# IS Policy

## *Information Security Policy*

*Information Systems*
Faithful+Gould
100 Canal Pointe Blvd
Suite 212
Princeton, NJ 08540
P. 609 514-0900
F. 609 514-9888

## Document Control

| Version | Date | Editor | Approved | Purpose |
|---|---|---|---|---|
| 1 | | Mark White | | Creation of policy |
| 2 | 7/25/2008 | Andy Wilhelm | Jim Nevada | Revision / update of policy |
| | | | | |
| | | | | |

# Table of Contents

## Definitions

| | |
|---|---|
| Company | Includes but is not limited to Faithful+Gould, Inc., W.S. Atkins, Inc., and Atkins Canada Consulting LLC. |
| Employee | All and any full and part-time salaried or hourly paid Employees, as well as any personnel employed by the Company on a contract basis |
| Director | Operations Directors, Senior Operations Directors, Vice Presidents, Senior Vice Presidents, and Management Board members |
| User | Any and all persons accessing Company networks and computers, including those accessing cellular and wireless networks provided, or with equipment provided, by F+G / Atkins |
| Network | Any point of access, including remote access, to Company networking infrastructure, and includes desktops, laptops, servers, printers, PDAs and other network-connected devices owned and/or operated by the Company |
| Domain | Any Company Windows NT, 2000, or 2003 domain, including the following named domains:<br>• WSATKINS<br>• ATKINSAMERICAS<br>• HANSCOMB – does this still exist?<br>• MSLENGINEERING – does this still exist? |
| Monitor / Monitoring | Include but are not limited to the act of, and the tools used for, the examination of stored Email, web sites visited, and information stored by electronic means, as deemed necessary by the Company and / or its Officers |

## Objective

The prime objective of the Information Security Policy is to promote business continuity and prevent damage to Company and Client information assets by minimizing the impact of security incidents, whether internal or external, deliberate or accidental.

To protect our corporate assets from being used for improper purposes and to safeguard the security of corporate information and the legal position of the Company, it is the expectation of the Company that all employees read and adhere to the Information Security Policy, agree to the spirit of this Policy, and behave securely and accurately when handling all Company information.

## Important Note

While this Policy is designed for, and written in the context of, electronic information generated or stored on computer assets, the concepts and spirit herein should be maintained when dealing with all Company information, as well as physical property owned or maintained by the Company. Physical information needs to be safe guarded as well. For example, confidential employee information in a secure database on a secure server is not protected when printed and left laying face up on a desk. Verbal information can also be confidential and a security risk. Speaking about trade secrets with a co-worker on a crowded elevator is one example.

## Scope

This policy covers the issue of Information Security in general, but specific attention should be paid to those sections relating to:

- E-Mail
- Telephone, Fax, and Voice Mail
- Internet

This Policy applies to users of Company-owned computers and systems as well as to those Employees using computers and systems owned by our Clients or joint venture partners, and any other computer when used for Company business, except where expressly stated. Where Client or joint venture partner policies exist, they should be added to this policy. Where clauses conflict, advice must be sought from the Information Services Director.

This policy should be read in conjunction with all other Information Services Policies and guidelines on a regular and repeated basis, all of which are available on the Portal. These include, but are not limited to:

- VOIP Policy (IS Policy)
- Cell Phone Policy (IS Policy)
- Air Card Policy (IS Policy)
- Email Policy (QSE Policy)

This document does not cover electronic data archiving policy.

## Responsibilities

In addition to the specific responsibilities provided for in this policy, the following personnel have these additional responsibilities.

### Information Services Director

To monitor adherence to the policy by commissioning appropriate and regular checks on all Information Systems, as well as modifying the policy to take account of technological and legal advances.

### Vice President of Human Resources

To provide all new Employees with an opportunity to read and accept the policy and acknowledge the same in writing. To provide guidance in any disciplinary matters relating to policy breach.

### Department of Information Services

To ensure all Employees are fully advised of the requirements of the policy and have the opportunity to seek clarification.

### Directors, Managers, and Supervisors

To enforce the requirements of the policy and to ensure that third parties undertaking work on behalf of the Company apply similar Information Security policies.

