls” [sic] selected through a risk-based approach (e.g. as presented in a statement of applicability) for information security management. It supports the information security risk management process and internal, external and third party audits of ISMS by explaining the relationship between the ISMS and its supporting controls. It provides guidance on how to verify the extent to which required “ISMS controls” are implemented. Furthermore, it supports any organization using ISO/IEC 27001 and ISO/IEC 27002 to satisfy assurance requirements, and as a strategic platform for information security governance.

ISO/IEC 27010

Source: <http://www.iso27001security.com>

This standard provides guidance in relation to sharing information about information security risks, controls, issues and/or incidents that span the boundaries between industry sectors and/or nations, particularly those affecting “critical infrastructure”.

ISO/IEC 27011

Source: <http://www.iso27001security.com>

This ISMS implementation guide for the telecom industry was developed jointly by ITU-T and ISO/IEC JTC1/SC 27, with the identical text being published as *both* ITU-T X.1051 and ISO/IEC 27011.

ISO/IEC 27013

Source: <http://www.iso27001security.com>

This standard provides guidance on implementing an integrated information security and IT service management system, based on both ISO/IEC 27001:2005 (ISMS) and ISO/IEC 20000-1:2011.

ISO/IEC 27014

Source: <http://www.iso27001security.com>

ISO/IEC JTC1/SC 27, in collaboration with the ITU Telecommunication Standardization Sector (ITU-T), has developed a standard specifically aimed at helping organizations govern their information security arrangements.

ISO/IEC TR 27015

Source: <http://www.iso27001security.com>

This is a guideline intended to help financial services organizations (banks, insurance companies, credit card companies etc.) implement ISMSs using the ISO27k standards.

Although the financial services sector already labors under a vast swathe of risk and security standards (such as ISO TR 13569 “Banking Information Security Guidelines”, SOX and Basel II/III), the ISMS implementation guidance developed by SC 27 reflects ISO/IEC 27001 and 27002 along with various general-purpose security standards such as COBIT and the PCI-DSS requirements.

ISO/IEC TR 27016

Source: <http://www.iso27001security.com>

It helps management appreciate and understand the financial impacts of information security in the context of an ISO27k ISMS, along with political, social, compliance and other potential impacts on the organization that collectively influence how much it needs to invest in protecting its information assets.

ISO/IEC 27017

Source: <http://www.iso27001security.com>

This standard provides guidance on the information security aspects of cloud computing, recommending and assisting with the implementation of a cloud-specific information security controls supplementing the guidance in ISO/IEC 27002 and other ISO27k standards.

ISO/IEC 27018

Source: <http://www.iso27001security.com>

This standard provides guidance aimed at ensuring that cloud service providers (such as Amazon and Google) offer suitable information security controls to protect the privacy of their customer's clients by securing PII (Personally Identifiable Information) entrusted to them. The standard will be followed by ISO/IEC 27017 covering the wider information security angles of cloud computing, other than privacy.

ISO/IEC TR 27019

Source: <http://www.iso27001security.com>

This standard (a Technical Report) is intended to help organizations in “the energy industry” interpret and apply ISO/IEC 27002:2005 in order to secure their electronic process control systems.

ISO/IEC 27031

Source: <http://www.iso27001security.com>

ISO/IEC 27031 provides guidance on the concepts and principles behind the role of information and communications technology in ensuring business continuity.

The standard:

- Suggests a structure or framework (actually a set of methods and processes) for any organization – private, governmental, and non-governmental.
- Identifies and specifies all relevant aspects including performance criteria, design, and implementation details, for improving ICT readiness as part of the organization's ISMS, helping to ensure business continuity.
- Enables an organization to measure its ICT continuity, security and hence readiness to survive a disaster in a consistent and recognized manner.

ISO/IEC 27032

Source: <http://www.iso27001security.com>

ISO/IEC 27032 addresses “Cybersecurity” or “Cyberspace security”, defined as the “preservation of confidentiality, integrity and availability of information in the Cyberspace”. In turn “the Cyberspace” (complete with definite article) is defined as “the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form”.

