Old Dominion University

Corporate Information Security Policy

Noah Salafranca
CYSE 300
Dr. Joseph Kovacic
September 15, 2023

Corporate information must be secure in today's vast and digitally driven corporate environment. Businesses use on-premises web, application, and database servers to manage sensitive data. A well-developed security policy is necessary to protect this data and guarantee company assets' confidentiality, integrity, and availability. To develop and implement security measures, building a firm policy that serves as a framework for information security is important. This information security policy will examine various concerns and obstacles essential to the security of confidential information and the effective functioning of the security system. This policy attempts to provide a complete approach to protecting corporate information systems by outlining policies and procedures relating to data classification, access control, network security, incident response, cybersecurity training, and more.

Firstly, the classification of data is essential to any effective security policy. Using a well-defined data categorization system will determine the sensitivity of information by classifying it into different categories, such as public, internal, sensitive, and confidential. Specific handling instructions that specify how data should be handled, stored, transported, and eventually disposed of securely are provided with each classification. The policy also addresses the crucial problem of access control, which identifies who inside the company has access to sensitive information and sets access limitations following that information.

Next, a system to control access to information must be implemented. Utilizing such a system ensures that every employee has the exact level of access to the information they should have to do their job. Included in this, it is also best to implement multi-factor authentication and password strengthening. Multi-factor authentication will introduce another layer of security with another step to complete to access information. With multi-factor authentication, the employee will be prompted to enter a username, password, or email to access certain information. The

employee must then enter a PIN or authentication code to gain access. Stricter password requirements should also be introduced. Increased password security, complex password combinations, regularly updating passwords, and more can be used to minimize unauthorized access.

Additionally, the information security policy must also prioritize network security. Separating web, application, and database servers from one another and the more extensive corporate network emphasizes network segmentation's significance. Additionally, to secure the network, it is also in the corporation's best interest to set up firewalls to protect from risky network traffic from the outside. Furthermore, intrusion detection and prevention systems are crucial in safeguarding and monitoring the network. Features such as encryption should be used to protect further information during transmission.

Now that a strong foundation is built to protect the network and sensitive data, it is essential to create an action plan for the possibility of a cybersecurity attack. An organized incident response strategy is a necessary component of every security policy. The policy outlines what should be done in the event of a security breach or data compromise and encourages immediate and efficient repair. Not only is an incident response plan essential, but constant monitoring is also needed. Monitoring includes reviewing trends and managing incidents such as intrusions.

With a security system put in place, it is also essential that this security policy extends to employees. The security of a corporation is only as strong as its weakest link, which is frequently one of its employees who may unintentionally compromise security. Therefore, providing employees with mandatory cybersecurity training is necessary to reduce human error as much as possible. Training would include the significance of cybersecurity education and awareness.

These training programs inform participants about security best practices, typical risks, and their part in securing an environment.

References

Baskerville, Goodman, Straub, Baskerville, Richard, Goodman, Seymour E, & Straub, Detmar W. (2015). *Information Security Policy, Processes, and Practices*.

It security policies: What they are and what to include - indeed. (n.d.). https://www.indeed.com/hire/c/info/security-policies

Michael Nieles Kelley Dempsey Victoria Yan Pillitteri - Nist. (n.d.-b). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf