Five Key Issues to Address on an Information System Security Policy

Celeste Meraz-Luna

Old Dominion University

CYSE 300

Professor Diwakar Yalpi

June 1, 2025

Designing a robust security policy is essential for any organization managing sensitive information, particularly when dealing with on-premises web, application, and database servers. In such environments, database servers often contain highly sensitive data, making it necessary to establish a comprehensive security policy. This essay outlines five critical issues that must be addressed in a corporate information system security policy to ensure confidentiality, integrity, and availability of data.

One of the foundational components of any effective security policy is a strong access control and identity management framework. Access to systems and data should be based on the principle of least privilege, meaning users are granted only the permissions necessary to perform their job functions. Role-Based Access Control (RBAC) can help enforce this principle by aligning access rights with specific job roles. Regular access reviews are also necessary to ensure that employees do not retain privileges they no longer need. According to Doherty and Fulford (2006), aligning access control strategies with organizational objectives ensures better policy effectiveness and enhances user accountability.

The classification of data based on sensitivity is crucial to determining the level of protection it requires. Organizations must establish a data classification system that categorizes information as public, internal, confidential, or restricted. Once data is classified, appropriate protection mechanisms such as encryption should be applied to secure data both at rest and in transit. Furthermore, Data Loss Prevention (DLP) technologies can be deployed to monitor and control the movement of sensitive data, reducing the likelihood of accidental or intentional leaks. Karyda, Kiountouzis, and Kokolakis (2005) emphasize that data classification strategies must be contextual and aligned with both technical and business environments to be effective.

A well-secured network acts as the first line of defense against cyber threats. Firewalls should be used to control and filter incoming and outgoing network traffic based on predefined security rules. Intrusion detection and Prevention Systems (IDPS) should also be implemented to monitor the network for suspicious activities and automatically respond to potential threats. Cram, Proudfoot, and D'Arcy (2017) note that the evolution of technical controls in security policies is driven by increasing complexity and connectivity of modern enterprise networks.

While digital security often takes center stage, physical security is equally important. Organizations must protect the facilities where servers and other critical infrastructure are located. This includes implementing physical access controls such as keycards, biometric scanners, and security personnel to ensure that only authorized individuals can enter sensitive areas. Physical and technical safeguards must be integrated, especially when protecting centralized database servers storing critical organizational assets (Karyda et al., 2005).

No matter how secure a system is, incidents can and do occur. As such, an effective security policy must include a comprehensive incident response and disaster recovery plan. A disaster recovery plan complements this by detailing how the organization will restore data and resume normal operations following a major disruption. According to Cram et al. (2017), an adaptable and well-communicated incident response strategy significantly strengthens organizational resilience and mitigates the impact of cyberattacks.

In conclusion, developing a security policy for a corporation information system requires a multi-layered approach that addresses both digital and physical vulnerabilities. By focusing on access control, data protection, network security, physical safeguards, and incident response, organizations can significantly reduce the risk of data breaches and other security incidents.

These measures not only protect sensitive information but also support the organization's long-term operational resilience and compliance with regulatory standards.

References

Cram, W. A., Proudfoot, J. G., & D'arcy, J. (2017). Organizational information security policies: a review and research framework. European Journal of Information Systems, 26(6), 605–641. https://doi.org/10.1057/s41303-017-0031-3

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. Computers & Security, 25(1), 55–63. https://doi.org/10.1016/j.cose.2005.09.010

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. Computers & Security, 24(3), 246–260. https://doi.org/10.1016/j.cose.2004.08.010