Information Risk Management Policy

Title
Risk Management of the CPA Firm of Ivan Richard Chusid, CPA, PLLC's Information.

Purpose
The purpose of this policy is to ensure that risks to the CPA Firm's information are identified, analyzed and managed, so that they are maintained at acceptable levels. Maintenance of this policy, will ensure compliance with the Recommended Minimum Practice (RMP) for the CPA NetProtect Security Professional Liability Insurance Program.

Guidelines
Workstation Security:

1. **Security Suite Software:** In order to maintain a secure working environment, the Firm will ensure that all workstations will be outfitted with AntiVirus, Anti-Spyware and Firewall Programs. This will mitigate most risks of intrusion through the public internet.
   Implementation:
   1. Kaspersky Internet Security Suite should be installed on all workstations.
   2. Virus Definitions will be automatically installed when available.
   3. The Security Suite will be configured to automatically scan email attachments and other downloads from the internet for malicious software. Execution of malicious software will be prevented,
   4. The Firewall will be explicitly configured to prevent FTP and Telnet Protocols both for incoming and outgoing traffic.
   5. The Firewall will be configured to prevent all incoming traffic, except for HTTP and HTTPS protocols.
   6. The Firewall will be configured to allow outgoing traffic.
   7. A Full Antivirus Scan will be scheduled to run to completion every week.
2. **Software Updating:** In order to prevent data breaches due to outdated software vulnerabilities, the Firm will maintain a preventive automated software updating policy, when available. For software lacking automatic software updating capabilities, the Firm, will check for updates on a biweekly basis, installing updates as they become available.
   Implementation:
   1. Windows Security Updates will be automatically installed
   2. The Security Suite will be configured to automatically check for updates and when available install the aforementioned updates.
   3. All software installed on the computer with the ability to auto-update will be configured to do so.
   4. Software on the computer without the ability to auto-update will be manually checked for updates on a biweekly basis. If a update exists, it will be installed immediately.
3. **User Training:** In order to ensure that employees understand the risks of certain actions taken on the workstation that may compromise information security, all employees will be trained on best practices.
   Implementation:
   1. Employees will be trained to not open email attachments or download files with the following executable extensions (exe, .vbs, .bat, .pif, .scr.).
   2. Employees will be trained to not open email attachments from unknown or unexpected sources.

3. Employees will be trained to use password managers, to ensure that their passwords are randomized, ensuring more cryptographically secure passwords for pertinent accounts.

Network Security:

1. **Hardware Firewall:** Default settings for the routers hardware firewall will be configured to meet the Firm's needs.
   Implementation:
   1. The Firewall will be set to block all incoming traffic except HTTP and HTTPS.
   2. Incoming traffic exceptions will be changed on an as need basis, based on the needs of corporate software.
   3. Incoming traffic will be monitored to identify malicious threats. Logs and firewall policy will ensure that IP addresses identified as malicious are banned and blocked.
   4. The Router/Firewall will change the default account credentials and create accounts for administrator access only.
   5. Outgoing traffic will generally be allowed, but monitored. If suspicious activity is suspected, new outgoing rules will be changed to prevent this activity.
2. **Servers**: Servers containing the Firm's information will follow best practices for security. Linux will be used.
   Implementation:
   1. Automatic Updates will be enabled
   2. Firewall will be configured to block incoming traffic, except as needed.
   3. Firewall will be configured to allow outgoing traffic.
   4. If serving webpages, the server will use a reverse proxy to provide an access point only available via SSL Encryption (HTTPS) to the end-user.
   5. Linux Groups and Permissions will be used to only allow authorized access to information and server administration.
   6. Strong password policies will be enforced including:
      1. Password changes every 90 days.
      2. Policies to only allow historically unique passwords.

Information Access Controls:

1. **USB Monitoring:** To prevent unauthorized data transfers via usb, usb ports will be monitored on all servers and workstations.
   Implementation:
   1. For Windows based workstations, Logman with the Microsoft Message Analyzer will be used to monitor usb operations.
2. **User Access Controls:** To prevent unauthorized access to shared data, group policies will be enforced, only allowing certain individuals in a group access to data, on a need to access basis.
   Implementation:
   1. All users will have their own accounts.
   2. A log of all active users will be kept on file.
   3. Inactive users will have their accounts terminated within 8 hours of formal request to Administrator by Managing Accountant.
   4. Shared data will be placed in folders with group policy controls.
   5. Administrators will change user and group permissions as needed to allow access to the information required to perform work related tasks.
      1. Administrators will change permissions within 8 hours of written or electronic request from Managing Accountant.

3. **Custom Password Policy:** In order to ensure that users only use strong and complex passwords to utilize accounts, a custom password policy will be setup using Window's Local Security Policy.
   Implementation:
   1. Prevent password reuse—enforcing password history.
   2. Ensure that password is change ever 90 days.
   3. Ensure that passwords have a minimum length of at least 6 characters.
   4. Ensure passwords do not include the user's account name or parts of the user's full name that exceed two consecutive characters
   5. To ensure a certain level of complexity, passwords must contain characters from three of the following four categories:
      1. English uppercase characters (A through Z)
      2. English lowercase characters (a through z)
      3. Base 10 digits (0 through 9)
      4. Non-alphabetic characters (for example, !, $, #, %)
4. **Network Access Policy:** Shared data will only be shared via Local Area Network (LAN).

   Implementation:

   1. Use Window's Workgroups to facilitate sharing amongst users in LAN.
   2. Remote access to this shared data will not be available at this time.