### All Users

All Users must ensure that they understand the requirements of this policy, adhere to those requirements and, in addition, report all breaches of the Information Security Policy to their Director in charge.

## Policy

All Users entrusted with any Company information, facilities, or equipment, including, but not limited to, computer, E-Mail, Network, Internet, telephone and Voice-Mail systems, cellular voice or data access, are prohibited from using any such Company assets for an improper purpose. This policy also applies to the use of Client provided facilities and equipment. Improper purpose includes but is not limited to:

- Any form of harassment or discrimination relating to gender, race, religion, national or regional origin, political persuasion or any other form of legally-protected harassment or discrimination against any Employee, Client or any other person.
- Pornography
- Indecent, obscene, libelous or malicious language.
- Unauthorized disclosure of Company or Client confidential information, or confidential information of any third party entrusted to the Company.
- Theft, or violation of any other law
- Attempting to influence the personal values or beliefs of others.
- Solicitation of any kind.
- Use of a Company computer to attempt to gain unauthorized access to any Company third party computer system.
- Knowingly performing any action that could interfere with or jeopardize the integrity and normal business operations of the Company.
- Any use of Company computers or other equipment which is not related to Company business or which is deemed, at the sole discretion of the Company, to be inappropriate and inconsistent with Company policies and corporate culture.

All employees are required to report any suspected breach of information security to the Department of Information Services. They are also expected to use and maintain the information for which they are responsible in a secure manner.

Any Employee who violates the Company's Information Security Policy is subject to disciplinary action, up to and including termination of employment.

Anyone found to be intentionally attempting to undermine or usurp the letter or spirit of this Policy, bypass either software or hardware security implemented anywhere on the Network, and / or otherwise fraudulently access information they do not have specific access to, for malicious intent or not, will be subject to Company discipline and / or Civil or Criminal litigation.

## Company Equipment

Any equipment or devices provided to any employee, including but not limited to computers, monitors, cellular phones, PDAs, Air Cards, are the property of the Company and will be maintained in asset registers and subject to regular audits.

- Computer equipment may not be removed from Company premises, unless specifically authorized by the Information Services Director and the appropriate Director or Vice President. If authorized, Users must adhere to the following:
    - All mobile devices, including removable storage media, must by locked away out of sight when not in use

  - Equipment and storage media should be hidden from external view when being transported in private vehicles
  - Equipment and storage media must not be left unattended in public places
  - Equipment should be carried as hand luggage and disguised where possible when traveling on public transport
  - Manufacturers' instructions for protecting equipment and media should be observed at all times, e.g. protection against exposure to strong electromagnetic fields, strong sunlight, extremes of temperature, etc.
- The Company reserves the right of immediate access to any Company equipment, including all information stored on any Company computer or phone system, upon reasonable suspicion that the User entrusted with such equipment is using it for an improper purpose or for any legitimate business purpose, subject to applicable laws.
- Permitting any non-Employee to use Company computer equipment is prohibited, unless specifically authorized by the Information Services Director and the appropriate Director or Vice President.

## Access Security

Login names and passwords are the main means of Company systems confirming the identity of, and therefore the information available to, users of Company systems. Both should be regarded as highly confidential and treated as such. As systems are monitored and / or audited for inappropriate use, the owner of a login name and password will be the individual identified when a problem is found.

- Passwords must not be disclosed to anyone. This includes any Employee including Managers, Directors or IS staff. Should Company representatives need access to your account in your absence your password will be replaced with a temporary password.
- Users are provided with approved login names for the purposes of accessing the Company network and other electronic resources. Under no circumstances should attempts be made to access the network with a login name other than that provided for the specific use of the person attempting such access.
- If any employee should obtain a login name and password, for any Company system, which is not their own, they are required to inform the Department of Information Services so the password may be appropriately changed and / or audited.
- Unattended systems must be shut down, logged out of the system, or locked.
- Upon login, anyone accessing the Network is presented with the notice of implied consent and acceptance. This notice reads as follows:

  "*This system is intended for business use within the Atkins Group of Companies. No individual right of privacy is intended and the Group reserves the right to monitor and control the use of the system. This system is private and access is restricted to those authorised by the Group's security system.*"
- Passwords required to access the Domain will be at least eight (8) characters long and should be a combination of numbers and letters.
- Passwords must not be associated with anything relating to you, your family, or anything else that may allow your password to be guessed.
- Passwords must not be written down.
- This policy in no way implies that your account is private. The Company reserves the right to monitor all electronic data in accordance with the provisions of this Information Security Policy and applicable laws.
- Providing any non-Employee with access information, e.g. User login names, passwords and modem telephone numbers, etc. is prohibited, except for said provision to approved subcontractors and consultants required to use Company resources and with

documented approval from the Information Services Director and the appropriate Director or Vice President.

