Security Essentials

Introduction

Generally, basic computer security focuses on protecting computer systems from unauthorized access and use. For your own personal computer security, this can include steps like installing antivirus software, using a password generator and protecting the data you share online.

Microsoft Security Essentials (MSE) is an antivirus software (AV) product that provides protection against different types of malicious software, such as computer viruses, spyware, rootkits, and Trojan horses.

What Is Information Security?

InfoSec, or information security, is a set of tools and practices that you can use to protect your digital and analog information. InfoSec covers a range of IT domains, including infrastructure and network security, auditing, and testing. It uses tools like authentication and permissions to restrict unauthorized users from accessing private information. These measures help you prevent harms related to information theft, modification, or loss.

Information Security vs Cybersecurity

Although both security strategies, cybersecurity and information security cover different objectives and scopes with some overlap. Information security is a broader category of protections, covering cryptography, mobile computing, and social media. It is related to information assurance, used to protect information from non-person-based threats, such as server failures or natural disasters. In comparison, cybersecurity only covers Internet-based threats and digital data. Additionally, cybersecurity provides coverage for raw, unclassified data while information security does not.

Confidentiality, Integrity and Availability (CIA Triad)

The CIA triad consists of three core principles – confidentiality, integrity, and availability (CIA). Together, these principles serve as the foundation that guides information security policies. Here is a brief overview of each principle:

Confidentiality – information must only be available to authorized parties.

Integrity – information must remain consistent, trustworthy, and accurate.

Availability – information must remain accessible to authorized parties, even during failures (with minimal or no disruption).

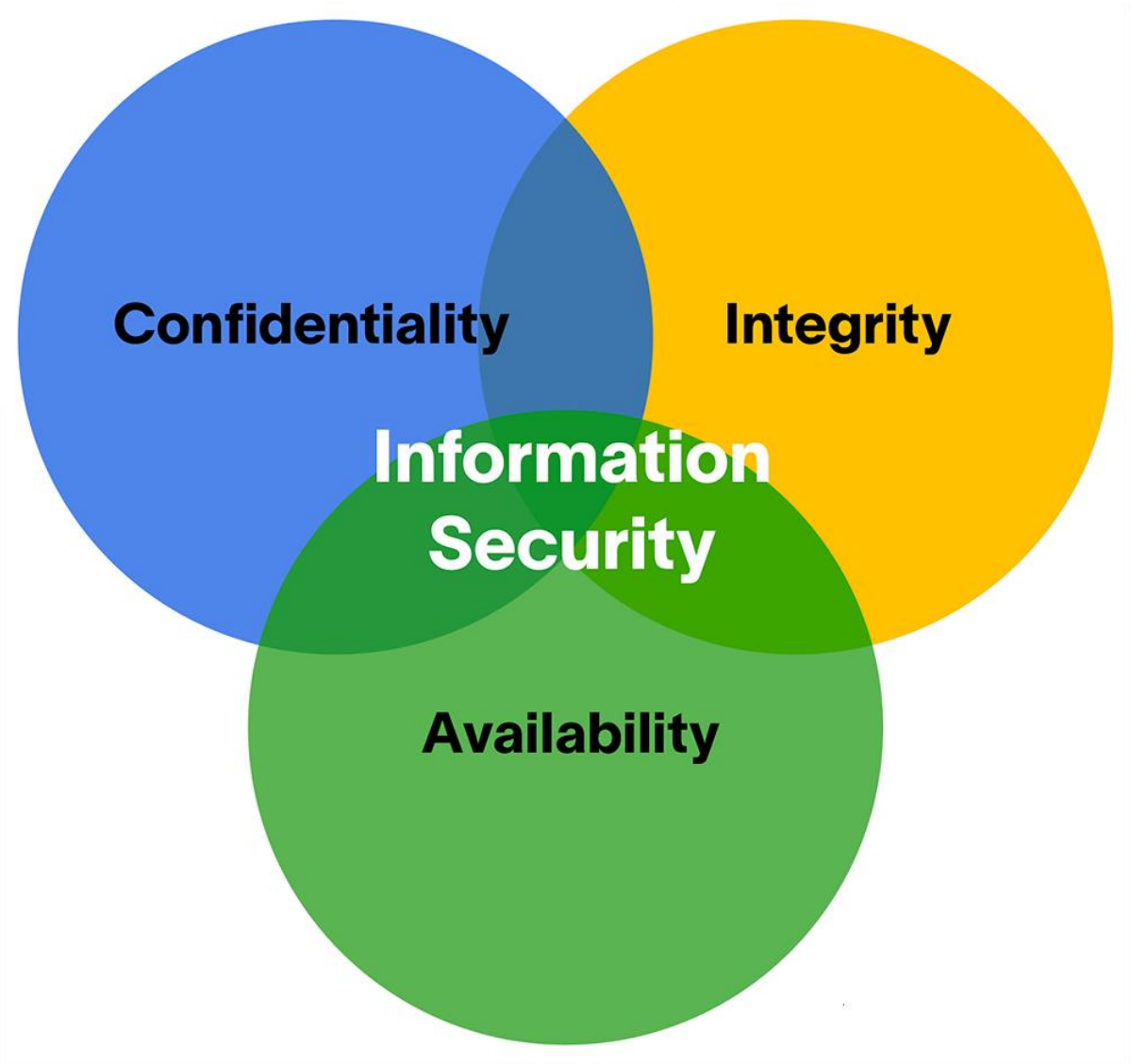
Ideally, information security policies should seamlessly integrate all three principles of the CIA triad. Together, the three principles should guide organizations while assessing new technologies and scenarios.

