# Cyber 7 Security Policies



Ariel Blackwood

Sanada Thomas

Rayon Graham

Brandon Danvers

Tajae Gordon

Lester Coley

Daniel Griffiths

# Introduction

The organization's network security environment is laid out in the network security policy, which also specifies how the security policies are applied throughout the network architecture and sets rules for computer network access.

Network security policies outline the security measures used by an organization. It seeks to prevent fraudulent users from entering while also minimizing dangerous individuals already present in your company. Understanding what data and services are accessible, to whom they are available, the potential for harm, and the existing safeguards is the first step in developing a policy.

In order to implement the regulations, the security policy should provide a hierarchy of access rights, allowing people access to just the information they require to complete their tasks.

The security policies for your organization's firewall and network controls, as well as the security policies for your IT infrastructure, need to be applied.

# Research and Analysis

**Research and analyze existing network security policies used by companies or government organizations (Hypothetical):**

Based on the hypothetical research and analysis of ABC Corporation's network security policies, here are some potential findings and analysis:

Finding 1: ABC Corporation's policies do not address social engineering attacks.

Analysis: Social engineering attacks are becoming increasingly common, and it's important for network security policies to address this threat. ABC Corporation should consider updating their policies to include training for employees on how to identify and prevent social engineering attacks.

Finding 2: ABC Corporation's incident response plan is not comprehensive enough.

Analysis: An incident response plan is critical for responding to security breaches and minimizing the impact of an attack. ABC Corporation's plan may not be comprehensive enough, which could lead to delays in responding to an incident or difficulty in containing the breach. ABC Corporation should review and update their incident response plan to ensure it is comprehensive and regularly tested.

Finding 3: ABC Corporation's policies require strong passwords, but not multi-factor authentication.

Analysis: Strong passwords are important, but they may not be enough to protect against unauthorized access. Multi-factor authentication can provide an additional layer of security by requiring a second factor, such as a code sent to a mobile device, to access the network. ABC Corporation should consider updating their policies to require multi-factor authentication.

Finding 4: ABC Corporation's policies do not address the use of personal devices for work purposes.

Analysis: With more employees working remotely, it's becoming common for personal devices to be used for work purposes. However, this can create security risks if the devices are not properly secured. ABC Corporation should consider updating their policies to address the use of personal devices for work purposes and require security measures, such as encryption and remote wipe capabilities.

Overall, these findings suggest that ABC Corporation's network security policies could be improved to better protect against potential threats. By addressing these gaps, ABC Corporation can improve their overall security posture and better protect their sensitive data and systems.

**Explore real-world examples and case studies to understand various elements and best practices in network security policy development:**

Below are a few real-world examples and case studies that illustrate various elements and best practices in network security policy development:

Target Data Breach: In 2013, Target suffered a massive data breach that compromised the personal and financial information of millions of customers. The breach was caused by a vulnerability in Target's network that was exploited by hackers. Target's incident response plan was criticized for not being comprehensive enough, and the breach led to a major overhaul of Target's network security policies and procedures.

Lessons Learned: Companies must have comprehensive incident response plans in place to respond quickly and effectively to security breaches. Vulnerability management must be a top priority, and regular security assessments should be conducted to identify and address potential weaknesses in the network.

Equifax Data Breach: In 2017, Equifax suffered a data breach that exposed the personal information of over 140 million people. The breach was caused by a vulnerability in a web application that Equifax was using. Equifax was criticized for failing to patch the vulnerability in a timely manner, as a patch had been available for several months prior to the breach.

Lessons Learned: Companies must prioritize patch management and ensure that all systems and applications are kept up to date with the latest security patches. Regular vulnerability scanning and assessments are also important to identify and address potential vulnerabilities before they can be exploited by hackers.

NIST Cybersecurity Framework: The National Institute of Standards and Technology (NIST) developed a cybersecurity framework that provides a set of guidelines and best practices for organizations to manage and reduce cybersecurity risks. The framework includes five core functions: Identify, Protect, Detect, Respond, and Recover.

Lessons Learned: Organizations should use frameworks like NIST to guide their network security policy development and ensure that all critical areas, such as access control, data encryption, and incident response, are addressed. The framework should be regularly reviewed and updated to reflect new threats and evolving best practices.

