

Recommended Computer Security Practices

ARC recognizes that many travel agencies may have already developed their own carefully planned internal Information Security Policies to address the issues surrounding business in the Electronic Age. The information stored in agency computer systems is obviously very sensitive to the agency, its customers, ARC, individual carriers, credit card companies and others. Such sensitive information should be protected from external and internal intrusion.

For those agencies that currently do not have an Information Security Policy, ARC strongly recommends that one be developed. A Security Policy has two purposes: protecting the agency from inappropriate resource use, security risks and legal liabilities, and ensuring that the agency's employees efficiently and effectively use resources for appropriate applications. A Security Policy should be clear and specific in detailing the guidelines that should be followed.

Below lists some of the more commonly included areas within an Information Security Policy:

- Network Acceptable Use guidelines
- Logging and reporting (e.g.: significant events, all user accesses, etc.).
- Virus Protection requirements
- Access restrictions (e.g.: inbound and outbound, specific applications or protocols, etc.).
- Protecting proprietary and sensitive information (e.g.: encryption, integrity, usage and disclosure issues, data ownership, etc.).
- Support resources (e.g.: who authorizes usage/access, internal problem reporting, etc.).

The use of layered security to protect your agencies data is the only route to take. Layer security protects your key network access points and protects against multiple types of attacks. Also if one layer of security is penetrated hopefully the other layers continue to protect your sensitive data.

Types of layers:

- Utilize current antivirus software, properly configure it, and update daily
- Utilize a software-based personal firewall
- Utilize a router/firewall device for your Internet connection
- Update your operating system with security updates
- Update your applications with security patches

When developing an information security policy or just securing your network ARC recommends reviewing information on the following web sites as a starting place:

- CIS - <http://cisecurity.org/>
- SANS – <http://www.sans.org/security-resources.php>
- NIST - <http://csrc.nist.gov/>
- PCI DSS for ARC and ARC Agents - <http://www.arccorp.com/legal/pci-data-security-standards.jsp>