ISO/IEC 27033-1 to -5

Source: <http://www.iso27001security.com>

ISO/IEC 27033 is a multi-part standard derived from the existing five-part network security standard ISO/IEC 18028. It is being substantially revised, not just renamed, to fit into the ISO27k suite.

ISO/IEC 27034 -1 & -5

Source: <http://www.iso27001security.com>

ISO/IEC 27034 offers guidance on information security to those specifying, designing and programming or procuring, implementing and using application systems, in other words business and IT managers, developers and auditors, and ultimately the end-users of ICT. The aim is to ensure that computer applications deliver the desired or necessary level of security in support of the organization's Information Security Management System, adequately addressing many ICT security risks.

ISO/IEC 27035

Source: <http://www.iso27001security.com>

Information security controls are imperfect in various ways: controls can be overwhelmed or undermined (e.g. by competent hackers, fraudsters or malware), fail in service (e.g. authentication failures), work partially or poorly (e.g. slow anomaly detection), or be more or less completely missing (e.g. not [yet] fully implemented, not [yet] fully operational, or never even conceived due to failures upstream in risk identification and analysis). Consequently, information security incidents are *bound* to occur to some extent, even in organizations that take their information security extremely seriously.

ISO/IEC 27036 -1 -2 & -3

Source: <http://www.iso27001security.com>

ISO/IEC 27036 is a multi-part standard offering guidance on the evaluation and treatment of information security risks involved in the acquisition of goods and services from suppliers. The implied context is business-to-business relationships, rather than retailing, and information-related products. The terms acquisition and acquirer are used rather than purchase and purchasing since the process and the risks are much the same whether or not the transactions are commercial.

ISO/IEC 27037

Source: <http://www.iso27001security.com>

This standard provides guidance on identifying, gathering/collecting/acquiring, handling and protecting/preserving digital forensic evidence i.e. "digital data that may be of evidential value" for use in court. The fundamental purpose of the ISO27k digital forensics standards is to promote best practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organizations and jurisdictions may well retain certain methods, processes and controls, it is hoped that standardization will (eventually) lead to the adoption of similar, if not identical approaches internationally, making it easier to compare, combine and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

ISO/IEC 27038

Source: <http://www.iso27001security.com>

Digital data sometimes have to be revealed to third parties, occasionally even published to the public, for reasons such as disclosure of official documents under Freedom of Information laws or as evidence in commercial disputes or legal cases. 'Redaction' is the conventional term for the process of denying file recipients' knowledge of certain sensitive data within the original files.

ISO/IEC 27039

Source: <http://www.iso27001security.com>

IDS (Intrusion Detection Systems) are largely automated systems for identifying attacks on and intrusions into a network or system by hackers and raising the alarm. IPS (Intrusion Prevention Systems) take the automation a step further by automatically responding to certain types of identified attack, for example by closing off specific network ports through a firewall to block identified hacker traffic. IDPS refers to either type.

ISO/IEC 27040

Source: <http://www.iso27001security.com>

The proposers of this standard felt that the information security aspects of data storage systems and infrastructures have been neglected due to misconceptions and limited familiarity with the storage technology, or in the case of [some] storage managers and administrators, a limited understanding of the inherent risks or basic security concepts.

ISO/IEC 27041

Source: <http://www.iso27001security.com>

The fundamental purpose of the ISO27k digital forensics standards is to promote best practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organizations and jurisdictions may well retain certain methods, processes and controls, it is hoped that standardization will (eventually) lead to the adoption of similar, if not identical approaches internationally, making it easier to compare, combine and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

ISO/IEC 27042

Source: <http://www.iso27001security.com>

The fundamental purpose of the ISO27k digital forensics standards is to promote best practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organizations and jurisdictions may well retain certain methods, processes and controls, it is hoped that standardization will (eventually) lead to the adoption of similar, if not identical approaches internationally, making it easier to compare, combine and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

ISO/IEC 27043

Source: <http://www.iso27001security.com>

The fundamental purpose of the digital forensics standards ISO/IEC 27037, 27041, 27042, 27043 and 27050 is to promote best practice methods and processes for forensic capture and investigation of digital evidence. While individual investigators, organizations and jurisdictions may well retain certain methods, processes and controls, it is hoped that standardization will (eventually) lead to the adoption of similar, if not identical approaches internationally, making

it easier to compare, combine and contrast the results of such investigations even when performed by different people or organizations and potentially across different jurisdictions.