Overall, these examples and case studies illustrate the importance of comprehensive network security policies that address a wide range of threats and vulnerabilities. Regular vulnerability assessments, incident response planning, and the use of established frameworks can help organizations stay ahead of potential threats and protect sensitive data and systems.

**Identify key areas covered by network security policies, such as access control, password management, data encryption, incident response, remote access, and acceptable use of resources:**

**Access control:** Network security policies should include guidelines for access control to prevent unauthorized access to the network and sensitive information. This may involve implementing authentication and authorization protocols, defining access levels, and limiting access to only those who require it.

**Password management:** Passwords are a crucial aspect of network security and should be managed appropriately. Policies should include guidelines for creating strong passwords, changing them regularly, and protecting them from unauthorized access.

**Data encryption:** Network security policies should require the encryption of sensitive data, both at rest and in transit. Encryption ensures that even if data is intercepted, it cannot be read without the appropriate decryption key.

**Incident response:** Policies should define procedures for responding to security incidents such as data breaches or malware infections. This may include identifying and containing the incident, assessing the damage, and notifying affected parties.

**Remote access:** As more employees work remotely, network security policies should address how to secure remote access to the network. This may involve implementing secure VPNs, limiting access to only necessary resources, and enforcing security policies on remote devices.

Acceptable use of resources: Policies should define acceptable use of network resources, such as email, internet, and company-owned devices. This helps prevent employees from inadvertently compromising network security or engaging in risky behavior.

# Policy Development

1. Introduction and Purpose of the Policy:

a. This Network Security Policy outlines the principles, guidelines, and

procedures that govern the security of the organization’s network

infrastructure.

b. Its purpose is to establish a secure environment for the organization&

information systems and data, safeguard against unauthorized access

and malicious activities, and ensure the confidentiality, integrity, and

availability of network resources.

2. Roles and Responsibilities:

a. Network Administrator: Responsible for the design,

implementation, and maintenance of the network infrastructure,

including security controls and monitoring.

b. System Administrators: Responsible for managing user accounts,

access controls, and network resources in accordance with this

policy.

c. Employees: Responsible for adhering to this policy, reporting any

security incidents, and following safe computing practices.

3. Access Control and User Management

a. User Account Provisioning: User accounts must be created based on the

principle of least privilege, granting access rights required for the user&#39;s job

responsibilities.

b. Account Termination: User accounts must be promptly deactivated upon

termination or change in employment status.

c. Access Review: Regular reviews of user access privileges must be conducted to

ensure the continued appropriateness of access rights.

d. User Authentication: Strong authentication mechanisms, such as multi-factor

authentication, must be implemented for access to sensitive systems and

resources.

4. Password and Authentication Guidelines:

a. Password Complexity: Passwords must meet minimum complexity

requirements, including a mix of uppercase and lowercase letters, numbers, and

special characters.

b. Password Expiration: Passwords must be changed at regular intervals, and

reuse of previous passwords should be prohibited.

c. Two-Factor Authentication: Two-factor authentication should be enforced for

all remote access and privileged accounts.

d. Account Lockout: Account lockout mechanisms must be implemented to

prevent brute-force attacks.

5. Data Protection and Encryption:

a. Data Classification: Data must be classified based on its sensitivity and

appropriate security controls applied accordingly.

b. Encryption: Strong encryption must be used for sensitive data in transit and at

rest, including email communications, databases, and backups.

c. Data Loss Prevention: Measures should be implemented to prevent the

unauthorized disclosure or loss of sensitive information.

6. Incident Response and Reporting:

a. Incident Identification: Employees must promptly report any suspected

security incidents to the IT department.

b. Incident Response Team: A designated incident response team should be

established to investigate and respond to security incidents.

c. Incident Reporting: Security incidents must be documented, including

the impact, remedial actions, and lessons learned.

7. Remote Access and Mobile Device Security:

a. Remote Access: Remote access to the organization&#39;s network

should only be permitted through secure and authenticated

channels.

b. Mobile Device Security: Mobile devices accessing the network

must adhere to security standards, including device encryption,

strong authentication, and remote wipe capabilities.

