Employee Computer Usage Security Agreement

General:

This information applies to all uses of AAPICO's computers and network and all methods of access, whether local or remote. The AAPICO Group of Companies (the Company) provides staff with computers, computing systems, and their associated communication systems to The Company's official business. Official business includes all authorized work connected with the, design, manufacture, finance, and operation of the Company. Its authorized programs in Oracle ERP, CAD/CAE design application including e-Mail and associated computer system. This access is for legitimate business purposes only. The confidential Information accessed through the Company's LAN, WAN or remote connection are monitored and recorded. Any misuse of disclosure, transmit, reproduce and distribute the confidential information that has a copyright, privilege is reported to management for appropriate disciplinary action.

These directives are intended to ensure that your use of the privileges authorized access does not violate:Statutes and Regulations;

- The Company's Code of Business Conduct; or
- The Company's policies and procedures related to external communications, information protection and computer systems.

Failure to follow the directives in this agreement:

- may subject you and/or the Company to liability; and
- will subject you to disciplinary action up to and including termination.

Responsibilities of Computer Users:

- User Accounts: All users shall accept responsibility for AAPICO's guidelines for protecting accounts.
- Software Protection: All users shall be responsible for complying with copyright, licensing, trademark protection, and fair-use restrictions.
- Virus-protection: All users must use the Company's virus protection software.
- Passwords: All users must adhere to the Company's Password and Authentication Policy.

Reasonable Use of Computers:

The Company allows the employee reasonable use of computing resources (for example, hardware, software, networks, and printers) for business purposes related employee's work assignment only.

Appropriate Use for the Company:

- Store your User ID and Password sheet in a safe, secure place. No one in Information Technology retains a copy of your password. If you lose or forget your User ID or password, call your support center to request a new one and change immediately at the first log on.
- Keep your ID and password secret. You are responsible for any access that occurs under your ID.
- Protect the Company's image, information and information systems. When you access e-Mail and send the message through the Company's connection, you are representing the Company. The Company may hold you liable for your actions.
- Do not provide access to anyone who has not been issued a User ID.
- Do not try to access unauthorized data or use operating system or program to access the confidential data, except as specifically authorized.
- If given a password, employee will immediately change the password
- Do not allow anyone else to have or use User ID, If the employee know that their password is compromised, employee will report this issue to their supervisor and Information System Security Point of Contact (ISSPOC)
- Do not write down password on any processor, personal computer, personal digital assistant (PDA), personal electronic device (PED), or on any magnetic or electronic media.
- Employee is responsible for all activity that occurs on owner individual account once User ID has been used to log on. If employee is a member of a group account, employee is responsible for all activity when employee is logged onto a system with that account.
- Employee will log completely off workstation, or use screen savers that require password to reactivate the workstation; any time employee leave the workstation unattended
- Scan all removable media (for example, disks, CDs, DVDs, thumb drives etc.) for malicious software (for example viruses, worms) before using it on any computer, system or network.
- Practice good housekeeping with all electronic equipment, including keeping food, beverages, or other contaminant away from computer and data storage media.
- Do not test or probe security mechanisms at either the Company's LAN or WAN sites.
- Do not make misleading, inflammatory, harassing or false statements on the e-mail messaging out about a person or a company.
- Do not keep any pornographic or sexually explicit material in individual storage, share storage and public folder.
- All electronic data are the Company Assets, Employee can not duplicate, reproduce, transmit or any method brings or sends out without the permission of the Company.
- Do not violate copyright laws, trademark law. Do not transmit material protected by copyright, trademark and send e-mail from the company to out site without the permission of the copyright owner.
- Before publishing Company information to out site, obtain approvals from President & CEO or On Behalf of President & CEO.
- Encrypt any information classified "Internal Use Only" or "Confidential" before sending it out site via e-Mail. Never send "Highly Restricted" information to out site

- “Internal Use Only” information can be used widely within the Company but should not be disclosed externally. An associate’s telephone number is an example.
- “Confidential” refers to information requiring more restricted access than “Internal Use Only.” Disclosing, altering or misusing confidential information can cause significant damage to the Company such as reducing profits or losing a competitive advantage. Operational business plans and customer contracts are examples.
- “Highly Restricted” refers to extremely sensitive business information to which access is the most restricted. Unauthorized disclosure, alteration or misuse of highly restricted information can cause severe damage to the Company. Product designs, acquisition plans and financial reports before public disclosure are examples.

- Do not use all removable media (for example, disks, CDs, DVDs, thumb drives etc.) for protection of publishing Company information. If you must use it, please get allow from your leader.

