

ScanAlert Inc.

Comprehensive Security Policy

For use by:

This information security policy and any other relevant security information should be disseminated to all system users including vendors, contractors, and business partners.

This information security policy should be reviewed and updated at least once per year.

All employees must sign an agreement verifying they have read and understood this document.

Table of contents

TABLE OF CONTENTS	2
INFORMATION TECHNOLOGY ASSETS USE	3
<i>Acceptable Use and Ethics</i>	3
<i>Password Policy</i>	3
<i>Remote Access</i>	3
<i>Information Sensitivity</i>	4
<i>Disciplinary Action</i>	4
NETWORK CONFIGURATION GUIDELINES	4
<i>Asset Configuration</i>	4
<i>Asset Deployment and Maintenance</i>	5
<i>Application Development</i>	5
<i>Access Control and Physical Security</i>	6
<i>Wireless Communications</i>	6
SECURITY PERSONNEL	6
<i>Information Security Officer</i>	6
<i>Incident Response</i>	6
<i>Incident Response Plan</i>	6
<i>Incident Response Team</i>	7

Information Technology Assets Use

Acceptable Use and Ethics

- All data contained on, or passing through corporate assets is subject to monitoring and remains the property of the corporation
- Under no circumstances is an employee authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing corporately-owned resources
- System users who receive a username and password must keep that information confidential and not allow use of their account by others
- System users who leave their workstations should enable a password protected screensaver or log off to prevent unauthorized access
- Employees must not use corporate accounts to post publicly accessible messages or posts
- System users must not tamper with or disable anti-virus software installed on their workstations
- System users are expressly forbidden to install any software on their workstations without prior approval from their supervisor
- System users must be very careful when opening email attachments, and should disregard unsolicited emails containing attachments
- System users may not perform vulnerability scans, monitor network traffic, or perform any action that is designed to elevate privileges or gain access to information that was not expressly intended for them
- System users must not reveal any information about corporate clients, employees, business practices, technology, schedules, or any other information not already publicly available to any outside resource or person without expressed permission from their supervisor
- System users must not use their corporate email accounts for purposes other than the conduct of corporate business. Forbidden actions include any and all forms of harassment, phishing, solicitation, spamming, forwarding chain letters and pyramid schemes, conducting personal business, and general personal correspondence

Password Policy

- Encrypted passwords should be enabled on any devices where it is not on by default
- Each corporate user should have a unique username and password that is not shared with any other user
- Corporate account passwords should be changed at least every 180 days
- A corporate accounts password should be strong and unique from previously used passwords
- Accounts should be locked after multiple password failures

Remote Access

- Any computer system used for remote access of company assets, not including public portions, must comply with corporate configuration guidelines
- Remote access software must use encrypted communications, be configured to use unique usernames and passwords for each user, and have any other security featured enabled

Information Sensitivity

Personal information is defined according to the California Civil Code Section 1798.29e and is an unencrypted combination of items 1 and 2:

1. First name (or first initial) and last name
2. Social Security Number, driver's license or identification card number, bank account or credit card numbers

Sensitive information is defined as any personal information items and also includes:

1. Usernames, passwords, addresses, phone numbers, and email addresses
- Sensitive information is not to be released unless prior written approval is received from the person whose information is in question
 - Sensitive information must be securely disposed of when no longer needed. Consult with the Information Security Officer (ISO) for specific disposal techniques
 - The full contents of credit card magnetic stripes (or chips, or other storage mechanism) may not be stored in any database, log files, or point of sale products
 - The card-validation code may not be stored in any database, log file, or point of sale product
 - All but the last four digits of credit card account numbers must be masked (ie. with X's or *'s) when displaying cardholder data
 - When account numbers are stored in a database (or logs, files, backups, etc.) they must be encrypted or truncated to the last 4 digits
 - 128-bit SSL (or other industry acceptable method) encryption should be used where sensitive information is transmitted over public networks
 - Encryption should be used when transmitting credit card account numbers over e-mail
 - Customer cardholder data should be sanitized before using in a development environment
 - The only personnel who should have access to customer sensitive information are those with explicit need-to-know
 - Sensitive information printed on paper or received by fax must be protected against unauthorized access
 - Employees that will need access to credit card account numbers should have a background investigation check
 - Third parties that have access to credit card data should be contractually obligated to comply with card association security standards

Disciplinary Action

Failure to comply with this security policy may, at management's discretion, result in disciplinary action up to and including termination of employment.