8. Acceptable Use Policy:

a. Internet Usage: Employees must use the organization&#39;s internet

resources responsibly and refrain from accessing inappropriate or

unauthorized websites.

b. Software Usage: Only authorized software should be installed on organization-

owned devices, and employees must comply with software licensing

agreements.

c. Social Engineering: Employees must be cautious of social engineering attempts

and report any suspicious activities.

9. Security Awareness Training:

a. Training Program: Security awareness training sessions must

be conducted regularly to educate employees on network

security best practices, threats, and their responsibilities.

b. Phishing Awareness: Employees should receive training on

identifying and reporting phishing attempts and suspicious

emails.

This Network Security Policy serves as a framework for maintaining the security of

the organization, network infrastructure. It is the responsibility of all employees to

adhere to this policy and report any violations or security incidents to the appropriate

authorities.

**A. Introduction and purpose of the policy**

The whole point of a network security policy is to protect a company network from internal and external network security threats. You’re responsible for your company’s customers and staff, physical assets, and data that travels across and lives within your networks. In order to protect them, you need to set security policies that describe detailed specific parameters like who and what is allowed to access which resources. The security policies become guidelines for accessing computer networks, covering the enforcement of these policies. They also determine the operational architecture of your network, including policy application. Once you finalize everything, your company will have integrated policies across the network, enabling consistency of service regardless of where your employees are, how they are connected, and what devices they will be using. Think of it as taking effective measures to improve security and communicate your commitment to the protection of your company’s data assets. Even your company employees will become more aware of data security best practices and be vigilant when doing their jobs.

**D. Password and authentication guidelines**

**Purpose**

Passwords are a critical part of information and network security. Passwords serve to protect against unauthorized access, but a poorly chosen password could put the entire institution at risk. As a result, all members of the company at risk the community should take appropriate steps to ensure that their passwords are strong and secure. The purpose of these guidelines is to set a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected.

**Scope**

These guidelines apply to all members of the company who have or are responsible for a computer account, or any form of access that supports or requires a password, on any system that resides at company or facility, or has access to level 3 assess network.

**General**

What is a password? A password is your personal key to a computer system. Passwords help to ensure that only authorized individuals access computer systems. Passwords also help to determine accountability for all transactions and other changes made to system resources, including data. If you share your password with a colleague or friend, you may be giving an unauthorized individual access to the system and may be held responsible for their actions. What if the individual gives your password to someone else? What if some of your files are deleted or otherwise rendered unusable? Are you willing to take the blame if an unauthorized individual uses your access to damage or to make unauthorized changes to data or systems?

Authentication of individuals as valid users, via the input of a valid password, is required to access any shared computer information system. Each user is accountable for the selection and confidentiality of passwords. Since you are responsible for picking your own password, it is important to be able to tell the difference between a good password and a bad one. Bad passwords jeopardize information that they are supposed to protect.

Your password should not be the same as your username. Your password should be unique. Do not use the same password across multiple accounts (Use a password manager to assist with maintaining unique passwords with all your accounts Network Security Enterprise Last Pass license. Contact itsecurity@Nselpl.edu if you would like to participate).   A good password is relatively easy to remember, but hard for somebody else to guess. There are a variety of techniques you can use to choose secure passwords. Listed below are some examples of creating passwords.

**But generally:**

* Passwords should be long and unique.
* Old passwords should not be re-used.
* All passwords should conform to the guidelines outlined below.

**Password Construction Guidelines**

Passwords are used to access any number of Companies. Poor, weak passwords are easily cracked, and put the entire system at risk. Therefore, strong passwords are required. Try to create a password that is also easy to remember.

* Passwords should be long. A password should really be a passphrase. Uses spaces between words to make them longer and harder to crack, but easier to remember.
* Passwords should contain at least 12 characters.
* Passwords should contain at least 1 uppercase letter
* Passwords should contain at least 1 lowercase letter
* Passwords should contain at least 1 numerical character
* Symbol characters are encouraged (e.g. @#$%^&!)

