Network Security Policy

George D Smith III

Cybersecurity, Old Dominion University

CYSE 425, Cyber Strategy and Policy

Francis "Skip" Hiser

August 15, 2025

This paper will be on Network Security Policy. Network security policy is used to "control their network environments and protect their organizations against evolving threats" (*Cisco*, 2025). I chose this policy because with my rising interest in finding an internship and jobs within my field, I felt like this would be an insightful topic to look into. First I wanted to look into why this policy was developed. This policy was developed to help protect an organization's data and assets. phoenixNAP says, "Network security policies were developed to protect an organization's data and assets while ensuring that employees can perform their jobs efficiently. They provide clear rules for secure access to company resources." (Andreja Velimirovic, 2023). In relation to the NIST framework, its core principles are intertwined with my policy. "Identify, Protect, Detect, Respond, and Recover" are the framework's core elements (Kelly, 2023).

Benefits of Network Security Policy

What are some benefits of a network security policy? One of the main benefits of this policy is the increased security. Being able to set lines and expectations on how network management and usage are to be enforced. These expectations allow staff to implement security measures that are up to standard and require additional security even when unneeded. Techniques and policies such as least privilege, enforced monitoring software, and defined IPS/IDS setups.

Application Of Network Security Policy

Now, how can this policy be applied within businesses and organizations? An article published on Rippling gives examples of rules within this policy, rules such as using strong and unique passwords while enabling multi-factor authentication (MFA), making sure that all company data is encrypted while in transit and at rest, or only allowing software and sites approved by the company on company devices (Krystian, 2025). These rules can be easily implemented by changing a multitude of rules and training within a company cyberspace. For example, training your employees on the importance of having a difficult/unique password while also changing the rules to the weakest type of password that can be changed to can help against brute force attacks. Another way you could put in place these rules is by implementing software onto your servers to protect and alert your staff if there are any changes to the integrity of your data while it's at rest. Things like a Data Loss Prevention, specifically a storage DLP, could help with servers maintaining data while it's at rest.

National and Global Use of Network Security Policy

Finally, on a national level and international level, how does this policy fit? As stated previously within the introduction, the NIST Framework core values are intertwined within my policy, but what about other frameworks and policies locally and globally? Taking a closer look at the national side, my policy provides detailed controls mirroring ideas such as remote control access on page 48 in the NIST SP 800-53 (NIST, 2020). A United States regulation involving my policy, HIPAA, which requires electronic health information in transit to be secure. Moving onto global frameworks, the European Union (EU) has expanded rules/requirements for information systems and network security over all critical infrastructure, which aligns directly with my policy (*NIS2 Directive*, 2022).

Conclusion

In conclusion, a network security policy is more than just a set of rules framed to follow but a great chunk of how modern cybersecurity strategy is shaped. By standardizing and enforcing different rules and techniques, this policy can strengthen an organization's defense within cyberspace. Its alignment with so many different frameworks globally and internationally shows its effectiveness in guiding infrastructure, especially critical infrastructure.

Sources and References

Drive into the future with Cisco Defense Orchestrator. (2025, May). Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-security-policy-management.html

Andreja Velimirovic. (2023, December 7). *What Is a Network Security Policy and Why Is It Important?* PhoenixNAP Blog. https://phoenixnap.com/blog/network-security-policy

Kelly, M. (2023, October 30). *Decoding NIST Compliance: Your Guide to the Cybersecurity Framework, NIST 800-53, and NIST 800-171*. Hyperproof. https://hyperproof.io/resource/a-complete-guide-to-nist-compliance/

Krystian, M. (2025, April 10). *Network Security Policy: Complete Guide & Examples | Rippling*. Rippling. https://www.rippling.com/blog/network-security-policy

NIST. (2020). Security and Privacy Controls for Information Systems and Organizations. *Security and Privacy Controls for Information Systems and Organizations*, *5*(5). https://doi.org/10.6028/nist.sp.800-53r5

Office. (2009, September 10). *The Security Rule*. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/security/index.html

NIS2 Directive: securing network and information systems. (2022). Shaping Europe’s Digital Future. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Luidold, C., & Jungbauer, C. (2024). Cybersecurity policy framework requirements for the establishment of highly interoperable and interconnected health data spaces. *Frontiers in Medicine*, *11*. https://doi.org/10.3389/fmed.2024.1379852

Alqahtani, F. H. (2017). Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science*, *124*, 691–697. https://doi.org/10.1016/j.procs.2017.12.206