Information Security Policy

Last Updated Feb 2nd, 2024

Searchie Inc

Purpose

Searchie Inc's Information Security Policy has been developed to: establish a general approach to information security and the minimization of information misuse, compromise or loss; document security processes and measures; uphold ethical standards and me et the company's regulatory, legal, contractual, and other obligations; control business risk; and ensure that the appropriate company image and reputation is presented.

Policy

Training

Management shall ensure that employees, contractors and third party users:

- Are properly briefed on their information security roles and responsibilities prior to being granted access to covered information or information systems;
- Are provided with guidelines which state security expectations of their role within the organization;
- Are regularly notified of security changes and updates, as well as reminded of security responsibilities to be undertaken, via annual security awareness training and annual policy acknowledgements;
- Are motivated and comply with the security policies of the organization;
- Achieve a level of awareness on security relevant to their roles and responsibilities within the organization;
- Conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working.

All new hires are required to complete information security awareness training as part of their new employee onboarding process and annually thereafter. New hire onboarding will be completed within 90 business days after the date the employee or contractor is hired. Ongoing training will include security and privacy requirements as well as training in the correct use of information assets and facilities.

In addition, consistent with assigned roles and responsibilities, incident response and contingency training to personnel will be done annually.

The organization will properly document that the training has been provided to all employees. All employees are required to acknowledge in writing their understanding of the Information Security Program which includes a Code of Conduct upon hire and annually thereafter.

The organization will properly communicate to its workforce and, if appropriate, contractors:

- Security updates, changes, and incidents, as needed, via email or appropriate Slack channels.
- Reminders for security responsibilities as part of the annual security awareness training.

Core Services/Internet Access and Use

Use of Searchie Inc computers, Services, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

- Participating in any way in the creation or transmission of unsolicited "spam" that is unrelated to legitimate Company purposes;
- Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms;
- Accessing networks, servers, drives, folders, or files to which the employee has not been granted access or authorization from someone with the right to make such a grant;
- Making unauthorized copies of Company files or other Company data;
- Destroying, deleting, erasing, or concealing Company files or other Company data, or otherwise making such files or data unavailable or inaccessible to the Company or to other authorized users of Company systems;
- Misrepresenting oneself or the Company;
- Violating the laws and regulations of federal, state, city, province, or local jurisdictions in any way;
- Engaging in unlawful or malicious activities;
- Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the Company's networks or systems or those of any other individual or entity;
- Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;
- Sending, receiving, or accessing pornographic materials;
- Causing congestion, disruption, disablement, alteration, or impairment of Company networks or systems;
- Defeating or attempting to defeat security restrictions on company systems and applications.

Such access will be discontinued upon termination of employment, completion of contract, end of service of non-employee, or disciplinary action arising from violation of this policy. In the case of a change in job function and/or transfer, the original access code will be discontinued, and only reissued if necessary and a new request for access is approved.

All user IDs that have been inactive for thirty (30) days will be revoked. The privileges granted to users must be reevaluated by management annually. In response to feedback from management, systems administrators must promptly revoke all privileges no longer needed by users.

Remote Access Tools

All remote access tools used to communicate between Searchie Inc assets and other systems must comply with the following policy requirements where applicable:

- Multi-factor authentication (such as authentication tokens and smart cards that require an additional PIN or password) is required for all remote access tools.
- Remote access tools must support the Searchie Inc application layer proxy rather than direct connections through the perimeter firewall(s).
- Remote access tools must support strong, end-to-end encryption of the remote access communication channels as specified in the *Encryption Policy*.
- All antivirus, data loss prevention, and other security systems must not be disabled, interfered with, or circumvented in any way.

Information Security Requirements Analysis & Specifications

Searchie Inc will identify its information security requirements through utilizing different methods, ensure the results of the identification are documented and reviewed by all stakeholders, and will integrate the requirements and associated processes in early stages of projects.

Methods

- Policies and regulations
- Threat modeling
- Incident reviews
- Use of vulnerability thresholds

Factors

- Level of confidence required towards the claimed identity of users, in order to derive user authentication requirements.
- Access provisioning and authorization processes, for business and privileged or technical users.
- Informing users and operators of their duties and responsibilities.
- Protection needs of assets, especially in terms of availability, confidentiality, integrity.
- Business processes (e.g., transaction logging and monitoring, non-repudiation requirements).
- Other security controls (e.g. interfaces to logging and monitoring or data leakage detection systems).

Employment Terms and Conditions

The following terms and conditions of employment at Searchie Inc are the contractual obligations for employees or contractors for the safeguarding of information. May include, but are not limited to:

- Signing a confidentiality or non-disclosure agreement (NDA) prior to access to confidential information and processing facilities.
- Legal responsibilities and rights, particularly concerning intellectual property.
- Responsibilities for the classification of information and management of organizational assets associated with information, information processing facilities and information services handled by an employee or contractor.
- Responsibilities for handling of information received from third parties.
- Reviewing and agreeing with the security policies of the company.
- Duration of responsibilities beyond end of employment.
- Actions to be taken for non-compliance with the terms and conditions, and the company’s security policies.