
# Information Technology Cyber Security Policy

Associated Pension Consultants Inc
POLICY MANUAL

Subject: CYBER SECURITY POLICY

## 1 DEFINITION

The use of the term "company" is in reverence to the following organization: Associated Pension Consultants Inc.

## 2 INTRODUCTION

This Cyber Security Policy is a formal set of rules by which those people who are given access to company technology and information assets must abide.

The Cyber Security Policy serves several purposes. The main purpose is to inform company users: employees, contractors and other authorized users of their obligatory requirements for protecting the technology and information assets of the company. The Cyber Security Policy describes the technology and information assets that we must protect and identifies many of the threats to those assets.

The Cyber Security Policy also describes the user's responsibilities and privileges, including acceptable use and rules regarding Internet access. The policy answers questions about user limitations and informs users there will be penalties for violation of the policy. This document also contains procedures for responding to incidents that threaten the security of the company computer systems and network.

## 3 WHAT ARE WE PROTECTING

It is the obligation of all users of the company systems to protect the technology and information assets of the company. This information must be protected from unauthorized access, theft and destruction. The technology and information assets of the company are made up of the following components:

- Computer hardware, CPU, disc, Email, web, application servers, PC systems, application software, system software, etc.
- System Software including: operating systems, database management systems, and backup and restore software, communications protocols, and so forth.
- Application Software: used by the various departments within the company. This includes custom written software applications, and commercial off the shelf software packages.

- Communications Network hardware and software including: routers, routing tables, hubs, switches, firewalls, private lines, and associated network management software and tools.

## 3.1 Classification of Information

User information found in computer system files and databases shall be classified as either confidential or non-confidential. The company shall classify the information controlled by them. The designated Security Administrator is required to review and approve the classification of the information and determine the appropriate level of security to best protect it.

## 3.2 Classification of Computer Systems

| Security Level | Description | Example |
|---|---|---|
| RED | This system contains confidential information – information that cannot be revealed to personnel outside of the company. Even within the company, access to this information is provided on a "need to know" basis. | Server containing confidential data and other department information on databases. Network routers and firewalls containing confidential routing tables and security information. |
| GREEN | This system does not contain confidential information or perform critical services, but it provides the ability to access RED systems through the network. | User department PCs used to access Server and application(s). Management workstations used by systems and network administrators. |
| WHITE | This system is not externally accessible. It is on an isolated LAN segment, unable to access RED or GREEN systems. It does not contain sensitive information or perform critical services. | A test system used by system designers and programmers to develop new computer systems. |
| BLACK | This system is externally accessible. It is isolated from RED or GREEN systems by a firewall. While it performs important services, it does not contain confidential information. | A public Web server with non-sensitive information. |

### 3.3 Local Area Network (LAN) Classifications

A LAN will be classified by the systems directly connected to it. For example, if a LAN contains just one RED system then all network users will be subject to the same restrictions as RED systems users. A LAN will assume the Security Classification of the highest-level systems attached to it.

## 4 DEFINITIONS

Externally accessible to public. The system may be accessed via the Internet by persons outside of the company without a logon id or password. It is possible to "ping" the system from the Internet. The system may or may not be behind a firewall. A public Web Server is an example of this type of system.

Non-Public, Externally accessible. Users of the system must have a valid logon id and password. The system must have at least one level of firewall protection between its network and the Internet. The system may be accessed via the Internet or the private Intranet. A private FTP server used to exchange files with business partners is an example of this type of system.

Internally accessible only. Users of the system must have a valid logon id and password. The system must have at least two levels of firewall protection between its network and the Internet. The system is not visible to Internet users. It may have a private Internet (non-translated) address and it does not respond to a "ping" from the Internet. A private intranet Web Server is an example of this type of system.

Chief Information Officer. The Director of the Department of Information Technology (IT) shall serve as the Chief Information Officer.

Security Administrator. An employee of IT shall be designated as the Security Administrator for the company.

## 5 Threats to Security

### 5.1 Employees

One of the biggest security threats is employees. They may do damage to your systems either through incompetence or on purpose. You must layer your security to compensate for that as well. You mitigate this by doing the following.