ISO/IEC 27799

Source: <http://www.iso27001security.com>

This International Standard provides guidance to healthcare organizations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of such information by implementing ISO/IEC 27002. Specifically, this International Standard addresses the special information security management needs of the health sector and its unique operating environments. While the protection and security of personal information is important to all individuals, corporations, institutions and governments, there are special requirements in the health sector that need to be met to ensure the confidentiality, integrity, adaptability, and availability of personal health information.

ISO/IEC 27001:2013: Information Technology — Security Techniques — Information Security Management Systems — Requirements

CND
Certified Network Defender

- ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization
- It is intended to be suitable for several different types of use, including the following:

Use within organizations to formulate security requirements and objectives		Identification and clarification of existing information security management processes
Use within organizations as a way to ensure that security risks are cost effectively managed		Use by the management of organizations to determine the status of information security management activities
Use within organizations to ensure compliance		Implementation of business-enabling information security
Definition of new information security management processes		Used by organizations to provide relevant information about information security to customers

<http://www.iso.org>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ISO/IEC 27001:2013 (Cont'd)

CND
Certified Network Defender

ISO/IEC 27001:2013 specifies 114 controls in 14 groups and 35 control objectives

Sr. No.	Group	Control Objectives
01	A.5	Information security policies (2 controls)
02	A.6	Organization of information security (7 controls)
03	A.7	Human resource security - 6 controls that are applied before, during, or after employment
04	A.8	Asset management (10 controls)
05	A.9	Access control (14 controls)
06	A.10	Cryptography (2 controls)
07	A.11	Physical and environmental security (15 controls)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ISO/IEC 27001:2013 (Cont'd)



Sr. No.	Group	Control Objectives
08	A.12	Operations security (14 controls)
09	A.13	Communications security (7 controls)
10	A.14	System acquisition, development and maintenance (13 controls)
11	A.15	Supplier relationships (5 controls)
12	A.16	Information security incident management (7 controls)
13	A.17	Information security aspects of business continuity management (4 controls)
14	A.18	Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ISO/IEC 27001:2013 (Cont'd)



Structure of ISO/IEC 27001:2013

ISO/IEC 27001:2013 has **ten** short clauses:

1. Scope of the standard
2. How the document is referenced
3. Reuse of the terms and definitions in ISO/IEC 27000
4. Organizational context and stakeholders
5. Information security leadership and high-level support for policy
6. Planning an information security management system; risk assessment; risk treatment
7. Supporting an information security management system
8. Making an information security management system operational
9. Reviewing the system's performance
10. Corrective action

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

ISO/IEC 27001:2013 specifies 114 controls in 14 groups and 35 control objectives:

- A.5: Information security policies (2 controls)
- A.6: Organization of information security (7 controls)
- A.7: Human resource security - 6 controls that are applied before, during, or after employment
- A.8: Asset management (10 controls)
- A.9: Access control (14 controls)
- A.10: Cryptography (2 controls)
- A.11: Physical and environmental security (15 controls)
- A.12: Operations security (14 controls)
- A.13: Communications security (7 controls)
- A.14: System acquisition, development and maintenance (13 controls)
- A.15: Supplier relationships (5 controls)
- A.16: Information security incident management (7 controls)
- A.17: Information security aspects of business continuity management (4 controls)
- A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls)

ISO/IEC 27001:2013 has the following sections:

1. **Introduction:** The standard uses a process approach.
2. **Scope:** It specifies generic ISMS requirements suitable for organizations of any type, size or nature.
3. **Normative references:** Only ISO/IEC 27000 is considered essential to users of '27001: the remaining ISO27k standards are optional.
4. **Terms and definitions:** A brief, formalized glossary, soon to be superseded by ISO/IEC 27000.
5. **Context of the organization:** Understanding the organizational context, the needs and expectations of 'interested parties', and defining the scope of the ISMS. Section 4.4 states very plainly that "The organization shall establish, implement, maintain and continually improve" a compliant ISMS.