Network Configuration Guidelines

Asset Configuration

Firewalls

- Firewalls should be configured to "Deny" all traffic that is not explicitly "Allowed"
- Firewalls should filter both inbound and outbound (ingress and egress) connections, limiting them to that which is required to conduct business

Servers and Workstations

- Databases that store credit card numbers or personal information should be located on an internal network and protected by a firewall
- Publicly accessible web servers should be located on a DMZ so they are separated from the internal network by a firewall
- Mobile computers that connect to the internet must have a personal firewall and up-to-date anti-virus software installed
- AntiVirus scanners should be installed on all servers and workstations and should be updated with the latest virus definitions
- All development, testing, and production systems should be updated with the latest vendor security patches

Asset Deployment and Maintenance

- All changes to firewalls must be reviewed and authorized by the Information Security Officer and logged for future reference
- Changes to the production environment should be authorized and logged before being implemented
- When an employee leaves the company, that employee's corporate user accounts and passwords should be immediately revoked
- System user accounts should regularly be reviewed and audited for malicious, obsolete, and unneeded accounts
- Inactive accounts should automatically be disabled after a pre-defined period
- Remote maintenance accounts should be enabled when needed and disabled when the maintenance process is completed
- All access to cardholder data should be logged
- Successful and unsuccessful login attempts and the accessing of the audit logs should be logged
- System clocks should be synchronized, and log files should contain date and time stamps
- The firewall, router, wireless access points, and authentication server logs should be regularly reviewed for unauthorized traffic
- Audit logs should be regularly backed up, secured, and retained for at least three months online and one year offline for all critical systems
- Wireless analyzers should be periodically run to identify all wireless devices
- Vulnerability scans or penetration tests should be performed on all applications and systems before they are put into a production environment
- All internet points of presence should be scanned daily using ScanAlert's HACKER SAFE service, which provides intrusion detection and prevention functionality
- Before going into production, all devices must undergo a lockdown procedure where unnecessary or default services, protocols, settings, accounts, and passwords are changed or disabled
- Only secure, encrypted communications should be used for remote administration of production devices

Application Development

- Software and application development should follow industry best practices and include information security throughout the development life cycle
- Web application should be designed using accepted security guidelines such as the OWASP Guide
- Web application authentication processes should not reveal if usernames or passwords are correct - only that a login failed or was successful
- User information, including credit card data that is stored in cookies, should be encrypted
- All web application input validation should be performed by the server, not by the client
- The minimum information to be required upon authentication should be a unique username and password

Access Control and Physical Security

- Multiple physical security controls should be implemented to prevent unauthorized access to datacenters
- Equipment and media containing sensitive information should be physically protected from unauthorized access
- The distribution and disposal of backups and other media containing sensitive information should be in accordance with a procedure approved by the Information Security Officer
- Media that contains sensitive information should be inventoried and securely stored
- Media that contains sensitive information should be deleted, shredded, or degaussed before disposal

Wireless Communications

- All wireless access points must be configured with encryption, MAC filters, or technology that limits access to those devices that are explicitly authorized
- Networks with wireless access should be separated by a firewall from networks that process credit card information
- Wireless access points that support WPA should be configured to use it
- Wireless communications should be encrypted with WPA, VPN, 128-bit SSL, or WEP
- Wireless communications encrypted with WEP should be 128-bit strength and shared WEP keys rotated quarterly at a minimum
- All wireless devices should be restricted to access only authorized access points, gateways, and other wireless devices

Security Personnel

Information Security Officer

For daily security matters, an Information Security Officer, who is an employee of the company is appointed. The Information Security Officer is responsible to oversee that the provisions of this Security Policy are performed as needed for all system users.

The assigned Information Security Officer is _____.

ScanAlert customers subscribing to the HACKER SAFE level of service can elect to have experienced ScanAlert personnel act as their Information Security Consultant for security and security policy implementation matters, as well as serve as an Incident Response Team in the case of a suspected information security incident.

Incident Response

Security incidents should be handled according to the security incident response plan, and that plan should be disseminated to appropriate parties.

Security incidents should be immediately reported to the Information Security Officer.

An incident response team will be appointed by the Information Security Officer, and will be ready for deployment in case of credit card data compromise.

Incident Response Plan

If a compromise is suspected:

1. Alert the Information Security Officer who will perform an initial investigation and notify the Incident Response Team if necessary.

2. Follow the steps recommended by VISA
http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html

Incident Response Team

ScanAlert HACKER SAFE level customers can utilize ScanAlert's incident response team by sending support requests through the online Management Console by logging in at <https://www.scanalert.com/customer/Login.sa>