Essential Elements of a Data Security Policy

Author: eFraudPrevention

BankUnited

Safeguard Data Privacy

Employees must understand that your privacy policy is a pledge to your customers that you will protect their information. Data should only be used in ways that will keep customer identity and the confidentiality of information secure. Of course, your employees and organizations must conform to all applicable laws and regulations.

Establish Password Management

A password policy should be established for all employees or temporary workers who will access corporate resources. In general, password complexity should be established according to the job functions and data security requirements. Passwords should never be shared.

Govern Internet Usage

Most people use the internet without a thought to the harm that can ensue. Employee misuse of the internet can place your company in an awkward, or even illegal, position. Establishing limits on employee internet usage in the workplace may help avoid these situations. Every organization should decide how employees can and should access the web. You want employees to be productive, and this may be the main concern for limiting internet usage, but security concerns should also dictate how internet guidelines are formulated.

Manage Email Usage

Many data breaches are a result of employee misuse of email that can result in the loss or theft of data and the accidental downloading of viruses or other malware. Clear standards should be established regarding the use of emails, message content, encryption, and file retention.

Govern and Manage Company-Owned Mobile Devices

When organizations provide mobile devices for their employees to use, a formal process should be implemented to help ensure that mobile devices are secure and used appropriately. Requiring employees to be responsible for protecting their devices from theft and requiring password protection in accordance with your password policy should be minimum requirements.

Establish an Approval Process for Employee-Owned Mobile Devices

With the increased capabilities of consumer devices, such as smartphones and tablets, it has become easy to interconnect these devices to company applications and infrastructure. The use of these devices to interconnect to company email, calendaring and other services can blur the lines between company controls and consumer controls. Employees who request and are approved to have access to company information via their personal devices should understand and accept the limitations and controls imposed by the company.

Govern Social Media

All users of social media need to be aware of the risks associated with social media networking. A strong social media policy is crucial for any business that seeks to use social networking to promote its activities and communicate with its customers. Active governance can help ensure employees speak within the parameters set by their company and follow data privacy best practices.

Oversee Software Copyright and Licensing

There are many good reasons for employees to comply with software copyright and licensing agreements. Organizations are obliged to adhere to the terms of software usage agreements and employees should be made aware of any usage restrictions. Also, employees should not download and use software that has not been reviewed and approved by the company.

Report Security Incidents

A procedure should be in place for employees or contractors to report malicious malware in the event it is inadvertently imported. All employees should know how to report incidents of malware and what steps to take to help mitigate damage.

All content is for informational purposes only and does not constitute legal, tax, or accounting advice. You should consult your legal and tax or accounting advisors before making any financial decisions.