6. **Leadership:** Top management must demonstrate leadership and commitment to the ISMS, mandate policy, and assign information security roles, responsibilities and authorities.
7. **Planning:** Outlines the process to identify, analyze and plan to treat information security risks, and clarify the *objectives* of information security.
8. **Support:** Adequate, competent resources must be assigned, awareness raised, documentation prepared and controlled.
9. **Operation:** A bit more detail about assessing and treating information security risks, managing changes, and documenting things (partly so that they can be audited by the certification auditors).
10. **Performance evaluation:** Monitor, measure, analyze and evaluate/audit/review the information security controls, processes and management system in order to make systematic improvements where appropriate.
11. **Improvement:** Address the findings of audits and reviews (*e.g.* nonconformities and corrective actions); make continual refinements to the ISMS.

Source: <http://www.iso27001security.com>

ISO/IEC 27033: Information technology -- Security techniques -- Network security

1 ISO/IEC 27033-1:2015 provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security.

2 It provides a detailed **vocabulary** of terms associated with information security and networking

3 It addresses issues regarding **implementation** and **operating** of network security controls and even the current monitoring and review process

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The purpose of ISO/IEC 27033 is to provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their interconnections. Those individuals within an organization that are responsible for information security in general, and network security in particular, should be able to adapt the material in this standard to meet their specific requirements.” [quoted from the introduction to 27033-1].

ISO/IEC 27033 provides detailed guidance on implementing the network security controls that are introduced in ISO/IEC 27002. It applies to the security of networked devices and the management of their security, network applications/services and users of the network, in addition to the security of information being transferred through communications links. It is aimed at network security architects, designers, managers and officers.

Source: <http://www.iso27001security.com>

Payment Card Industry Data Security Standard (PCI-DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards.

PCI DSS applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data.

High level overview of the PCI DSS requirements developed and maintained by Payment Card Industry (PCI) Security Standards Council:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	Implement Strong Access Control Measures
Protect Cardholder Data	Regularly Monitor and Test Networks
Maintain a Vulnerability Management Program	Maintain an Information Security Policy

<https://www.pcisecuritystandards.org>

Failure to meet the PCI DSS requirements may result in fines or termination of payment card processing privileges

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. This standard offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements, and support resources to help organizations ensure the safe handling of cardholder information. PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data. PCI DSS comprises a minimum set of requirements for protecting cardholder data. High-level overview of the PCI DSS requirements developed and maintained by the Payment Card Industry (PCI) Security Standards Council.

Source: <https://www.pcisecuritystandards.org>

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA's Administrative Simplification Statute and Rules

Electronic Transaction and Code Sets Standards		Requires every provider who does business electronically to use the same health care transactions, code sets, and identifiers
Privacy Rule		Provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information
Security Rule		Specifies a series of administrative, physical, and technical safeguards for covered entities to use and assure the confidentiality, integrity, and availability of electronic protected health information
National Identifier Requirements		Requires that health care providers, health plans, and employers have standard national numbers that identify them on standard transactions
Enforcement Rule		Provides standards for enforcing all the Administration Simplification Rules

<http://www.hhs.gov>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule permits the disclosure of health information needed for patient care and other important purposes. The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to assure the confidentiality, integrity, and availability of electronic protected health information.

The office of civil rights implemented HIPAA's Administrative Simplification Statute and Rules, as discussed below:

- **Electronic Transaction and Code Sets Standards**

Transactions are electronic exchanges involving the transfer of information between two parties for specific purposes. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) named certain types of organizations as covered entities, including health plans, health care clearinghouses, and certain health care providers. In the HIPAA regulations, the Secretary of Health and Human Services (HHS) adopted certain standard transactions for Electronic Data Interchange (EDI) of health care data. These transactions are claims and encounter information, payment and remittance advice, claim status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits and premium payment. Under HIPAA, if a covered entity conducts one of the adopted transactions electronically, they must use the adopted standard—either from

ASC X12N or NCPDP (for certain pharmacy transactions). Covered entities must adhere to the content and format requirements of each transaction.

