Information Systems Security Policies: Key Elements for Success

Sean M. Shreve

Old Dominion University

CYSE-300: Introduction to Cybersecurity

Dr. Joseph Kovacic

14 September, 2025

Information Systems Security Policies: Key Elements for Success

A sound security policy for a corporate information system must establish and enforce key protections. This paper examines five key issues that should be addressed in such a policy: access control and authentication, perimeter security including network segmentation, patch management, encryption, and monitoring and countermeasures. With these safeguards implemented, database server storage security will be significantly stronger. It should be noted that information system security is a constant assessment of risk, threat and vulnerability management; no single combination of measures can ensure complete protection.

Access control and authentication is a core first entry point to the information systems network. One of the three tenets of information systems security is confidentiality, which involves authorizing users to access and view information (Kim & Solomon, 2023). Controlling who logs into workstation computers, whether locally or remotely, establishes the baseline standard of protection. There can also be specific authorization categories that reinforce these standards, such as content-based, context-based, and custom authorizations (Mohamed et al., 2023).

Networking segmentation combined with perimeter security is an effective strategy to regulate both inbound and outbound traffic. In a corporate setting, it is advised to have a combination of a border router with several firewalls, with the option of implementing demilitarized subnets in between those firewalls for additional protection (Department of Defense & National Security Agency, 2022). These measures help reduce possible vulnerabilities in a network while preserving the ability to expand with further implementation of security systems, such as a strong monitoring software as an example.

Security software patch management is essential for maintain system security. Over time, system architecture and software becomes outdated and requires timely updates through patches. The patching process also brings up its own risks and vulnerabilities, such as being at risk from a zero day attack. This is the type of method used by hackers to exploit an opening made by a bug or outdated software before the patching is implemented or finished (Kim & Solomon, 2023). Keep the systems updated, mitigate risks by using precautions during patching and maintenance, and system security should be at a strong security posture.

Encryption, in essence, is the process of converting data into code to prevent unauthorized access (Dizon, 2025). Encryption of the corporate server data, and its transfer between users and their workstations, is critical in terms of systems security. Security baseline goals rely on the triad of confidentiality, integrity, and availability (Kim & Solomon, 2023), and encryption plays a significant role primarily in the first two. It addresses the identification and integrity of the data itself more so than its availability (Dizon, 2025). If the security perimeter of the information systems is compromised, encryption can be the difference in minimizing the impact of an overall attack.

Monitoring and general countermeasure implementation reinforce all other categories of security for the information systems. Monitoring includes several methods. These can range from surveillance of physical locations such as the facility where the servers are stored to electronic methods. These methods include monitoring traffic, emails, communications via admin privileges and more. Countermeasures are controls that exercise restraint or management of an activity and they must have a specific purpose (Kim & Solomon, 2023). The types of countermeasures are unlimited in variety, such as maintaining an insurance policy for equipment

failure or data loss. Many come at a cost, but if able to afford them countermeasures can ensure long-term security strength for the corporation's information system.

In conclusion, a comprehensive security policy must address access control, network segmentation and perimeter defense, patch management, encryption, countermeasures and monitoring to create a resilient corporate information system. Together, these measures protect confidentiality, integrity, and availability while reducing the risk of unauthorized access and data loss. By regularly reviewing and reinforcing these five areas, organizations can maintain a strong security posture and safeguard their most critical assets.

References

Department of Defense / National Security Agency. (2022, June 15). *Network Infrastructure Security Guide*. U.S. Department of Defense. https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.pdf

Dizon, M. A. C. (2025). *Technical principles and protocols of encryption and their applications*. *Journal of Information Technology*, *39*(1), 1-20. https://doi.org/10.1080/13600834.2024.2404280

Kim, D. & Solomon, M. (2023). *Fundamentals of Information Systems Security* (4th ed.). Jones & Bartlett Learning.

Mohamed, A., Auer, D., Hofer, D., & Küng, J. (2023). *A systematic literature review of authorization and access control requirements and current state of the art for different database models*. *International Journal of Web Information Systems, 20*(2). https://doi.org/10.1108/IJWIS-04-2023-0072