If you have questions about information classification, consult with your head of department.

If you become aware of or suspect that sensitive or classified Company information has been lost or disclosed or that unauthorized use of the Company's systems is taking place, immediately call the Information System Security Point of Contact- ISSPOC (Information Technology Department).

From time to time, the Company may update these directives and publish additional Computer Usage Security directives, which also apply to network both LAN WAN, remote users security and access at the Company. If you have questions about these directives, contact your immediate supervisor or IT representative.

You must sign this agreement certifying that you have read, understand and will comply with the Company’s Computer Usage Security directives. Failure to return the signed agreement may result disciplinary action and the loss of employee’s privileges at the Company. Failure to follow the directives in this agreement:

- may subject you and/or the Company to liability; and
- will subject you to disciplinary action up to and including termination.

Information Technology Department.

Employee Internet Access Agreement

The AAPICO Group of Companies (the Company) provides Internet access to a limited number of associates. This access is for legitimate business purposes only; recreational use is not permitted. Internet sites accessed through the Company's Internet connection are monitored and recorded. Any misuse of Internet privileges is reported to management for appropriate disciplinary action.

These directives are intended to ensure that your use of the Internet does not violate:

- Statutes and regulations;
- The Company's Code of Business Conduct; or
- The Company's policies and procedures related to external communications, information protection and computer systems.

Failure to follow the directives in this agreement:

- may subject you and/or the Company to liability; and
- will subject you to disciplinary action up to and including termination.

Store your Internet ID (same as User ID) and Password sheet in a safe, secure place. No one in Information Technology retains a copy of your password. If you lose or forget your Internet ID or password, call your support center to request a new one and change immediately at the first log on.

Keep your ID and password secret. You are responsible for any access that occurs under your ID.

Protect the Company's image, information and information systems. When you access the Internet through the Company's connection, you are representing the Company. The Company may hold you liable for your actions.

Do not access any sites that could be reasonably perceived to be offensive. See the Company's Policy for additional information.

Do not access any site that contains pornographic or sexually explicit material.

Do not access any site for non-Company business-related reasons.

Do not download games or other non-business files onto the Company's computers.

Scan all downloaded files for viruses using anti-virus software on your computer. If you suspect that a virus has infected your computer, call your local support center.

Do not test or probe security mechanisms at either the Company's Internet sites or other Internet sites.

Do not make misleading, inflammatory, harassing or false statements on the Internet about a person or a company.

Do not violate copyright laws. Do not copy material protected by copyright from or onto the Internet without the permission of the copyright owner.

Do not violate trademark laws. Do not use trademarks owned by our Company or another company without proper permission.

Before publishing Company information on the Internet, obtain approvals from President & CEO or On Behalf of President & CEO.

Encrypt any information classified “Internal Use Only” or “Confidential” before sending it over the Internet. Never send “Highly Restricted” information over the Internet.

- “Internal Use Only” information can be used widely within the Company but should not be disclosed externally. An associate’s telephone number is an example.
- “Confidential” refers to information requiring more restricted access than “Internal Use Only.” Disclosing, altering or misusing confidential information can cause significant damage to the Company such as reducing profits or losing a competitive advantage. Operational business plans and customer contracts are examples.
- “Highly Restricted” refers to extremely sensitive business information to which access is the most restricted. Unauthorized disclosure, alteration or misuse of highly restricted information can cause severe damage to the Company. Product design, acquisition plans and financial reports before public disclosure are examples.

If you have questions about information classification, consult with your head of department.

Do not discuss sensitive or classified Company information on bulletin boards or in “chat rooms”; they are public media.

If you become aware of or suspect that sensitive or classified Company information has been lost or disclosed or that unauthorized use of the Company's systems is taking place, immediately call the Information Security Center (Information Technology Department).

From time to time, the Company may update these directives and publish additional Internet directives, which also apply to Internet information security and access at the Company. If you have questions about these directives, contact your immediate supervisor or IT representative.

Accessing the Internet at the AAPICO Group of Companies

Within the Company, you must use one of these browser applications to access the Internet:

- Microsoft Internet Explorer 6.0 for all other systems.
- Mazola Fire fox 2.0 for all other systems.
- Google Chrome 42 for all other systems.

Contact your IT representative if you need browser software installed on your computer.

You must sign this agreement certifying that you have read, understand and will comply with the Company’s Internet directives. Failure to return the signed agreement may result disciplinary action and the loss of Internet privileges at the Company. Failure to follow the directives in this agreement:

- may subject you and/or the Company to liability; and
- will subject you to disciplinary action up to and including termination.

