Docupile

CPA Cybersecurity Checklist

The frequent and alarming instances of significant cybersecurity breaches have desensitized numerous accountants to the security risks posed by criminal hackers.

There is a prevailing misconception that this is primarily a concern for large corporations, but the truth is that businesses of all sizes are now more susceptible than ever.

Recent news highlights the increased interest in CPA firms due to the valuable client financial data stored within their networks.

It is crucial for firm owners to recognize their fiduciary duty to safeguard this data entrusted to them by clients, as it is a prime target for hackers.

Although achieving absolute protection from cybersecurity threats is impossible, there are numerous measures that firms can adopt to substantially reduce the risk of falling victim to such incidents.

Presented below are 22 cybersecurity best practices that CPAs should consider implementing to safeguard their firms and client data.

Docupile
Document Management Software

CYBERSECURITY BEST PRACTICES

1) Limit Unauthorized Access to Workstations

□ **Automatic Screen Lock:**
Screens should automatically lock after 5-20 minutes of non-use to minimize unauthorized access.

□ **Power Off:**
Turn off computers when not in use.

2) Enforce Password Policies

□ **Change Passwords Regularly:**
Require users to change their passwords four times per year.

□ **Terminate Access for Departing Employees:**
Ensure IT is involved when any employee leaves the firm to terminate network access and passwords.

□ **Encourage Complex Passwords:**
Use complex passwords or passphrases with a combination of numbers, letters, and special characters.

3) Use Enhanced Password Controls

□ **Multi-Factor Authentication:**

Implement tools such as physical security fobs, biometric scans, or two-factor authentication applications.

□ **Password Managers:**

Use password managers to generate unique, complex passwords for each application.

4) Keep On-Premise Data Secure

□ **Secure File Servers:**

Place file servers in an unmarked, locked room.

□ **Encrypted Storage:**

Use encrypted storage disks for workstations or secure servers/clouds.

□ **Alarm System:**

Have an updated alarm system with unique codes for each employee.

□ **Shred Physical Documents:**

Shred and dispose of physical documents once digitized.

5) Document All Firm-Owned Equipment

□ **Inventory Tags:**

Utilize inventory tags to track equipment and document acquisitions, assignments, and dispositions.

6) Secure Client Data Locations

□ **Data Mapping:**

Know where all client data resides and secure it. Limit access to these systems.

7) Validate Users and Equipment

□ **Trusted Users/Devices:**

Only allow trusted, validated users and equipment to connect to IT resources.

□ **Mobile Device Management:**

Require registration for each device to connect to the network.

8) Automatically Update Systems

□ **Operating System Updates:**

Set workstations to automatically update the operating system and key applications.

9) Minimize Access Levels

□ **Administrator Privileges:**

Minimize users with administrator privileges and set access levels to the minimum required.

10) Ensure Current Operating Systems

□ **Review Updates:**

Regularly review updates for all equipment comprising the network and change default passwords on all connected devices.

11) Antivirus/Security Software

□ **Install and Update Software:**

Ensure each fileserver, workstation, and mobile device has up-to-date antivirus/security software.

12) Regular Backup Reviews

□ **Backup Logs:**

Regularly review backup logs and verify data accessibility. Make shadow copies of changed files throughout the day.

13) Use Encrypted Email and Portals

□ **Training:**

Train all personnel on utilizing encrypted email and portal solutions for secure file transmission.

14) Secure Connections Outside the Office

□ **VPN:**

Use a VPN connection when outside the office and verify secure connections.

15) Annual IT Policy Reviews

□ **Policy Updates:**

Review IT policies annually and remind users of changes.

16) Security Training

□ **Annual CPE Curriculum:**

Provide security training as part of the firm's annual CPE curriculum.

17) Phishing Awareness

□ **Regular Reminders:**

Regularly remind employees of current phishing schemes and recommended responses.

18) Background Checks

□ **Access Control:**

Conduct background checks on anyone given access to the firm network.

19) Visitor Policies

□ **Greet Office Visitors:**

Train employees to assist unrecognized visitors and verify their purpose.

21) Breach Response Plan

□ **Incident Response Plan:**

Develop a cybersecurity incident response plan before a breach occurs.

22) Review Insurance Policies

□ **Insurance Coverage:**

Review insurance policies to understand coverage for cybersecurity breaches and related damages.

100% SECURE

Explore Docupile, a cutting-edge document management system designed to secure your document handling processes.

Wish to secure your files?

Schedule your demo today! Scan Here

4522 Schlipf Rd, Katy, TX, 77493
call: (281) 942-4545
contact@docupile.com
www.docupile.com