What is an information security policy?

Security threats are constantly evolving, and compliance requirements are becoming increasingly complex. Organizations must create a comprehensive information security policy to cover both challenges. An information security policy makes it possible to coordinate and enforce a security program and communicate security measures to third parties and external auditors.

To be effective, an information security policy should:

- Cover end-to-end security processes across the organization
- Be enforceable and practical
- Be regularly updated in response to business needs and evolving threats
- Be focused on the business goals of your organization



The importance of an information security policy
Information security policies can have the following benefits for an organization:

- **Facilitates data integrity, availability, and confidentiality** —Effective information security policies standardize rules and processes that protect against vectors threatening data integrity, availability, and confidentiality.
- **Protects sensitive data** — Information security policies prioritize the protection of intellectual property and sensitive data such as personally identifiable information (PII).

- **Minimizes the risk of security incidents** — An information security policy helps organizations define procedures for identifying and mitigating vulnerabilities and risks. It also details quick responses to minimize damage during a security incident.
- **Executes security programs across the organization** — Information security policies provide the framework for operationalizing procedures.
- **Provides a clear security statement to third parties** — Information security policies summarize the organization's security posture and explain how the organization protects IT resources and assets. They facilitate quick response to third-party requests for information by customers, partners, and auditors.
- **Helps comply with regulatory requirements** — Creating an information security policy can help organizations identify security gaps related to regulatory requirements and address them.

12 Elements of an Information Security Policy

A security policy can be as broad as you want it to be, from everything related to IT security and the security of related physical assets, but enforceable in its full scope. The following list offers some important considerations when developing an information security policy.

1. Purpose

First state the purpose of the policy, which may be to:

Create an overall approach to information security., especially as touches standards, security requirements, and best practices adopted by the organization.

Detect and pre-empt information security breaches such as misuse of networks, data, applications, and computer systems.

Maintain the reputation of the organization, and uphold ethical and legal responsibilities and applicable governance.

Respect employee and customer rights, including how to react to inquiries and complaints about non-compliance.

2. Audience

Define the audience to whom the information security policy applies. You may also specify which audiences are out of the scope of the policy (for example, staff in another business unit which manages security separately may not be in the scope of the policy).

