NHCAA
National Health Care Anti-Fraud Association®

Information Security Structure and Policy

Purpose

The purpose of this policy is to implement effective administrative, technical and physical safeguards for NHCAA's information technology infrastructure and for any personal information of its members and customers collected within the normal course of its business.

IT Infrastructure

General Information Technology Services & Support

There are a number of information systems that are critical to the routine business function of NHCAA.

BAIS2 is NHCAA's service provider for Information Technology (IT) support and maintenance.

BAIS2 supports NHCAA's full user and application environment. Microsoft Office 365 is utilized as NHCAA's email solution and optionally for Office licensing. BAIS2 coordinates and manages user rights and access to the system, computers and peripherals. Virus protection is also provided by BAIS2 in conjunction with necessary software vendor support contracts through Panda Cloud Security & Meraki Network Security.

All NHCAA's computers, printers, scanners, servers, unique devices, routers, switches, firewalls, VPN connections, tunnels, bridges, and connections to outside systems are supported by BAIS2 who also serves as the first point of contact for all such equipment and devices, including those under support contracts with other vendors. BAIS2 coordinates with any outside vendors for necessary support on equipment with outside support contracts.

BAIS2 employs 24/7 monitoring of NHCAA's information systems and services and provides immediate (1hr Emergency SLA) response to all alerts.

A ticketing system is utilized for submission, handling, and monitoring of routine computer and user issues as they arise. Phone support is also available as required.

Once a quarter BAIS2 performs routine updates and maintenance on all machines. At the end of every year, BAIS2 develops a comprehensive computer report that includes

recommendations for hardware replacement as well as any other necessary or appropriate system upgrades.

Microsoft Windows Server (Shared Files, User & Computer Management)

System Redundancy, Monitoring, and Maintenance

The Microsoft Windows Server provides basic redundancy of hard disks through a RAID (Redundant Array of Independent Disks) configuration, allowing it to remain operational in the case of up to one hard drive failure. A Remote Monitoring System is currently in place to monitor all critical conditions on the server (not just drives). This system alerts BAIS2 of impending system issues (such as hardware failure), so immediate action can be taken to prevent loss of functionality, and data. Maintenance on this server is configured to offer 4-hour response times in the case of a critical system failure (warranty provided by Dell).

Data Management

Shared files are maintained on a file server housed in the NHCAA office. The shared file structure is divided into two primary areas, NHCAA Archive and NHCAA Current Files.

Software Patch Management and Anti-Virus Software Update Process

NHCAA uses multiple software applications to accomplish software and system patch management for all Windows and third party computer applications. Patch Management application is installed and configured on NHCAA's onsite windows server. Windows and security Patches are deployed to NHCAA's computer systems as needed automatically by the Windows Server.

Panda Endpoint Protection Anti-Virus is deployed on all NHCAA computer systems and servers. Anti-virus software definition updates are scheduled to automatically download and install daily. Antivirus policies are managed from centralized console by BAIS2's Helpdesk/NOC team. Panda creates an alert as soon as there is a detection of a virus or malware attack on NHCAA's computer systems.

The Meraki Network Security product updates automatically per Meraki's managed update schedule. Third party applications are handled through Ninite on an as-needed basis.

Managing Computer and User accounts

Computer system access accounts are created with minimum privileges required for new employees. NHCAA management informs BAIS2 whenever an employee leaves employment so his or her computer access account could be disabled immediately.

Data Back Up and Protection

In order to protect the NHCAA Current Files, an online backup service called CrashPlan Enterprise is run on a nightly basis. This service provides the ability to store the backed up data in an encrypted fashion outside NHCAA offices, in order to ensure reliable data recovery in the event of a major disaster event affecting NHCAA offices (flood, fire, theft, earthquake, etc.). The data is fully encrypted via industry-standard encryption algorithms before it leaves the network and is stored in BAIS2's redundant datacenter, located in Riverdale Park, MD. In the event of system failure requiring access to the online data, all files are available for download via standard internet connections. Additionally, a physical copy of the data can be facilitated by BAIS2 by extracting the data from the online vault and placed in a USB drive that can be shipped to NHCAA for recovery purposes.