- **Privacy Rule**

The HIPAA Privacy Rule establishes national standards to protect individual's medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patient's rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

- **Security Rule**

The HIPAA Security Rule establishes national standards to protect individual's electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

- **Employer Identifier Standard**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that employers have standard national numbers that identify them on standard transactions.

- **National Provider Identifier Standard (NPI)**

The National Provider Identifier (NPI) is a Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Standard. The NPI is a unique identification number for covered health care providers. Covered health care providers and all health plans and health care clearinghouses must use the NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a 10-position, intelligence-free numeric identifier (10-digit number). This means that the numbers do not carry other information about healthcare providers, such as the state in which they live or their medical specialty.

- **Enforcement Rule**

The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.

Source: <http://www.hhs.gov>

Information Security Acts: Sarbanes Oxley Act (SOX)

C|ND
Certified Network Defender

- Sarbanes–Oxley is a United States federal law that sets new or enhanced standards for all US public company **boards, management, and accounting firms**.
- The rules and enforcement policies outlined by the SOX Act amend or supplement existing legislation dealing with **security regulations**.

Section 302

- A mandate that requires senior management to certify the accuracy of the reported financial statement
- CEOs and CFOs of accounting company's clients must sign statements verifying the completeness and accuracy of the financial reports

Section 404

- A requirement that management and auditors establish internal controls and reporting methods on the adequacy of those controls
- CEOs, CFOs, and auditors must report on, and attest to the effectiveness of internal controls for financial reporting

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Enacted in 2002, the Sarbanes-Oxley Act aims to protect investors and the public by increasing the accuracy and reliability of corporate disclosures. This act does not explain how an organization needs to store records, but describes records that organizations need to store and the duration of the storage. The Act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud.

Key requirements and provisions of SOX are organized into 11 titles:

- Title I: Public Company Accounting Oversight Board (PCAOB)**

Title I consists of nine sections and establishes the Public Company Accounting Oversight Board, to provide independent oversight of public accounting firms providing audit services ("auditors"). It also creates a central oversight board tasked with registering audit services, defining the specific processes and procedures for compliance audits, inspecting and policing conduct and quality control, and enforcing compliance with the specific mandates of SOX.

- Title II: Auditor Independence**

Title II consists of nine sections and establishes standards for external auditor independence, to limit conflicts of interest. It also addresses new auditor approval requirements, audit partner rotation, and auditor reporting requirements. It restricts auditing companies from providing non-audit services (e.g., consulting) for the same clients.

- **Title III: Corporate Responsibility**

Title III consists of eight sections and mandates that senior executives take individual responsibility for the accuracy and completeness of corporate financial reports. It defines the interaction of external auditors and corporate audit committees, and specifies the responsibility of corporate officers for the accuracy and validity of corporate financial reports. It enumerates specific limits on the behaviors of corporate officers and describes specific forfeitures of benefits and civil penalties for non-compliance.

- **Title IV: Enhanced Financial Disclosures**

Title IV consists of nine sections. It describes enhanced reporting requirements for financial transactions, including off-balance-sheet transactions, pro-forma figures and stock transactions of corporate officers. It requires internal controls for assuring the accuracy of financial reports and disclosures, and mandates both audits and reports on those controls. It also requires timely reporting of material changes in financial condition and specific enhanced reviews by the SEC or its agents of corporate reports.

- **Title V: Analyst Conflicts of Interest**

Title V consists of only one section, which includes measures designed to help restore investor confidence in the reporting of securities analysts. It defines the codes of conduct for securities analysts and requires disclosure of knowable conflicts of interest.

- **Title VI: Commission Resources and Authority**

Title VI consists of four sections and defines practices to restore investor confidence in securities analysts. It also defines the SEC's authority to censure or bar securities professionals from practice and defines conditions to bar a person from practicing as a broker, advisor, or dealer.