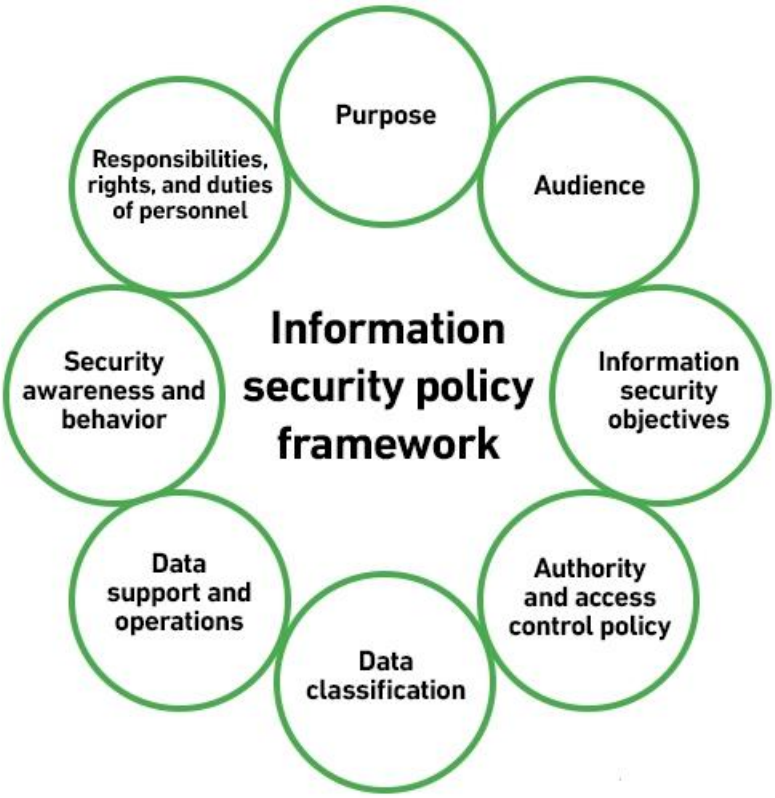
3. Information security objectives

Guide your management team to agree on well-defined objectives for strategy and security. Information security focuses on three main objectives:

Confidentiality — Only authenticated and authorized individuals can access data and information assets.

Integrity — Data should be intact, accurate and complete, and IT systems must be kept operational.

Availability — Users should be able to access information or systems when needed.



4. Authority and access control policy

Hierarchical pattern — A senior manager may have the authority to decide what data can be shared and with whom. The security policy may have different terms for a senior manager vs. a junior employee or contractor. The policy should outline the level of authority over data and IT systems for each organizational role.

Network security policy — Critical patching and other threat mitigation policies are approved and enforced. Users are only able to access company networks and servers via unique logins that demand authentication, including passwords, biometrics, ID cards, or tokens. You should monitor all systems and record all login attempts.

5. Data classification

The policy should classify data into categories, which may include “top secret,” “secret,” “confidential,” and “public.” The objectives for classifying data are:

To understand which systems and which operations and applications touch on the most sensitive and controlled data, to properly design security controls for that hardware and software.

To ensure that sensitive data cannot be accessed by individuals with lower clearance levels

To protect highly important data, and avoid needless security measures for unimportant data

6. Data support and operations

Data protection regulations — systems that store personal data, or other sensitive data — must be protected according to organizational standards, best practices, industry compliance standards, and relevant regulations. Most security standards require, at a minimum, encryption, a firewall, and anti-malware protection.

Data backup — Encrypt data backup according to industry best practices, both in motion and at rest. Securely store backup media, or move backup to secure cloud storage.

Movement of data — Only transfer data via secure protocols. Encrypt any information copied to portable devices or transmitted across a public network.

7. Security awareness and behaviour

Share IT security policies with your staff. Conduct training sessions to inform employees of your security procedures and mechanisms, including data protection measures, access protection measures, and sensitive data classification.

Social engineering — Place a special emphasis on the dangers of social engineering attacks (such as phishing emails or informational requests via phone calls). Make all employees responsible for noticing, preventing, and reporting such attacks.

Clean desk policy — Secure laptops with a cable lock. Shred sensitive documents that are no longer needed. Keep printer areas clean so documents do not fall into the wrong hands.

Work with HR to define how the internet should be restricted both on work premises and for remote employees using organizational assets. Do you allow YouTube, social media websites, etc.? Block unwanted websites using a proxy.

8. Encryption policy

Encryption involves encoding data to keep it inaccessible to or hidden from unauthorized parties. It helps protect data stored at rest and in transit between locations and ensure that sensitive, private, and proprietary data remains private. It can also improve the security of client-server communication. An encryption policy helps organizations define:

The devices and media the organization must encrypt

When encryption is mandatory

The minimum standards applicable to the chosen encryption software

9. Data backup policy

A data backup policy defines rules and procedures for making backup copies of data. It is an integral component of overall data protection, business continuity, and disaster recovery strategy. Here are key functions of a data backup policy:

Identifies all information the organization needs to back up

Determines the frequency of backups, for example, when to perform an initial full backup and when to run incremental backups

Defines a storage location holding backup data

Lists all roles in charge of backup processes, for example, a backup administrator and members of the IT team

10. Responsibilities, rights, and duties of personnel

Appoint staff to carry out user access reviews, education, change management, incident management, implementation, and periodic updates of the security policy. Responsibilities should be clearly defined as part of the security policy.

11. System hardening benchmarks

The information security policy should reference security benchmarks the organization will use to harden mission-critical systems, such as the Center for Information Security (CIS) benchmarks for Linux, Windows Server, AWS, and Kubernetes.

12. References to regulations and compliance standards

The information security policy should reference regulations and compliance standards that impact the organization, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Payment Card Industry Data Security Standard (PCI DSS), the Sarbanes-Oxley Act (SOX), and the Health Insurance Portability and Accountability Act (HIPAA).

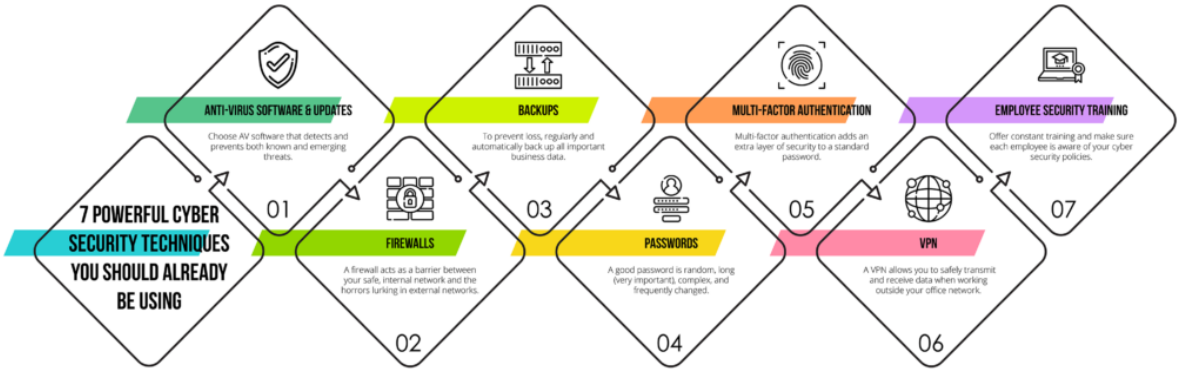
9 Best Practices for Successful Information Security Policies

1. **Information and data classification** — helps an organization understand the value of its data, determine whether the data is at risk, and implement controls to mitigate risks
2. **Developers, security, and IT operations** — should work together to meet compliance and security requirements. Lack of cooperation between departments may lead to configuration errors. Teams that work together in a DevSecOps model can coordinate risk assessment and identification throughout the software development lifecycle to reduce risks.
3. **Security incident response plan** — helps initiate appropriate remediation actions during security incidents. A security incident strategy provides a guideline, which includes initial threat response, priorities identification, and appropriate fixes.
4. **SaaS and cloud policy** — provides the organization with clear cloud and SaaS adoption guidelines, which can provide the foundation for a unified cloud ecosystem and standards of configuration, especially for development environments. This policy can help mitigate ineffective complications and poor use of cloud resources.
5. **Acceptable use policies (AUPs)** — helps prevent data breaches that occur through misuse of company resources. Transparent AUPs help keep all personnel in line with the proper use of company technology resources.
6. **Identity and access management (IAM) regulations** — let IT administrators authorize systems and applications to the right individuals and let employees know how to use and create passwords in a secure way. A simple password policy can reduce identity and access risks.
7. **Data security policy** — outlines the technical operations of the organization and acceptable use standards in accordance with all applicable governance and compliance regulations.
8. **Privacy regulations** — government-enforced regulations such as GDPR and CCPA protect the privacy of end users. Organizations that don't protect the privacy of their user's risk fines and penalties, and in some cases court action.
9. **Personal and mobile devices** — Nowadays, most organizations have moved business processes to the cloud. Companies that permit employees to access company software assets from any location from any device risk

introducing vulnerabilities through personal devices such as laptops and smartphones. Creating a policy for proper security of personal devices can help prevent exposure to threats via employee-owned assets.