Microsoft Windows Server Destruction/Failure

In the event the Microsoft Windows Server is damaged, corrupted or accidently or intentionally deleted, an online data restore process will be initiated from the BAIS2 backup server to restore from the last successful backup.

If the NHCAA physical office location is unavailable, NHCAA will immediately transition to a telework model and lease a temporary server form BAIS2. DNS services for the affected system will be modified to point to the new temporary server until normal operations can be restored. BAIS2 will be the initial contact and should be able to provision a Windows based file server, and any outage should be recoverable within three business days.

System Security

Network-Level Security

Network level security is handled by a Meraki MX64 security appliance with an Advanced Security license. The Meraki appliance monitors network traffic in and out of the network and performs active threat detection on outside traffic. The appliance also provides malware scanning, provided by Source Fire on traffic entering the network. The appliance serves as the gateway firewall for entering the network and regulating traffic

and network access. Content filtering is enabled on the appliance to restrict potentially malicious sites.

Antivirus Security

Antivirus software and protection is provided by Panda Security Group. Panda installs client-based security on each workstation and server in the office (and mobile computers). This protection is tied back to a central cloud controller for continual updates, monitoring, and logging of issues and potential security threats.

Server & Device Level Security

The centralized Active Directory server provides user/device network authentication and regulates access to files per defined security permissions. Additionally, each server/workstation has a built in firewall and malware scanner that runs in parallel to Panda Security.

Telecommunications & Internet Services

Vector Data Systems provides the following telecommunication services to NHCAA:

- Dial tone service (SIP trunking) for NHCAA's IPOffice phone system
- Internet access for NHCAA's office
- Resold Verizon fax line

Vector Data Systems actively monitors the dial tone service and internet access and in the event of a service disruption or failure, they will proactively reach out to the Sr. Manager of Operations to coordinate problem resolutions.

In an emergency situation, power failure, or weather emergency, Vector Data Systems can assist with redirecting calls to a different location, an emergency mailbox, or a recording.

NHCAA Website

The NHCAA website is maintained and hosted by BAIS2. In the event that the NHCAA website becomes inoperable the Senior Manager of Information Systems and Services along with the Sr. Manager of Operations will serve as the onsite liaison with BAIS2 to

coordinate restoration efforts. NHCAA's website operates via an HTTPS protocol for secure internet communication.

Microsoft Office 365

Microsoft Office 365 is used by NHCAA to provide email and staff calendaring services. The Office 365 email service resides on Microsoft's secure cloud platform.

At the service level, Office 365 uses the defense-in-depth approach to provide physical, logical, and data layers of security features and operational best practices related to ensure physical security, data security, and administrative and user controls.

Microsoft Office 365 is a global service providing continuous compliance. Microsoft Office 365 is verified to meet requirements specified in ISO 27001, EU model clauses, HIPAA BAA, and FISMA.

NHCAA's Microsoft Office 365 includes Exchange Online Protection for email security, and focuses on spam detection. NHCAA uses Microsoft's email security to provide comprehensive protection against many email-born threats. NHCAA utilizes Backupify to back-up the email system.

Abila netFORUM Enterprise (Association Management System)

netFORUM functions as the Association Management platform for NHCAA. This encompasses our customer (members, vendors and prospects) data, event data, expo data, accounting data, membership records, certification records and the public facing Website for event transactions and member login.

netFORUM Enterprise is an independent solution hosted in a secure Network Operations Center (NOC). Production databases are backed up in full daily and replicated off site. Full system backups occur weekly. In the event of data loss, the RTO (Recovery Time Objective) from Data Backup should be less than 2 hours.

Merchant Services

PayFlow Pro provides the payment gateway and virtual terminal services for the secure processing of credit cards. These gateways are hosted by PayPal and securely

connected through Abila netFORUM. They may be accessed via a standard Web browser for virtual terminal and reporting.