Given below is the continuation of SOX titles:

- **Title VII: Studies and Reports**

Title VII consists of five sections and requires the Comptroller General and the Securities and Exchange Commission (SEC) to perform various studies and report their findings. Studies and reports include the effects of consolidation of public accounting firms, the role of credit rating agencies in the operation of securities markets, securities violations, and enforcement actions, and whether investment banks assisted Enron, Global Crossing, and others to manipulate earnings and obfuscate true financial conditions.

- **Title VIII: Corporate and Criminal Fraud Accountability**

Title VIII, also known as the "Corporate and Criminal Fraud Accountability Act of 2002," consists of seven sections. It describes specific criminal penalties for manipulation, destruction, or alteration of financial records or other interference with investigations, while providing certain protections for whistle-blowers.

- **Title IX: White-Collar-Crime Penalty Enhancement**

Title IX, also known as the "**White Collar Crime Penalty Enhancement Act of 2002**," consists of six sections. This title increases the criminal penalties associated with white-collar crimes and conspiracies. It recommends stronger sentencing guidelines and specifically adds failure to certify corporate financial reports as a criminal offense.

- **Title X: Corporate Tax Returns**

Title X consists of one section and states that the Chief Executive Officer should sign the company tax return.

- **Title XI: Corporate Fraud Accountability**

Title XI consists of seven sections. Section 1101 recommends the following name for this title: "**Corporate Fraud Accountability Act of 2002**." It identifies corporate fraud and records tampering as criminal offenses and joins those offenses to specific penalties. It also revises sentencing guidelines and strengthens their penalties. This enables the SEC to resort to temporarily freeze "large" or "unusual" transactions or payments.

Source: www.soxlaw.com

Information Security Acts: Gramm-Leach-Bliley Act (GLBA)



- The objective of the **Gramm-Leach-Bliley Act** was to ease the transfer of **financial** information between **institutions** and **banks** while making the rights of the individual through **security** requirements more specific.



Key Points Include:

- Protecting consumer's **personal financial information** held by financial institutions and their service providers
- The officers and directors of the financial institution shall be subject to, and personally liable for, a civil penalty of not more than **\$10,000 for each violation**



Although the **penalty** is small, it is easy to see how it could impact a **bank**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

Source: <https://www.ftc.gov>

Information Security Acts: The Digital Millennium Copyright Act (DMCA) and Federal Information Security Management Act (FISMA)



The Digital Millennium Copyright Act (DMCA)

- The DMCA is a United States copyright law that implements two 1996 treaties of the **World Intellectual Property Organization** (WIPO).
- It defines **legal prohibitions** against the circumvention of technological protection measures employed by copyright owners to protect their works, and against the **removal** or **alteration** of copyright management information.



<http://www.copyright.gov>

Federal Information Security Management Act (FISMA)

- The FISMA provides a comprehensive framework for ensuring the **effectiveness of information security controls** over information resources that support Federal operations and assets.
- It includes
 - Standards for **categorizing** information and information systems by mission impact
 - Standards for minimum **security requirements** for information and information systems
 - Guidance for selecting appropriate **security controls** for information systems
 - Guidance for **assessing security controls** in information systems and determining security control effectiveness
 - Guidance for the security authorization of information systems

<http://csrc.nist.gov>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Digital Millennium Copyright Act (DMCA)

The DMCA is a United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. It defines legal prohibitions against circumvention of technological protection measures employed by copyright owners to protect their works, and against the removal or alteration of copyright management information in order to implement US treaty obligations. The DMCA contains five titles:

▪ Title I: WIPO TREATY IMPLEMENTATION

Title I implements the WIPO treaties. First, it makes certain technical amendments to US law, in order to provide appropriate references and links to the treaties. Second, it creates two new prohibitions in Title 17 of the U.S. Code—one on circumvention of technological measures used by copyright owners to protect their works and one on tampering with copyright management information—and adds civil remedies and criminal penalties for violating the prohibitions.

▪ Title II: ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION

Title II of the DMCA adds a new section 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. The limitations are based on the following four categories of conduct by a service provider:

- Transitory communications

- System caching
- Storage of information on systems or networks at direction of users
- Information location tools

New section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions.