AAPICO

Virtual Private Network (VPN) Policy

1. Purpose

The purpose of this policy is to provide guidelines for Remote Access **Virtual Private Network (VPN)*** connections to the AAPICO **network.*** (* see Definitions section)

2. Scope

This policy applies to all AAPICO employees, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the AAPICO network. This policy applies to implementations of VPN that allow direct access to the AAPICO network from outside the AAPICO network.

3. VPN approval

a. Approved AAPICO employees and authorized third parties (vendor support, etc.) may utilize the benefits of a VPN, which is a **"user managed" service**.* Staff level and sub-contractor are NOT eligible to use VPN services.
b. VPN profiles will be created only at the request of a user's supervisor or manager, or departmental representative (consultants, and vendors) by submitting the appropriate **VPN Access Request form.** Additionally, the user must have read, understood, and acknowledged this policy before using the VPN service.
c. VPN profiles for non-AAPICO personnel (customers, vendors, etc.) must be requested by the head of unit area. Additionally, a copy of the VPN Request Form (including VPN Policy, and the confidentiality agreement) must be signed by the designated company Approving Authority. Accounts will not be issued until this process has been completed.
d. VPN profiles are typically created in 1 days. Multiple requests may take longer to process. Urgent requests will be reviewed on a case-by-case basis.

4. VPN user responsibilities

a. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the AAPICO network, and as such are subject to the same rules and regulations that apply to AAPICO owned equipment, i.e., their machines must be configured to comply with all AAPICO security policies.
b. All computers connected to AAPICO networks via VPN must use up-to-date virus-scanning software and virus definitions. Use of anti-virus software other than McAfee, Norton, or Trend must be approved for use by the AAPICO Information Security Officer (ISO). Additionally, all relevant security patches must be installed; this includes personal computers.
c. Users of this service are responsible for the procurement and cost associated with acquiring basic Internet connectivity, and any associated service issues. VPN services work best over broadband connections (cable modem or DSL). Use of dial-up Internet service is not recommended for regular VPN activity.
d. It is the responsibility of the employee or company with VPN privileges to ensure that unauthorized users are not allowed access to AAPICO networks.
e. VPN access is controlled using ID and password authentication. The password must comply with the AAPICO Password Policy. Each VPN user must have a unique profile. Shared profiles are not permitted.

5. VPN restrictions

a. AAPICO VPN services are to be used solely for AAPICO business purposes. All users are subject to auditing of VPN usage.
b. When actively connected to the AAPICO network, the VPN will force all traffic to and from the remote node through the VPN tunnel. To prevent potential 'back-doors' to the network dual (split) tunneling is NOT permitted. Only one network connection is allowed per VPN session.
c. AAPICO network access for non-AAPICO personnel will be limited to the resources to which they need access. Open access for these accounts will not be permitted. Additionally, VPN tunnels made to AAPICO must contain access restrictions at the remote termination point of the tunnel that prevent unauthorized access to the network. Tunnels should not be accessible by unauthorized users or the Internet.
d. All VPN gateways on the network will be set up and managed by AAPICO Network Services Group (NSG). NTG will provide approved users with appropriate client software.
e. User created VPN gateways will not be permitted on the network.
f. VPN users may be automatically disconnected from the AAPICO network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Artificial network processes are not to be used to keep the connection open. User connections to the VPN may be limited to an absolute connection time of eight (8) hours per day.

6. Definitions

a. A **Virtual Private Network (VPN)**, uses encryption and tunneling to connect users or branch offices securely over a public network, usually the Internet. Typically, a VPN will be configured to allow an authorized user to obtain remote desktop control of his/her office system. In the absence of a user controlled system on the network, permissions will be configured only for remote access to the systems for which the user has prior authorized access.
b. **"User managed" service** means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, and installing any required software on their personally owned remote access device (computer, laptop, palm device, etc.).
c. **Network** refers to the interconnected local and wide area networks maintained and managed by the AAPICO Network Services Group (NSG).

7. Enforcement

This policy regulates the use of all VPN services to the AAPICO network. To maintain security, VPN services will be terminated immediately if any suspicious activity is found. Service may also be disabled until the issue has been identified and resolved. Any AAPICO employee found to have intentionally violated this policy might be subject to disciplinary action, up to and including termination of employment. Non-AAPICO employees and vendors are directly responsible for damage as a direct result of policy violation. Intentional and non-intentional violation will result in termination of service and may result in revocation of contract.