Protection of Member and Customer Information

Collection and Use of Personal Information

In the course of providing services, NHCAA collects personal information of its members and customers. This information may include name, title, organization, telephone numbers, fax number, email and mailing address voluntarily provided by such individuals.

NHCAA does not disclose to third parties any information it gathers from individuals. The only exception to this policy is that NHCAA provides its Premier Supporting Members and exhibitors with a pre-conference and post-conference mailing list of attendees for its Annual Training Conference. Each list is limited to one-time use. These lists disclose name, title, organization and mailing address; email addresses and phone numbers are not provided. The attendee list, minus the mailing address, is also made available to Annual Training Conference attendees. NHCAA does not make its attendees list available to any other third party.

NHCAA also collects information through its website, and its Privacy Policy is detailed on the site.

NHCAA Credit Card Information Security Policy

Purpose

Credit card data is highly sensitive and confidential. The purpose of this policy is to help ensure the NHCAA and NHCAA Institute (collectively, “NHCAA”) are adequately protecting the privacy and security of its customer’s credit card information.

NHCAA collects credit card information voluntarily provided by individuals through its website and other means to process payment for its various products, services and education programs. Credit card number are encrypted and protected with encryption software SSL when transmitted to NHCAA. Credit card information is not stored or re-used in any manner. Only authorized staff personnel with specific IDs and passwords can access credit card information solely for the purpose of processing authorized transactions.

Scope

All employees of NHCAA and employees and agents of NHCAA contractors and consultants having access to credit card data or involved in the storing and/or processing of credit card payments (hereinafter the "Users") must upon hire, and on an annual basis thereafter, agree to adhere to this policy.

Any proposal for a change in a process (electronic or paper) related to the storage, transmission or processing of credit card data must be brought to the attention of, and be approved by, the Chief Executive Officer.

General Requirements

- Only Users who are properly trained may accept and/or access cardholder information or devices or systems which store or access cardholder information. Training will be provided by the Senior Manager of Information Systems and Services.
- Users may not allow third party access to NHCAA systems using accounts assigned to them.
- All Users must be assigned a unique ID before allowing them to access systems or cardholder data.
- Users must maintain strong passwords that are not known by others. Passwords should be updated every 90 days.
- Users will not use vendor-supplied defaults for system passwords and other security parameters.
- When accessing NHCAA systems from public locations, Users will ensure sensitive information is not visible to unauthorized individuals at any time.
- Storage of credit card data on any computer, server or database, including excel spreadsheets is prohibited.
- Once a payment transaction has been fully processed, physical credit card data shall be permanently deleted or redacted from all records such that account information is unreadable and cannot be reconstructed. Papers containing credit card numbers that are being disposed of must be shredded.

- If temporarily maintained to complete the payment transaction, physical cardholder data must be locked in a secure area. If a secure location is not available within your department, contact the Sr. Manager of Operations for alternative options.

- Credit card data should not be left visible on a computer screen or on papers on a desk.

- Never send cardholder information via email. Credit card numbers must not be transmitted in an insecure manner, such as email, unsecured fax or through the mail.

- Fax transmittal of cardholder data is permissible only if the receiving fax is located in a secure environment. The fax machine must be checked on a regular basis

- The events and circumstances of a suspected security breach which could negatively affect cardholder information must be immediately reported to the Senior Manager of Information Systems and Services and the Chief Executive Officer.

Procedure for known or suspected breach of credit card security

Any known or suspected breach of credit card security shall be immediately reported to the Sr. Manager of Operations and the CEO. At the direction of the CEO, the individual whose credit card information was or may have been acquired by an unauthorized person shall be notified of the nature of the breach and any steps NHCAA has taken in response to the incident. NHCAA's insurance carrier shall also be notified of the breach.

There shall be a mandatory post-incident review of events and actions taken with a view to determining whether any changes to NHCAA security practices should be made to improve security.