SCIGON
Technology Consulting | Engineering | Products

Security Policies: HR, Logical Access, Physical Security

Contents

Key Contacts/ 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
Anna Kousgaard	Marketing/Communications Manager	akousgaard@scigon.com Annakousgaard1@gmail.com	847-951-2662
Julia Fosco	Office Manager/Communications Backup	jfosco@scigon.com Julia.fosco@gmail.com	877-554-5678 847-393-6341
Caitlin Nowlan	Administrative/Support	cnowlan@scigon.com cnowlan@gmail.com	847-453-4386 708-476-9368

Purpose

SCIGON Solutions, Inc. ("Company") stores internal personal and sensitive information. Information security is very important to help protect the interests and confidentiality of the Company and its customers. Information security is achieved by technical and physical means, and must also be enforced and applied by people. This policy addresses these security issues.

The procedures accompanying this policy are split into 3 key areas:

- Human Resources/people-focused security policy
- Logical access security policy
- Physical access security policy

The following general guidelines govern these policies:

1. Prior to granting access to information or information systems, checks must be made to ensure that the individual is suitable for access to Company information systems.
2. Users must be trained and equipped to use systems securely and their access must be regularly reviewed to ensure it remains appropriate.
3. When a user's requirement for access to information or information systems ends (i.e. when a user terminates their employment with SCIGON, or changes their role so that access is no longer required), access needs to be removed in a controlled manner.

This policy also addresses third party access to Company information systems (e.g. contractors, service providers, agencies and partners).

Scope

This policy applies to any person that requires access to Company information systems or information of any type or format (electronic and paper documents that have not yet been converted to electronic format and shredded).

The policy applies automatically to all SCIGON personnel, partners, customers or vendors with access to Company systems.

Where access is to be granted to any third party (e.g. contractors, service providers, agencies, partners) compliance with this policy must be agreed and documented. Responsibility for ensuring this lies with the Company employee that initiates this third party access.

Policy Statement

SCIGON will ensure that individuals are checked to ensure that they are authorized to access Company information systems. Except for Company's Executive Management team, no individual will be issued keys or codes to physically secured areas or storage equipment. SCIGON will ensure that users are trained to use information systems securely. SCIGON will ensure that user access to information systems is removed promptly when the requirement for access ends.

SCIGON understands that to reduce the risk of theft, fraud or inappropriate use of its information systems, anyone that is given access to Company information systems and physically-secured facilities **must**:

- Be suitable for their roles.
- Fully understand their responsibilities for ensuring the security of the information.
- Only have access to the information they need.
- Request that this access be removed as soon as it is no longer required.

This policy must therefore be applied prior, during and after any user's access to information or information systems used to deliver Company business. Access to Company information systems will not be permitted until the requirements of this policy have been met.

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 Compliance

If any user is found to have breached this policy, they may be subject to disciplinary procedures, including termination of employment. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

Personnel who do not understand the implications of this policy or how it may apply to their work, should seek advice from SCIGON's President or COO.

Policy Governance

The following table identifies who within SCIGON is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

Responsible – the person(s) responsible for developing and implementing the policy.
Accountable – the person who has ultimate accountability and authority for the policy.
Consulted – the person(s) or groups to be consulted prior to final policy implementation or amendment.
Informed – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	CEO/Chief Technologist/Response Team Lead COO/Response Team Lead Backup Office Manager
Accountable	CEO/Chief Technologist/Response Team Lead
Consulted	CEO/Chief Technologist/Response Team Lead COO/Response Team Lead Backup Marketing/Communications Manager Office Manager/Communications Backup Administrative/Support
Informed	All SCIGON personnel

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Policy review will be undertaken by CEO/Chief Technologist/Response Team Lead

Human Resources Security Policy

References

The following SCIGON documents are directly relevant to this policy:

- Business Conduct Policy
- Electronic Telephonic Communication Policy
- Employee onboarding documents

The following SCIGON documents are indirectly relevant to this policy:

- Disaster Recovery Plan & Policy
- Business Continuity Plan and Emergency Procedures
- Data Breach Policy

Personnel with Access to Client or Partner Systems

Personnel with access to client or partner systems, such as SCIGON consultants who provide services on-site at client or partner location(s) using client or partner equipment, facilities and systems, must agree to, confirm understanding of, and conform to security-related policies and practices of those partners or clients before they initiate performance of work using client or partner equipment, facilities and systems.

Awareness and Background Check Considerations

- All SCIGON personnel must be aware of, understand, and agree to the following policies
    - Business Conduct Policy
    - Electronic Telephonic Communication Policy
- Background verification checks must be carried out on all users with access to SCIGON systems.
- All users must receive appropriate information security awareness training and regular updates in related organizational policies and procedures as relevant for their role.
- All access rights of users of Company information systems shall be removed in a timely manner upon termination or suspension of their employment, contract or agreement.

