SCIGON
Technology Consulting | Engineering | Products

Information Systems Audit Policy/Procedures

Contents

Response Team

Name	Roles	Emails	Office/Mobile
John Scifers	CEO/Chief Technologist/Response Team Lead	jscifers@scigon.com jscifers@gmail.com	847-453-8890 630-544-9798
Eugene Gonchar	COO/Response Team Lead Backup	egonchar@scigon.com egonchar@hotmail.com	847-453-8885 224-212-0505

Purpose

Audit controls and effective security safeguards are part of normal operational management processes to mitigate, control, and minimize risks that can negatively impact business operations and expose sensitive data. Operational, process, and security audits help to ensure that proper controls are sufficient and effective at providing information confidentiality, protecting Personally Identifiable Information (PII), ensuring system availability, and fostering a higher degree of data integrity. This policy sets forth SCIGON's practices regarding information system related audits

Scope

This policy applies to all SCIGON personnel involved in the creation, deployment, operations, or support of application and system software used throughout the Company.

Current State

SCIGON does not store, process or otherwise handle personally identifiable information, Protected Health Information (PHI), or other sensitive data for any partner or customer. Personally identifiable information or Protected Health Information (PHI) of SCIGON personnel, and sensitive company data, is stored in an encrypted format in systems to which only SCIGON's management team has access.

Policy

General

A regular and proactive audit policy helps to manage and reduce risks to SCIGON's information systems, the data it manages, and the users it services.

The Chief Technologist or designee uses security audits to assist in ensuring security controls and safeguards are appropriate, sufficient, and effective at treating operational and security risks. Within this framework, the Chief Technologist works with SCIGON's management team to define:

- **Resources** – Identify resources to perform the audit
- **Audit Scope** – Define the scope of the systems being certified and their boundaries
- **Requirements** – Prepare a list of security and/or privacy requirements that are relevant
- **Description** – Technically and functionally describe the system including functional systems description, system operational environment, criticality, system architecture, interfaces, data flow, and any data privacy / system security requirements

Audit Scope

The Chief Technologist considers the following when determining organizational audit scope:

- **Security Vulnerabilities** – Identifies security vulnerabilities using reputable outside sources.
- **Risk Evaluation** – Identifies methods for evaluating vulnerabilities and assigning risk ratings to systems. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. Vulnerabilities are considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or result in a potential security compromise or breach if not addressed. Examples of critical educational systems include premise security, general financial, and personnel systems. It also includes any public-facing system, database, or transmission mechanism around sensitive information or PII.
- **Administrative Safeguards** – Defines protocols, policies, procedures, training plans and other administrative security controls (e.g. – these policies are a good example of a procedural control) useful to an auditor in comparing against a standard of operation.
- **Penetration Testing** – Evaluates whether penetration testing may be used to identify system vulnerabilities. Examples of penetration testing include evaluations of firewalls and other external network entry points, analysis of software applications and websites, review of logging and account procedures, social engineering tests of staff.

Audit Procedures

Access to audit tools shall be controlled and restricted to prevent possible misuse or compromise resources and log data. Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimize disruptions to normal business operations.

Annually

On at least an annual basis, the Chief Technologist or designee shall:

- Confirm that all SCIGON computer equipment has been configured to support automatic Operating System updates
- Confirm that all SCIGON computer equipment has been configured with anti-virus/anti-malware that actively uses background full system scans, automatic virus/malware definition updates, e-Mail attachment scans, and application scans
- Inventory all key business technology equipment and other information resources
- Inventory all key business documents and data to ensure storage and format conforms to SCIGON's security policies
- Assess safeguards with respect to preserving the integrity of SCIGON's business operations and sensitive data under SCIGON's control
- Ensure that relevant personnel understand and continue to conform to all security-related policies and procedures.
- Confirm that all user access controls are configured to ensure administrative access to computer equipment only by the Chief Technologist or COO, with limited privileges for normal User accounts
- Review policies and procedures to ensure compliance with current industry practices and a security posture commensurate with SCIGON's handling of data.
- Assess whether any SCIGON systems currently or will store sensitive non-SCIGON data. In the event SCIGON begins storing, processing, transmitting, or otherwise handling sensitive non-SCIGON data, the audit will include an assessment by a third-party auditor, penetration tester, or other appropriate professional, to ensure the security of that data. If such an audit identifies vulnerabilities, effective remediation will be undertaken.

As Needed

New Equipment

Chief Technologist or designee shall ensure that new equipment is:

- Configured with Administrative account User Access only for the Chief Technologist and COO, with limited privileges for normal User accounts
- configured with installation and configuration of effective anti-virus/anti-malware that actively uses background full system scans, automatic virus/malware definition updates, e-Mail attachment scans, and application scans
- Utilizing relevant application-based security in eMail clients, business applications, and other device-based software installed on that equipment

Emergent Security Vulnerabilities

Chief Technologist or designee shall ensure that emergent security vulnerabilities affecting systems, software and infrastructure used by SCIGON have been addressed.

Enforcement

Any SCIGON personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their relationship terminated.

Definitions

Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;

Information Resource - The data and information assets of an organization, department or unit.

Safeguards - Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.
Sensitive data - Data that is encrypted or in plain text and contains PII or PHI data.