Key Elements of a Data Security Policy

Having a well-documented data security policy in place can help protect your employees, sensitive information and customers from security breaches. To develop a holistic policy, it is important to analyze all the areas that could be of potential threat.

Use this checklist to ensure your data security policy includes all the key elements required to maintain data privacy and security.

SAFEGUARD DATA PRIVACY: Apart from complying with the existing rules and regulations, a data privacy policy will guide your employees on how to handle sensitive information in such a way that it is not compromised.

PASSWORD MANAGEMENT: Setting up a password policy will ensure your company resources are protected and only accessible by authorized personnel. The guidelines should include password length, complexity and how often it needs to be changed.

INTERNET USAGE: An internet usage policy that defines best practices while accessing the internet, such as restricting employees from visiting certain sites or prohibiting unnecessary file downloads, will help set limitations and minimize security risks.

EMAIL USAGE: Companies often fall victim to data breaches due to employee negligence or email misuse. With an email policy in place, your employees will be aware of what is expected of them and how company information should be disseminated internally and externally.

COMPANY DEVICES: As the use of mobile devices for work gains momentum, it also opens the door to several security threats. Implementing a comprehensive policy will help mitigate the risks associated with data theft and stolen devices, and ensure the devices are used responsibly within the set guidelines.

PERSONAL EMPLOYEE DEVICES: Unlike company-owned devices, it's difficult to have complete control over personal devices. A security policy, such as accessing company resources only through a secure VPN, or installing an antivirus or mobile device management software, will set certain boundaries or limitations.

SOCIAL MEDIA PRESENCE: Protecting your company's reputation is critical not only within the workplace but outside as well. A social media policy will help regulate your employees' online activities.

SOFTWARE USER AGREEMENTS: Violating a software license agreement can lead to legal implications. A software user agreement policy will ensure your employees comply with the procedures regarding the appropriate use of company-owned software.

REPORTING SECURITY BREACHES: Implementing a Security Incident Reporting policy is important to minimize negative impacts. Your employees should be educated on how to report real or suspected security breaches and what steps they need to take to prevent them from happening.

Data security risks can arise at any time and from anywhere.

To know how to set up effective policies and procedures to fortify your data security, contact us today.

PCnet
total IT management

2026 East Phelps, Springfield, Missouri 65802 • P: (417)-831-1700 F: (314)-558-8424

PCNETINC.COM