- **Title III: COMPUTER MAINTENANCE OR REPAIR**

Title III of the DMCA allows the owner of a copy of a program to make reproductions or adaptations when necessary to use the program in conjunction with a computer. The amendment permits the owner or lessee of a computer to make or authorize the making of a copy of a computer program in the course of maintaining or repairing that computer.

- **Title IV: MISCELLANEOUS PROVISIONS**

Title IV contains six miscellaneous provisions, where the first provision provides Clarification of the Authority of the Copyright Office. The second provision grants exemption for the making of "ephemeral recordings". The third provision promotes the distance education study. The fourth provision provides exemption for Nonprofit Libraries and Archives. The fifth provision allows Webcasting Amendments to the Digital Performance Right in Sound Recordings, and the sixth provision addresses concerns about the ability of writers, directors and screen actors to obtain residual payments for the exploitation of motion pictures in situations in which the producer is no longer able to make these payments.

- **Title V: PROTECTION OF CERTAIN ORIGINAL DESIGNS**

Title V of the DMCA, entitles the Vessel Hull Design Protection Act (VHDPA). It creates a new system for protecting original designs of certain useful articles that make the article attractive or distinctive in appearance. For purposes of the VHDPA, "useful articles" are limited to the hulls (including the decks) of vessels no longer than 200 feet.

Federal Information Security Management Act (FISMA)

FISMA is the Federal Information Security Management Act of 2002 to produce several key security standards and guidelines required by Congressional legislation. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Source: <http://www.copyright.gov>, Source: <http://csrc.nist.gov>

Other Information Security Acts and Laws

The grid contains the following information:

1 USA Patriot Act 2001	5 The Audit Investigation and Community Enterprise Act 2005
2 The Data Protection Act 1998	6 The Human Rights Act 1998
3 Freedom of Information Act (FOIA)	7 The Freedom of Information Act 2000
4 The Electronic Communications Privacy Act	8 Computer Fraud and Abuse Act

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

USA Patriot Act 2001

Source: <https://www.fincen.gov>

The purpose of the USA PATRIOT Act is to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and other purposes, some of which include:

- To strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorism
- To subject to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts that are susceptible to criminal abuse
- To require all appropriate elements of the financial services industry to report potential money laundering
- To strengthen measures to prevent use of the U.S. financial system for personal gain by corrupt foreign officials and facilitate repatriation of stolen assets to the citizens of countries to whom such assets belong.

The Data Protection Act 1998

Source: <https://www.gov.uk>

The Data Protection Act controls how your personal information is used by organizations, businesses or the government. Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights kept safe and secure
- not transferred outside the European Economic Area without adequate protection

Freedom of Information Act (FOIA)

Source: <http://www.foia.gov>

The Freedom of Information Act (FOIA) has provided the public the right to request access to records from any federal agency. It is often described as the law that keeps citizens in the know about their government. Federal agencies are required to disclose any information requested under the FOIA unless it falls under one of nine exemptions, which protect interests such as personal privacy, national security, and law enforcement.

The Electronic Communications Privacy Act

Source: <https://it.ojp.gov>

The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986. The ECPA updated the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone lines, but did not apply to interception of computer and other digital and electronic communications. Several subsequent pieces of legislation, including The USA PATRIOT Act, clarify and update the ECPA to keep pace with the evolution of new communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases.

The Audit Investigation and Community Enterprise Act 2005

Source: <http://www.legislation.gov.uk>

An Act to amend the law relating to company auditors and accounts, to the provision that may be made in respect of certain liabilities incurred by a company's officers, and to company investigations; to make provision for community interest companies; and for connected purposes.

The Human Rights Act 1998

Source: <http://www.legislation.gov.uk>

An Act to give further effect to rights and freedoms guaranteed under the European Convention on Human Rights; to make provision with respect to holders of certain judicial offices who become judges of the European Court of Human Rights; and for connected purposes.

The Freedom of Information Act 2000

Source: <http://www.legislation.gov.uk>

An Act to make provision for the disclosure of information held by public authorities or by persons providing services for them and to amend the Data Protection Act 1998 and the Public Records Act 1958; and for connected purposes.

Computer Fraud and Abuse Act

Source: <https://ilt.eff.org>

The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, is an amendment made in 1986 to the Counterfeit Access Device and Abuse Act that was passed in 1984 and essentially states that, whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer if the conduct involved an interstate or foreign communication shall be punished under the Act. In 1996 the CFAA was, again, broadened by an amendment that replaced the term "federal interest computer" with the term "protected computer."18 U.S.C. § 1030. While the CFAA is primarily a criminal law intended to reduce the instances of malicious interferences with computer systems and to address federal computer offenses, an amendment in 1994 allows civil actions to bring under the statute, as well.

Cyber Law in Different Countries



Country Name

Country Name	Laws/Acts	Website
United States	Section 107 of the Copyright Law mentions the doctrine of "fair use"	http://www.copyright.gov
	Online Copyright Infringement Liability Limitation Act	
	The Lanham (Trademark) Act (15 USC §§ 1051 - 1127)	http://www.uspto.gov
	The Electronic Communications Privacy Act	https://www.fas.org
	Foreign Intelligence Surveillance Act	https://www.fas.org
	Protect America Act of 2007	http://www.justice.gov
	Privacy Act of 1974	http://www.justice.gov
	National Information Infrastructure Protection Act of 1996	http://www.nrotc.navy.mil
	Computer Security Act of 1987	http://csrc.nist.gov
	Federal Information Security Management Act (FISMA)	http://csrc.nist.gov
The Digital Millennium Copyright Act (DMCA)	http://www.copyright.gov	
Sarbanes Oxley Act (SOX)	https://www.sec.gov	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Law in Different Countries (Cont'd)



Country Name

Country Name	Laws/Acts	Website
Australia	The Trade Marks Act 1995	
	The Patents Act 1990	
	The Copyright Act 1968	
	Cybercrime Act 2001	http://www.comlaw.gov.au
United Kingdom	The Copyright, Etc. and Trademarks (Offenses And Enforcement) Act 2002	
	Trademarks Act 1994 (TMA)	http://www.legislation.gov.uk
	Computer Misuse Act 1990	
China	Copyright Law of People's Republic of China (Amendments on October 27, 2001)	http://www.npc.gov.cn
	Trademark Law of the People's Republic of China (Amendments on October 27, 2001)	http://www.saic.gov.cn
India	The Patents (Amendment) Act, 1999, Trade Marks Act, 1999, The Copyright Act, 1957	http://www.ipindia.nic.in
	Information Technology Act	http://www.dot.gov.in
Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	http://www.cybercrimelaw.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cyber Law in Different Countries (Cont'd)



Country Name	Laws/Acts	Website
Italy	Penal Code Article 615 ter	http://www.cybercrimelaw.net
Japan	The Trademark Law (Law No. 127 of 1957), Copyright Management Business Law (4.2.2.3 of 2000)	http://www.iip.or.jp
Canada	Copyright Act (R.S.C., 1985, c. C-42), Trademark Law, Canadian Criminal Code Section 342.1	http://www.laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	http://www.statutes.agc.gov.sg
South Africa	Trademarks Act 194 of 1993 Copyright Act of 1978	http://www.cipc.co.za http://www.nlsa.ac.za
South Korea	Copyright Law Act No. 3916 Industrial Design Protection Act	http://home.heinonline.org http://www.kipo.go.kr
Belgium	Copyright Law, 30/06/1994 Computer Hacking	http://www.wipo.int http://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	http://www.mosstingrett.no
Hong Kong	Article 139 of the Basic Law	http://www.basiclaw.gov.hk

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary



- Security policies outline constraints using rules and regulations concerning every aspect of an organization's network security
- The security policy is an integral part of the Information Security Management Program for organizations
- Security Policy Training and Awareness is required for effective implementation of security policies

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

In this module, you have learned the various aspects of security policies such as the role of security policies, its characteristics, policy content, policy statement, types of information security policy, etc.

Through design considerations, the module also provided guidance on how to design a policy statement for various types of security policies for your organization. The module also taught you the various laws and standards that you may need to comply with.