Prior to System Access

The Company must ensure that potential users are recruited in line with the Company's recruiting and onboarding practices for the roles they are considered for and to reduce the risk of theft, fraud or misuse of information or information systems by those users.

Roles and Responsibilities

Decisions on the appropriate level of access to information or information systems for a particular user are the responsibility of the CEO/Chief Technologist/Response Team Lead, COO/Response Team Lead Backup and Office Manager.

The Office Manager, under the direction of the CEO/Chief Technologist/Response Team Lead and COO/Response Team Lead Backup, is responsible for ensuring that creation of new users, changes in role, and termination of users is accomplished in a timely manner, using the standard processes.

User Screening

Background verification checks must be carried out on all personnel. The level of such checks must be appropriate to the business requirements, the classification of the information to be accessed, and the risks involved.

- The basic requirements for Company employment includes:
- Minimum of two satisfactory references.
- Completeness and accuracy check of employee's application form.
- Confirmation of claimed academic and professional qualifications.
- Identity check against a passport or other government-issued document that contains a photograph.

Users who require potential access to sensitive company information must meet the following minimum requirements:

- Minimum of 2 satisfactory references.
- Completeness and accuracy check of employee's application form.

- Confirmation of claimed academic and professional qualifications.
- Identity check against a passport or other government-issued document that contains a photograph.
- Verification of full employment history for the past 3 years.
- Verification of nationality and immigration status.
- Verification of criminal record

Terms and Conditions of Employment

As part of their obligation, personnel must agree and sign the terms of their employment contract or equivalent instrument, which shall incorporate SCIGON's policies related to information security. This must form an integral part of the conditions of employment.

Each employee must sign a statement that they understand the nature of the information they access, that they will not use the information for unauthorised purposes and that they will return or destroy any information or assets when their employment terminates.

Applying the Policy – During Access to Information or Information Systems

During Continued Employment

The Company must ensure that all users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their work, and to reduce the risk of human error. It is also necessary that user changes in role or business environment are carried out in an orderly manner that ensures the continuing security of the information systems to which they have access.

Management Responsibilities

Office Manager must notify the COO in a timely manner of any changes in a user's role or business environment, to ensure that the user's access can be changed as appropriate. Processes must ensure that access to information systems is extended to include new user requirements and also that any access that is no longer needed is removed.

Any changes to user access must be made in a timely manner and be clearly communicated to the user.

All management personnel will ensure that personnel performing services under their direction do not undertake any work that requires SCIGON equipment, facilities or technology in the storage, processing or transmission of sensitive information of SCIGON's clients or partners.

Information Security Awareness, Education and Training

All users with access to sensitive information must receive appropriate information security awareness training and regular updates in related statute and organizational policies and procedures as relevant for their role.

Applying the Policy – When Access to Information or Information Systems is No Longer Required

Secure Termination of Employment

Termination of employment may be due to resignation, change of role, suspension or the end of a contract or project. The key requirement is that access to SCIGON information assets is removed in a timely manner when no longer required by the user.

Termination Responsibilities

The Office Manager must notify the COO in a timely manner of the impending termination or suspension of employment so that their access can be confirmed as suspended.

Return of Assets

The Office Manager must ensure that users return all of the organization's assets in their possession upon termination of their employment, contract or agreement. This must include any copies of information in any format.

Removal of Access Rights

The COO must ensure that all access rights of users of Company information systems shall be removed in a timely manner upon termination or suspension of their employment, contract or agreement.

Logical Access Security Policy

Definition

Access control rules and procedures are required to regulate who can access SCIGON information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Company information in any format, and on any device.

References

The following SCIGON documents are directly relevant to this policy:

- Business Conduct Policy
- Electronic Telephonic Communication Policy
- Employee onboarding documents

The following SCIGON documents are indirectly relevant to this policy:

- Disaster Recovery Plan & Policy
- Business Continuity Plan and Emergency Procedures
- Data Breach Policy

Roles and Responsibilities

Administration

Office Manager, COO and Chief Technologist must be aware of, understand, and agree to administration of measures under this policy. All personnel with access to SCIGON systems must be aware of, understand, and agree to practices under this policy. The Office Manager is accountable for ensuring that all personnel comply.

Unusual Access Activities Investigation

Chief Technologist or designee must investigate any unusual system access activities observed in logs, reported to helpdesk@scigon.com, or indicated through system-generated security alerts.

User Access Review

COO or designee must perform a biannual review of User Access. This review must include:

- review of existing accesses for continued necessity and appropriateness of level
- review of user accesses for inactivity
- confirm continued necessity, taking into account:
    - continuing employment
    - personnel roles and responsibilities and/or any changes
    - access levels and/or any needed changes

Access Levels

SCIGON shall employ the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions

Passwords

Choosing Passwords

Passwords are the first line of defense for SCIGON's systems and together with the user ID help to establish that people are who they claim to be. A poorly chosen or misused password is a security risk and may impact the confidentiality, integrity or availability of our computers and systems.