Security Techniques

You know that cyber security is an important part of any business, but are you unsure of how to become cyber secure? You may already be using some of the top security best practices and not even realize it.



1. **Anti-Virus Software & Updates**
   When faced with the enormous task of securing your business, it's easy to forget about the basics. You want AV software that detects and prevents both known and emerging threats. But don't just download any free AV software you find online. Only install an anti-virus program from a trusted, legitimate source and always keep it (and your computer) up to date. Updates and patches for your applications and devices guarantee you have the most comprehensive protection.

2. **Firewalls**
   A firewall acts as a barrier between your safe, internal network and the horrors lurking in external networks. Firewalls filter incoming and outgoing traffic based on a set of security rules. They're a critical safeguard for both large and small businesses, as well as home networks. You'll want

to opt for a next-gen firewall, which as the name suggests, offers more advanced features than a traditional firewall.

3. **Backups**
   Regularly and automatically back up all important business data. The SBA suggests backing up all word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Be sure to store in the cloud or off-site. In the event of a ransomware attack, natural disaster, or device failure, you won't lose everything.

4. **Passwords**
   Let's be real, passwords can be a hassle. It's hard to come up with a strong one and even harder to remember what is actually is. When you get a reminder to update your password, what do you normally do? Probably hit "ignore". When it's time to create a new password for yet another application, what do you normally do? Reuse an easy to remember one. If everyone does it, is it really that bad? Oh, yes. Verizon's 2019 Data Breach Investigations Report found that 80% of all hacking-related breaches are the result of weak passwords. On top of that, 29% of all breaches, regardless of attack vector, involve the use of stolen credentials.

   Passwords can be a simple and effective way to ward off cyber criminals. A good password is random, long (very important), complex, and frequently changed. Passphrases are also useful and sometimes easier to remember than a random string of letters/numbers/special characters. You can use a password manager to keep track of all your passwords. You can also check out our eBook, Passwords: Your Greatest Vulnerability for more password tips.

5. **Multi-Factor Authentication**

Multi-factor authentication (MFA), or two-factor authentication, adds an extra layer of security to a standard password. MFA is a combination of two or more of the following:

Something you have (such as a randomly-generated code sent to your mobile phone)

Something you are (such as a fingerprint)

Something you know (such as a password)

MFA decreases your risk of compromise. If a cyber criminal happens to know your password but you have MFA enabled, it's unlikely that they'll also have access to the code your mobile device received – effectively locking them out of your account.

6. **VPN**

Public WiFi is risky and using a public network while accessing private business accounts puts your entire organization at risk. When you use public WiFI, everything you do is out in the open for anyone to see. A virtual private network (VPN) is a great tool when working outside your secure office network; and it allows you to safely transmit and receive data.

7. **Employee Security Training**
   If you've read any of our other blog posts, you'll know by now that we're a little obsessed with security training. It's inexpensive and easy, but still comes with a huge pay-off. When it comes down to it, your first line of defense against cyber-attacks is the people sitting in the cubicles right in front of you. Offer constant training and make sure each employee is aware of your cyber security policies & knows where to report suspicious activity. Teach them what not to click and you're golden.

9 Steps on Implementing an Information Security Program

Step 1: Build an Information Security Team
Before you begin this journey, the first step in information security is to decide who needs a seat at the table. One side of the table holds the executive team, made up of senior-level associates responsible for crafting the mission and goals of the security program, setting security policies, risk limitations, and more. On the other side of the table sits the group of individuals responsible for daily security operations. As a whole, this group designs and builds the framework of the security program.