- ✓ Only give out appropriate rights to systems. Limit access to only business hours.
- ✓ Don't share accounts to access systems. Never share your login information with co-workers.
- ✓ When employees are separated or disciplined, you remove or limit access to systems.
- ✓ Advanced – Keep detailed system logs on all computer activity.
- ✓ Physically secure computer assets, so that only staff with appropriate need can access.

### 5.2 Amateur Hackers and Vandals.

These people are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be a large number of attacks. These are usually crimes of opportunity. These amateur hackers are scanning the Internet and looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favorite targets. Once they find a weakness, they will exploit it to plant viruses, Trojan horses, or use the resources of your system for their own means. If they do not find an obvious weakness, they are likely to move on to an easier target.

### 5.3 Criminal Hackers and Saboteurs.

The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

## 6 User Responsibilities

This section establishes usage policy for the computer systems, networks and information resources of the office. It pertains to all employees and contractors who use the computer systems, networks, and information resources as business partners, and individuals who are granted access to the network for the business purposes of the company.

### 6.1 Acceptable Use

User accounts on company computer systems are to be used only for business of the company and not to be used for personal activities. Unauthorized use of the system may be in violation of the law. Unauthorized use of the company computing system and facilities may constitute grounds for either civil or criminal prosecution.

Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon IDs and passwords. Furthermore, they are prohibited from making unauthorized copies of such confidential information and/or distributing it to unauthorized persons outside of the company.

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to company systems for which they do not have authorization.

Users shall not attach unauthorized devices on their PCs or workstations, unless they have received specific authorization from the employees' manager and/or the company IT designee. Users shall not download unauthorized software from the Internet onto their PCs or workstations.

Users are required to report any weaknesses in the company computer security, any incidents of misuse or violation of this policy to their immediate supervisor.

## 6.2 Use of the Internet

The company will provide Internet access to employees and contractors who are connected to the internal network *and* who has a business need for this access. Employees and contractors must obtain permission from their supervisor and file a request with the Security Administrator.

The Internet is a business tool for the company. It is to be used for business-related purposes such as: communicating via electronic mail with suppliers and business partners, obtaining useful business information and relevant technical and business topics.

The Internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature or any other purpose which is illegal or for personal gain.

## 6.3 User Classification

All users are expected to have knowledge of these security policies and are required to report violations to the Security Administrator. Furthermore, all users must conform to the Acceptable Use Policy defined in this document. The company has established the following user groups and defined the access privileges and responsibilities:

| User Category | Privileges & Responsibilities |
|---|---|
| Department Users (Employees) | Access to application and databases as required for job function. (RED and/or GREEN cleared) |
| System Administrators | Access to computer systems, routers, hubs, and other infrastructure technology required for job function. Access to confidential information on a "need to know" basis only. |
| Security Administrator | Highest level of security clearance. Allowed access to all computer systems, databases, firewalls, and network devices as required for job function. |
| Systems Analyst/Programmer | Access to applications and databases as required for specific job function. Not authorized to access routers, firewalls, or other network devices. |
| Contractors/Consultants | Access to applications and databases as required for specific job functions. Access to routers and firewall only if required for job function. Knowledge of security policies. Access to company information and systems must be approved in writing by the company director/CEO. |

| | |
|---|---|
| Other Agencies and Business Partners | Access allowed to selected applications only when contract or inter-agency access agreement is in place or required by applicable laws. |
| General Public | Access is limited to applications running on public Web servers. The general public will not be allowed to access confidential information. |

### 6.4 Monitoring Use of Computer Systems

The company has the right and capability to monitor electronic information created and/or communicated by persons using company computer systems and networks, including e-mail messages and usage of the Internet. It is not the company policy or intent to continuously monitor all computer usage by employees or other users of the company computer systems and network. However, users of the systems should be aware that the company may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with company policy.

## 7 Access Control

A fundamental component of our Cyber Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of the system, including the network. Access control is implemented by logon ID and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and databases available to users based on their job requirements.

### 7.1 User System and Network Access – Normal User Identification

All users will be required to have a unique logon ID and password for access to systems. The user's password should be kept confidential and MUST NOT be shared with management & supervisory personnel and/or any other employee whatsoever. All users must comply with the following rules regarding the creation and maintenance of passwords:

- Password must not be found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools".
- Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.
- Password must be changed every 90 days.
- User accounts will be frozen after 3 failed logon attempts.
- Logon IDs and passwords will be suspended after 90 days without use.