A *weak password* is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of children and pets, car registration numbers and simple patterns of letters from a computer keyboard.

A *strong password* is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.

All personnel with access to SCIGON systems must use strong passwords with a minimum standard of:

- At least seven characters.
- Contain a mix of alpha and numeric, with at least one digit
- More complex than a single word (such passwords are easier for hackers to crack).

Protecting Passwords

It is of utmost importance that the password remains protected at all times. The following guidelines must be adhered to at all times:

- System-generated passwords (e.g. email/Exchange) are to be changed upon first use
- Never reveal passwords to anyone.
- Never use the 'remember password' function.
- Never write passwords down or store them where they are open to theft.
- Never store passwords in a computer system without encryption.
- Do not use any part of username within the password.
- Do not use the same password to access different SCIGON systems.
- Do not use the same password for systems inside and outside of work.

Personnel Access

User Access Management

User access control procedures must be followed for each application and information system to ensure authorized user access and to prevent unauthorized access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User access rights must be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

User Responsibilities

It is the responsibility of all SCIGON personnel/users to prevent their userID and password being used to gain unauthorized access to SCIGON systems by:

- Following the Password Policy
- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing Office Manager of any changes to their role and access requirements.

Application and Information Access

Access within software applications must be restricted using the security features built into the individual product. Only managers will have administrative access to SCIGON-owned or SCIGON-licensed products. Users with administrative access are responsible for granting access to personnel for these systems. The access must:

- Be compliant with the User Access Management section and the Password section above.
- Be separated into clearly defined roles.

- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.

Physical Access Security Policy

Definition

Physical access security rules are required to regulate who can access SCIGON facilities and physically-secured systems, documents and equipment within those facilities. The granting, controlling and monitoring of the physical access to SCIGON facilities is extremely important for an overall security program. This policy applies at all times and should be adhered to whenever accessing Company facilities.

References

The following SCIGON documents are directly relevant to this policy:

- Business Conduct Policy
- Electronic Telephonic Communication Policy
- Employee onboarding documents

The following SCIGON documents are indirectly relevant to this policy:

- Disaster Recovery Plan & Policy
- Business Continuity Plan and Emergency Procedures
- Data Breach Policy

Roles and Responsibilities

Administration

Office Manager, COO and Chief Technologist must be aware of, understand, and agree to administration of measures under this policy. All personnel with access to SCIGON systems must be aware of, understand, and agree to practices under this policy. The Office Manager is accountable for ensuring that all personnel comply.

Issuance of Keys and Codes

COO and Chief Technologist are the sole personnel authorized to issue keys to employees.

Physical Access Safeguards

Physical access safeguards help to establish best practices for the appropriate granting, controlling, and monitoring of physical access for SCIGON facilities. Physical access safeguards include the following:

- All SCIGON facilities must be physically protected in proportion to the criticality and confidentiality of their function
- All SCIGON facilities must have physical access controls in proportion to the importance, sensitivity, and accountability requirements of the data and systems housed in that facility.

- Access to SCIGON facilities will only be granted to authorized personnel whose job responsibilities require such action.
- Keys must not be shared with others.
- Keys that are no longer required must be returned to the COO or Chief Technologist.
- Lost keys must be reported to the COO or Chief Technologist as soon as possible.
- Visitors must be escorted in all SCIGON work spaces.
- All physical security systems must comply with applicable regulations, including but not limited to, building codes and fire prevention codes.
- Keys must not have identifying information.

Procedures

General Workspace Access

SCIGON's general office workspace is a locked facility. Keys are issued by the COO and Chief Technologist only to employees assigned to regular work in this space who have authority to access that space.

Confidential Area Access

Physical access to records containing sensitive information, and storage of such records and data in locked facilities, storage areas, or containers shall be restricted:

- Only SCIGON's COO and Chief Technologist are authorized to possess keys to confidential areas, such as internal offices.
- Only SCIGON's COO and Chief Technologist are issued codes, keys and location information for accessing the offsite safe that houses backup media for key business data and documents.

Sensitive IT resources located in unsecured areas shall be secured to prevent physical tampering, damage, theft, or unauthorized physical access to sensitive information

Visitors

Visitors must be escorted in all SCIGON work spaces.

Portable media

Portable media, such as portable hard drives, USB drives, DVDs, and CDs that contain sensitive Company documentation and data must be in the personal possession of the COO or Chief Technologist, or must be stored in the offsite safe that houses backup media for key business data and documents.

Return of Keys

The COO or Chief Technologist must ensure that personnel return any keys upon termination of employment.