Step 2: Inventory and Manage Assets
The security team's first job is to understand which assets exist, where those assets are located, ensure the assets are tracked, and secure them properly. In other words, it's time to conduct an inventory of everything that could contain sensitive data, from hardware and devices to applications (both internally and third party developed) to databases, shared folders, and more. Once you have your list, assign each asset an owner, then categorize them by importance and value to your organization should a breach occur.

Step 3: Assess Risk
To assess risk, you need to think about threats and vulnerabilities. Start by making a list of any potential threats to your organization's assets, then score these threats based on their likelihood and impact. From there, think about what vulnerabilities exist within your organization, categorize and rank them based on potential

impact. These vulnerabilities can consist of people (employees, clients, third parties), processes or lack thereof, and technologies in place.

Look at the two lists you've created and find where threats and vulnerabilities may intersect, showing you where your greatest levels of risk exist. A high-impact threat with high vulnerability becomes a high risk, for example. Contact us if you need assistance putting together a risk analysis like this.

Step 4: Manage Risk
Now that you have your risks ranked, decide whether you want to reduce, transfer, accept, or ignore each risk.

+

Identify and apply fixes to counter the risk (e.g., setting up a firewall, establishing local and backup locations, purchasing water leak detection systems for a data centre).

Transfer the risk: Purchase insurance for assets or bring on a third party to take on that risk.

Accept the risk: If the cost to apply a countermeasure outweighs the value of the loss, you can choose to do nothing to mitigate that risk.

Avoid the risk: This happens when you deny the existence or potential impact of a risk, which is not recommended as it can lead to irreversible consequences.

Step 5: Develop an Incident Management and Disaster Recovery Plan
Without an Incident Management and Disaster Recovery Plan, you put your organization at risk should any security incident or natural disaster occur. This includes things like power outages, IT system crashes, hacking, supply chain problems, and even pandemics like COVID-19. A good plan identifies common incidents and outlines what needs to be done—and by whom—in order to recover data and IT systems.

Step 6: Inventory and Manage Third Parties
Make a list of vendors, suppliers, and other third parties who have access to your organization's data or systems, then prioritize your list based on the sensitivity of

the data. Once identified, find out what security measures high-risk third parties have in place or mandate necessary controls. Be sure to consistently monitor and maintain an updated list of all third-party vendors.

Step 7: Apply Security Controls

You've been busy identifying risks and deciding on how you'll handle each one. For the risks you want to act on, it's time to implement controls. These controls will mitigate or eliminate risks. They can be technical (e.g., encryption, intrusion detection software, antivirus, firewalls), or non-technical (e.g., policies, procedures, physical security, and personnel). One non-technical control you'll implement is a Security Policy, which serves as the umbrella over a number of other policies such as a Backup Policy, Password Policy, Access Control Policy, and more.

Step 8: Establish Security Awareness Training

Conduct frequent security awareness trainings to share your information security plan and how each employee plays a role in it. After all, new security measures and policies do nothing if employees working with the data are not educated on how to minimize risk. Any time an element of your security program changes, your employees need to be aware. And be sure to document and retain evidence of trainings for future auditing purposes.

Step 9: Audit, audit, audit

The best way to determine the effectiveness of your information security program is to hire a third-party auditor to offer an unbiased assessment on security gaps. In some cases, this is mandatory to confirm compliance. Third-party assessors can also perform vulnerability assessments, which include penetration tests to identify weaknesses in your organization's networks, systems, and applications, along with audits against criteria such as ISO 27001, PCI DSS, FedRAMP, and HITRUST; as well as SOC 2® reports using the AICPA Trust Service Principles. Your company can also conduct internal audits to assess controls, policies, procedures, risk management, and more.

A Model for Network Security

When we send our data from the source side to the destination side, we have to use some transfer method like the internet or any other communication channel by which we are able to send our message. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. When the transfer of data happened from one source to another source some logical information channel is established between them by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals. When we use the protocol for this logical information channel the main aspect of security has come. who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

1. A security-related transformation on the information to be sent.
2. Some secret information is shared by the two principals and, it is hoped, unknown to the opponent.

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission. This model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of secret information.
4. Specify a protocol to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service.

Basic Terminologies in Network Security

Network security involves safeguarding computer networks and their data from unauthorized access, attacks, and damage. Here are some basic terminologies in network security:

1. **Firewall:** A security barrier that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It helps prevent unauthorized access and potential cyber threats.

2. **Intrusion Detection System (IDS):** A system that monitors network or system activities for malicious activities or security policy violations. It detects and alerts administrators about potential security incidents.

3. **Intrusion Prevention System (IPS):** Similar to IDS, but with the added capability to actively prevent or block detected security threats in real-time.

4. **Encryption:**The process of converting data into a secure format to prevent unauthorized access. It ensures that even if data is intercepted, it remains unreadable without the appropriate decryption key.

5. **Virtual Private Network (VPN):** A technology that establishes a secure and encrypted connection over an untrusted network, such as the internet. It is commonly used to provide secure remote access to a private network.

6. **Authentication:** The process of verifying the identity of a user, device, or system. Authentication methods include passwords, biometrics, smart cards, and multi-factor authentication (MFA).

7. **Authorization:** The process of granting or denying access to specific resources or actions based on the authenticated user's permissions.

8. **Access Control:** The practice of restricting access to certain resources or areas based on the user's identity, role, or other attributes.

9. **Vulnerability:** A weakness in a system's design, implementation, or configuration that could be exploited by attackers to compromise the security of the system.

10. **Patch:** A piece of software designed to fix or update a computer program or its supporting data to address security vulnerabilities or improve functionality.

11. **Penetration Testing:** The process of actively evaluating a system, network, or application for security vulnerabilities. It simulates real-world attacks to identify and address potential weaknesses.

12. **Security Policy:** A set of rules and practices that define how an organization manages and protects its information assets, networks, and systems.

13. **Incident Response:** The coordinated process of responding to and managing a security incident. It involves identifying, containing, eradicating, recovering from, and learning from security breaches.

14. **Phishing:** A type of social engineering attack where attackers use deceptive emails, websites, or other means to trick individuals into revealing sensitive information, such as passwords or credit card numbers.

15. **Malware:** A broad term for malicious software, including viruses, worms, Trojans, ransomware, and other harmful programs designed to disrupt, damage, or gain unauthorized access to computer systems.

Information Security Categories

1. **Network Security:** Firewalls: Implementing firewalls to monitor and control incoming and outgoing network traffic.

   Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): Monitoring and responding to suspicious activities and preventing unauthorized access.

2. **Data Security:** Encryption: Protecting data by converting it into a secure format that can only be accessed with the proper decryption key.

   Access Controls: Implementing mechanisms to control and restrict access to sensitive data based on user roles and permissions.

   Data Loss Prevention (DLP): Preventing unauthorized access, use, or sharing of sensitive data.

3. **Application Security:** Secure Coding Practices: Ensuring that software applications are developed with security in mind to prevent vulnerabilities.

   Web Application Firewalls (WAF): Protecting web applications from various security threats and attacks.

   Authentication and Authorization: Verifying the identity of users and controlling their access to applications.

4. **Endpoint Security:** Antivirus and Antimalware Solutions: Protecting individual devices from malicious software.

   Device Management: Implementing controls and policies to secure and manage endpoint devices.

5. **Physical Security:** Access Control Systems: Restricting physical access to facilities or data centers.

   Surveillance Systems: Monitoring and recording activities to enhance physical security.

6. **Incident Response and Management:** Security Incident and Event Management (SIEM): Monitoring and responding to security events in real-time.

   Forensics: Investigating and analyzing security incidents to understand their causes and mitigate future risks.

7. **Security Policies and Procedures:** Policy Development: Establishing rules and guidelines for information security within an organization.

   Employee Training and Awareness: Educating employees about security policies and best practices.

8. **Security Governance and Risk Management:** Risk Assessment: Identifying and assessing potential risks to information security.

   Compliance Management: Ensuring adherence to industry regulations and standards.

9. **Cloud Security:** Identity and Access Management (IAM): Managing and securing access to cloud resources.

   Data Encryption in the Cloud: Ensuring the security of data stored in cloud environments.

10. **Mobile Security:** Mobile Device Management (MDM): Managing and securing mobile devices within an organization.

    Mobile App Security: Ensuring the security of applications on mobile devices.