Users are not allowed to access password files on any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

Users will not be allowed to logon as a System Administrator. Users who need this level of access to production systems must request a Special Access account as outlined elsewhere in this document.

Employee Logon IDs and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the company office.

Supervisors / Managers shall immediately and directly contact the company IT Manager to report change in employee status that requires terminating or modifying employee logon access privileges.

Employees who forget their password must call the IT department to get a new password assigned to their account. The employee must identify himself/herself by to the IT department.

Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee's password and ID. Employees shall not logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

## 7.2 System Administrator Access

System Administrators, network administrators, and security administrators will have access to host systems, routers, hubs, and firewalls as required to fulfill the duties of their job.

All system administrator passwords will be *DELETED/CHANGED* immediately after any employee who has access to such passwords is terminated, fired, or otherwise leaves the employment of the company.

## 7.3 Special Access

Special access accounts are provided to individuals requiring temporary system administrator privileges in order to perform their job. These accounts are monitored by the company and require the permission of the user's company IT Manager. Monitoring of the special access accounts is done by entering the users into a specific area and periodically generating reports to management. The reports will show who currently has a special access account, for what reason, and when it will expire. Special accounts will expire in 5 days and will not be automatically renewed without written permission.

## 7.4 Connecting to Third-Party Networks

This policy is established to ensure a secure method of connectivity provided between the company and all third-part companies and other entities required to electronically exchange information with company.

"Third-party" refers to vendors, consultants and business partners doing business with company, and other partners that have a need to exchange information with the company. Third-party network connections are to be used only by the employees of the third-party, only for the business purposes of the company. The third-party company will ensure that only authorized users will be allowed to access information on the company network. The third-party will not allow Internet traffic or other private network traffic to flow into the network.

This policy applies to all third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed.

All requests for third-party connections must be made by submitting a written request and be approved by the company.

### 7.5 Connecting Devices to the Network

Only authorized devices may be connected to the company network(s). Authorized devices include PCs and workstations owned by company that comply with the configuration guidelines of the company. Other authorized devices include network infrastructure devices used for network management and monitoring.

Users shall not attach to the network: non-company computers that are not authorized, owned and/or controlled by company.

NOTE: Users are not authorized to attach any device that would alter the topology characteristics of the Network or any unauthorized storage devices, e.g. thumb drives and writable CD's.

### 7.6 Remote Access

Only authorized persons may remotely access the company network. Remote access is provided to those employees, contractors and business partners of the company that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the network or a remote network to company network connection. The only acceptable method of remotely connecting into the internal network is using a secure ID.

### 7.7 Unauthorized Remote Access

The attachment of devices (e.g. hubs) to a user's PC or workstation that is connected to the company LAN is not allowed without the written permission of the company. Additionally, users may not install personal software designed to provide remote control of the PC or workstation. This type of remote access bypasses the authorized highly secure methods of remote access and poses a threat to the security of the entire network.

## 8 Penalty for Security Violation

The company takes the issue of security seriously. Those people who use the technology and information resources of company must be aware that they can be disciplined if they violate

this policy. Upon violation of this policy, an employee of company may be subject to discipline up to and including discharge. The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of the Cyber Security Policy, prior violations of the policy committed by the individual, state and federal laws and all other relevant information. Discipline which may be taken against an employee shall be administrated in accordance with any appropriate rules or policies and the company Policy Manual.

In a case where the accused person is not an employee of company the matter shall be submitted to the designated Security Administrator. The designated Security Administrator may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

## 9 Security Incident Handling Procedures

This section provides some policy guidelines and procedures for handling security incidents. The term "security incident" is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the company network. Some examples of security incidents are:

- Illegal access of a company computer system. For example, a hacker logs onto a production server and copies the password file.
- Damage to a company computer system or network caused by illegal access. Releasing a virus or worm would be an example.
- Denial of service attack against a company web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against other computer outside of the company network. For example, the system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Employees, who believe their terminal or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to their designated Security Administrator immediately. The employee shall not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.