**Password Protection Guidelines**

* Passwords should be treated as confidential information. No one is to give, tell, or hint at their password to another person, including IT staff, administrators, superiors, other co-workers, friends, or family members, under any circumstances.
* If someone demands your password, refer them to these guidelines or have them contact the IT Department.
* Passwords should not be transmitted electronically over the unprotected Internet, such as via email.
* No one is to keep an unsecured written record of their passwords, either on paper or in an electronic file. If it proves necessary to keep a record of a password, then it must be kept in a controlled access place if in hardcopy form or in an encrypted file if in electronic form. Contact itsecurity@ Nselpl.edu if you need access to Last Pass
* Do not use the “Remember Password” feature of applications such as web browsers. They may allow an attacker to view your passwords in clear text.
* Passwords used to gain access to staff systems should not be used as passwords to access non-staff systems.
* Do not use the same password to access multiple accounts/systems. Password reuse is the #1 vector attackers use to gain unauthorized access.
* If you suspect that your password has been compromised, it must be reported to the Information Security Office and the password changed immediately.
* Finally, please do not use any of the password examples shown in this document.

**E. Data protection and encryption**

Data Security and Encryption

Data Security is the protection of data from unauthorized access, use, change, disclosure and destruction.  UVa classifies data as either highly sensitive, moderately sensitive, or non-sensitive (public), and the requirements for data security are different for each one. The company Data Protection Standards (behind NetBadge) provides guidance on the requirements for each type.

Make sure your data is safe in regards to:

* **Network security**
  + Keep confidential data off the internet
  + Put highly sensitive materials on computers not connected to the internet
* **Physical Security**
  + Restrict access to buildings and rooms where computers or media are kept
  + Only let trusted individuals troubleshoot computer problems
* **Computer Systems & Files**
  + Keep virus protection up to date
  + Don’t sent confidential data via e-mail or FTP (use encryption, if you must)
  + Use strong passwords on files and computers

**Encryption**

Encryption offers protection by scrambling data, so only the owner of the key or password can read the data.  This protects the confidentiality of the data so that if an unauthorized person gained access to the storage device or service, they would be unable to see the data.  It also protects the integrity of the data so that it cannot be tampered with without the owner knowing it.

VPN: A VPN scrambles data as it is transmitted between your mobile device and a server. This allows you to access sensitive data securely stored on a remote server. we offer three types of VPNs for accessing the company resources: The VPN, the More Secure Network (MSN), and the High Security VPN.

* VPN: Provides an Off-Grounds connection to resources that normally require you to be on Grounds to use them such as Library resources, the UVA Home Directory Service, the Exchange Server, servers restricted by departments, etc. It provides an on-Grounds IP address for all applications on your computer, thereby protecting *all* network traffic, whether or not it is Web-based, between your machine and the UVa network.
* A More Secure Network (MSN): The MSN uses a firewall*,*a network security device designed to help protect your computer from hackers and other malicious people on the Internet. Your computer can make outbound connections to access resources on the internet, but the firewall blocks inbound connections from remote computers.
* Joint VPN: Enables academic users access to resources protected by the highest security using a UVA Identity Token, from on- or off-grounds.

**F. Incident response and reporting**

**Incident Response**

* Incident Response Steps: 6 Phases of the Incident Response Lifecycle
* What Is an Incident Response Plan (IRP)?
* Incident Response Frameworks
* What is an Incident Response Team?
* Building a CSIRT in Your Organization
* What are Incident Response Services?
* Incident Response Automation
* Automated Incident Response with Cynet 360

Incident response (IR) is a set of information security policies and procedures that you can use to identify, contain, and eliminate cyberattacks. The goal of incident response is to enable an organization to quickly detect and halt attacks, minimizing damage and preventing future attacks of the same type.

This is part of an extensive series of guides about data security.

Incident Response Steps: 6 Phases of the Incident Response Lifecycle

There are six steps to incident response. These six steps occur in a cycle each time an incident occurs. The steps are:

* Preparation of systems and procedures
* Identification of incidents
* Containment of attackers and incident activity
* Eradication of attackers and re-entry options
* Recovery from incidents, including restoration of systems
* Lessons learned and application of feedback to the next round of preparation

Preparation ⇒ ­Identification ⇒ Containment ⇒ Eradication ⇒ Recovery ⇒ Lessons Learned

# Policy Presentation and Discussion

# Comparison & Reflection

Network security policies have a significant impact on organizations, employees, and overall cybersecurity. Let's examine each of these aspects:

1. Impact on Organizations:

a. Protection of Assets: Network security policies help protect an organization's valuable assets, including sensitive data, intellectual property, and critical infrastructure. By implementing policies that outline security measures and controls, organizations can prevent unauthorized access, data breaches, and potential damage to their reputation and financial well-being.

b. Regulatory Compliance: Network security policies ensure that organizations adhere to industry regulations and data protection laws. Compliance with these regulations not only avoids legal penalties but also builds trust with customers, partners, and stakeholders.

c. Business Continuity: Effective network security policies contribute to business continuity by minimizing disruptions caused by security incidents or system failures. By implementing policies that include disaster recovery plans and incident response procedures, organizations can quickly recover from incidents, reducing downtime and ensuring operational resilience.

2. Impact on Employees:

a. Security Awareness: Network security policies promote security awareness among employees. By providing clear guidelines and procedures, organizations educate their workforce on potential risks, best practices, and the importance of maintaining a secure network environment. This helps employees understand their roles and responsibilities in protecting organizational assets.

b. Compliance and Accountability: Network security policies establish rules and guidelines for employees to follow, ensuring compliance with security protocols. Through regular training and policy enforcement, employees become more accountable for their actions and are less likely to engage in risky behaviors that could compromise network security.

c. Empowerment: Well-defined network security policies empower employees to actively contribute to the organization's cybersecurity efforts. By providing them with a clear framework, organizations enable employees to report security incidents, identify vulnerabilities, and participate in maintaining a secure network environment.

3. Impact on Overall Cybersecurity:

a. Risk Mitigation: Network security policies play a vital role in identifying and mitigating risks. By implementing policies that address vulnerabilities, organizations can proactively reduce the likelihood and impact of security incidents.

b. Standardization and Consistency: Network security policies establish standard practices and procedures across the organization. This ensures consistency in security measures, making it easier to monitor and enforce security controls.

c. Incident Response: Network security policies provide guidelines for incident response, allowing organizations to handle security incidents effectively. By having predefined procedures in place, organizations can detect, respond to, and recover from security breaches more efficiently, minimizing the potential damage.

In summary, network security policies have a profound impact on organizations, employees, and overall cybersecurity. They protect assets, ensure compliance, promote security awareness, empower employees, mitigate risks, and contribute to a more secure network environment. By implementing and enforcing robust network security policies, organizations can enhance their cybersecurity posture and effectively safeguard their data, systems, and reputation.

# Reflection

Network security policies are of utmost importance in today's digital landscape. First and foremost, these policies help protect sensitive information from unauthorized access or disclosure. By implementing stringent access controls, encryption standards, and data handling procedures, organizations can safeguard customer data, intellectual property, and other confidential information. This protection not only preserves the trust of customers and stakeholders but also prevents potential legal and financial consequences that can arise from data breaches or compliance violations.

Furthermore, network security policies are crucial for minimizing risks and vulnerabilities. They serve as a roadmap for establishing secure network configurations, identifying potential threats, and implementing preventive measures. With well-defined policies in place, organizations can effectively manage risks related to malware infections, unauthorized access attempts, phishing attacks, and other cyber threats. By promoting security awareness, enforcing best practices, and implementing proactive measures, network security policies help organizations mitigate risks, ensuring the integrity and availability of their networks and critical data.

In summary, network security policies are essential for protecting sensitive information, minimizing risks, and maintaining the trust of stakeholders. These policies provide organizations with a comprehensive framework to establish robust security measures, adhere to regulatory requirements, and maintain business continuity in an ever-evolving digital landscape. By prioritizing network security policies, organizations can proactively defend against cyber threats and safeguard their valuable assets in an increasingly interconnected world.

Network security policies have a significant impact on organizations, employees, and overall cybersecurity. Let's examine each of these aspects:

1.Impact on Organizations:

a. Protection of Assets: Network security policies help protect an organization's valuable assets, including sensitive data, intellectual property, and critical infrastructure. By implementing policies that outline security measures and controls, organizations can prevent unauthorized access, data breaches, and potential damage to their reputation and financial well-being.

b. Regulatory Compliance: Network security policies ensure that organizations adhere to industry regulations and data protection laws. Compliance with these regulations not only avoids legal penalties but also builds trust with customers, partners, and stakeholders.

c. Business Continuity: Effective network security policies contribute to business continuity by minimizing disruptions caused by security incidents or system failures. By implementing policies that include disaster recovery plans and incident response procedures, organizations can quickly recover from incidents, reducing downtime and ensuring operational resilience.

2. Impact on Employees:

a. Security Awareness: Network security policies promote security awareness among employees. By providing clear guidelines and procedures, organizations educate their workforce on potential risks, best practices, and the importance of maintaining a secure network environment. This helps employees understand their roles and responsibilities in protecting organizational assets.

b. Compliance and Accountability: Network security policies establish rules and guidelines for employees to follow, ensuring compliance with security protocols. Through regular training and policy enforcement, employees become more accountable for their actions and are less likely to engage in risky behaviors that could compromise network security.

c. Empowerment: Well-defined network security policies empower employees to actively contribute to the organization's cybersecurity efforts. By providing them with a clear framework, organizations enable employees to report security incidents, identify vulnerabilities, and participate in maintaining a secure network environment.

3. Impact on Overall Cybersecurity:

a. Risk Mitigation: Network security policies play a vital role in identifying and mitigating risks. By implementing policies that address vulnerabilities, organizations can proactively reduce the likelihood and impact of security incidents.

b. Standardization and Consistency: Network security policies establish standard practices and procedures across the organization. This ensures consistency in security measures, making it easier to monitor and enforce security controls.

c. Incident Response: Network security policies provide guidelines for incident response, allowing organizations to handle security incidents effectively. By having predefined procedures in place, organizations can detect, respond to, and recover from security breaches more efficiently, minimizing the potential damage.

In summary, network security policies have a profound impact on organizations, employees, and overall cybersecurity. They protect assets, ensure compliance, promote security awareness, empower employees, mitigate risks, and contribute to a more secure network environment. By implementing and enforcing robust network security policies, organizations can enhance their cybersecurity posture and effectively safeguard their data, systems, and reputation.

# Conclusion

Network security policies play a crucial role in establishing a secure work environment and protecting sensitive information within an organization. Let's explore their significance in these areas:

1. Establishing a Secure Work Environment:

Network security policies provide a framework for creating a secure work environment by:

a. Defining Security Measures: These policies outline the necessary security measures, including access controls, firewalls, intrusion detection systems, and encryption protocols. By establishing these measures, organizations can create barriers against unauthorized access, malicious activities, and external threats.

b. Implementing Best Practices: Network security policies incorporate industry best practices and standards, such as secure password management, regular software updates, and employee training on cybersecurity. These policies guide employees in adopting secure behaviors and using secure technologies, reducing the likelihood of security incidents.

c. Monitoring and Auditing: Network security policies outline monitoring and auditing procedures to detect and respond to potential security breaches. They enable organizations to track network activities, identify anomalies, and conduct regular security assessments to ensure compliance with established policies.

2. Protecting Sensitive Information:

Network security policies are instrumental in safeguarding sensitive information from unauthorized access or disclosure by:

a. Access Control: Policies define access controls, including user authentication mechanisms, role-based access permissions, and restrictions on data access and sharing. By implementing these controls, organizations ensure that only authorized individuals can access sensitive information, reducing the risk of data breaches.

b. Data Encryption: Network security policies often require the encryption of sensitive data, both in transit and at rest. Encryption converts data into unreadable formats, making it useless to unauthorized individuals even if they gain access to it. This measure adds an extra layer of protection to sensitive information, mitigating the impact of potential security breaches.

c. Incident Response: Network security policies outline incident response procedures to handle security breaches promptly and effectively. By defining steps for incident detection, containment, mitigation, and recovery, organizations can minimize the damage caused by security incidents, ensuring that sensitive information remains protected.

In summary, network security policies are crucial for establishing a secure work environment and protecting sensitive information within an organization. They provide guidelines for implementing security measures, best practices, monitoring, and incident response procedures. By adhering to these policies, organizations can create a robust security posture, mitigate risks, and safeguard sensitive data from unauthorized access or disclosure, ensuring the confidentiality, integrity, and availability of their information assets.