Cybersecurity Policies

Christiane Joy Galang

Introduction to CyberSecurity

Dr. Joseph Kovacic

13 September 2025

When storing private and sensitive information on the web, companies must take precautions to keep the data safe from unauthorized users. According to Robinson, a cybersecurity policy is a formal set of protocols that outlines how an organization can protect its system from cyber threats. This includes providing employees with instructions on how to practice security measures to protect the organization from unauthorized access. It also includes access control, monitoring, and incident response, data protection, and data back-ups. To ensure the company's security against new and advancing threats, cybersecurity policies must be regularly updated and closely monitored.

One important way to keep software secure is to spread awareness and properly train employees against threats. Cybersecurity policies would be useless if employees fell for social engineering attacks such as phishing or other scams. If they receive a suspicious email or message through their work account, they should be trained to report it immediately. This will allow the IT department to take action against these threats and spread further awareness. Additionally, if employees bring their own devices to work, they must ensure they take care of their devices. One example of this is connecting to a public Wi-Fi network; if employees connect to an unsecured Wi-Fi network, a hacker could easily install malware on their work devices. Lastly, if their devices get lost or stolen, they must immediately report it to the company (Nico P., 2025). If the work device gets into the hands of an attacker, they could gain access to unauthorized data in the company's system.

The next policy to implement is access control. Employees must create strong passwords, ones that have not been used in any other personal accounts. This will reduce the likelihood of attackers guessing the password and gaining access to the system. The company should also implement multi-factor authentication. This ensures that only authorized users may enter the

system and notify users of any potential breaches. Access control will ensure that the company has more control over who can see certain information.

Another policy they should implement is an incident monitoring and response. An incident response is the process and technologies organizations use to detect and respond to cyberattacks or security breaches. Organizations should mitigate threats, but sometimes, breaches happen, and they must be ready to handle any incidents with minimal damage to the business's infrastructure and reputation (Shafique, 2021). There should be constant security solutions installed in the system to monitor any threats before they happen. If there are any breaches, each employee should be aware of their responsibilities and know what to avoid doing throughout the response plan. Organizations should have plans on how to handle different types of attacks, such as DDoS attacks, malware, ransomware, and phishing attacks (Holdsworth, Kosinki, 2024). Once resolved, organizations must retrieve any lost data from the system.

The next issue to be addressed is data protection. Whether or not it is being transmitted, private data must always be encrypted. There are end-to-end protection measures such as Advanced Encryption Standard (AES) to protect the transmission of data online; it is the standard encryption protocol. However, even if the data is at rest, it still must be encrypted. The best way to practice still-data encryption is using a hardware security module. It is a technology that has security controls that stop encryption keys from leaving the device without an authorized user to access them (Beer, 2025). Data encryption is important to the organization's system as it ensures that unauthorized users cannot simply read or access sensitive information.

The last security measure that should be addressed is backing up important data in the system. Data must be regularly backed up to avoid any data loss from cyber attacks. Software programs must be implemented in the system to ensure automatic back-ups on company devices.

Employees must also be encouraged to ensure their data has been backed up and ready for any possible cyber attacks (Nico P., 2025). If any files are lost during a breach, the company must be prepared to restore any data.

Organizations must be protected from cyber attacks and breaches at all times. The systems contain sensitive information about the company and its customers; any breaches could affect the trust between customers and affect the company's revenue and reputation. The company's security policy must include training employees against cyber threats, access control, monitoring incident response, and data protection and back-ups.

References

Beer, K. (2025, February 12). *The importance of encryption and how AWS can help | Amazon Web Services*. AWS. Retrieved September 13, 2025, from https://aws.amazon.com/blogs/security/importance-of-encryption-and-how-aws-can-help/

Holdsworth, J., & Kosinki, M. (2024, August). *What is Incident Response?* IBM. Retrieved September 13, 2025, from https://www.ibm.com/think/topics/incident-response

P., N. (2025, June 2). *Cyber security training for employees: a how-to guide*. https://preyproject.com/blog/how-to-educate-employees-about-cybersecurity

Robinson, K., & Noonan, L. (n.d.). *What Is A Cyber Security Policy? Importance And Best Practices*. MetaCompliance. Retrieved September 12, 2025, from https://www.metacompliance.com/blog/data-breaches/what-is-a-cyber-security-policy

Shafique, S. (2021, November 24). *5 Must-Have Cyber Security Policies for your Organization*. Idenhaus. Retrieved September 12, 2025, from https://idenhaus.com/5-must-have-security-policies-for-your-organization/