- Non-Company computers must not be connected to the Company network. Exceptions to this will be equipment owned by approved business partners and home computers approved for business use, with documented approval from the Information Services Director and the appropriate Director or Vice President. Where Employees of Clients or contractors need to connect their equipment to the Company network their escort is required to contact the Department of Information Services prior to establishing a network connection. Such computers may only be approved for business use if they are up-to-date with the Company's chosen Anti-Virus and firewall software. The Company may also stipulate that a hardware firewall be installed. Company IS Employees must be given access to the computer for the purposes of verification and, where applicable, maintenance.
- Third parties must not be allowed access to Company networks other than through authorized 'firewalled' connections.
- Remote Network access must not be allowed other than through authorized, access controlled connection points.

## Email

Email is one of the most commonly used tools for business communication, and often passes over unsecured mediums such as the Internet. Users must be cautious both when sending emails and receiving emails, and ensure they know where they are going and where they are coming from.

- The Company reserves the right to conduct random reviews of Company owned computers, including E-Mail systems for the purpose of ensuring that equipment is being used for the intended business purposes and not for any improper purpose, subject to restrictions imposed by law.
- As Company records, E-Mail is subject to disclosure to law enforcement or government officials or to other third parties through subpoena or other processes. E-mail is considered written documentation, and thus becomes a part of Company records and is subject to public disclosure in litigation. Consequently, you should always ensure that the business information contained in these messages is accurate, appropriate, professional, and lawful.
- Consistent with the above, Users may not expect or assert a right of privacy in connection with any Company owned assets. Stored E-Mail messages are to be treated like paper files, with the expectation that anything in them is available for review by authorized Company representatives. Users should also be aware that deleted files remain retrievable for an indeterminable period of time.
- All E-Mail files are considered Company records and should be transmitted only to individuals with a business need to receive them. Those who have personal confidential matters to communicate should, to assure privacy, not use Company computers or systems.
- To provide adequate access for business use, personal E-Mail use should be restricted to less than ten (10) text-only messages per week. Personal messages shall conform to the guidelines for content described herein.
- Announcements that any Users wish to make over the Company E-Mail system that are not strictly related to Company business must be (a) of general interest to Company Employees AND (b) approved in advance by a Director.
- Consistent with the Anti-Virus Protection section herein, Users must not view or open any E-Mail message where the origin is questionable. In such circumstances the E-Mail message should be immediately deleted.

- Disclaimers must not be used in E-Mail signatures. The following signature will be automatically appended to all E-Mails going outside of the Company:
  *"This email and any attached files are confidential and copyright protected. If you are not the addressee, any dissemination of this communication is strictly prohibited. Unless otherwise expressly agreed in writing, nothing stated in this communication shall be legally binding."*
- Wherever possible, E-Mail attachments should be limited to 5mb in size. This may be achieved by 'zipping' the file in question. Should a need arise to send multiple files whose combined size is greater than 5mb, send multiple messages. If any doubt exists as to the size of any attachment, seek the advice of the Department of Information Services.
- As appropriate, Users shall ensure that E-Mails are stored offline, archived or deleted once read and addressed. Offline storage relates to the transfer of E-Mails to "PST" files.
- In addition to Company imposed storage limits, all E-Mail messages retained on the E-Mail server are subject to automatic deletion after a period of six (6) months from the date of sending or receiving. Prior to any deletion, a global communication will be issued giving full details of the process. This does not apply to messages stored in offline storage files.
- Project specific E-Mail print outs shall be treated as incoming mail and filed as appropriate with other project documents.
- In addition to the requirements of this policy, the following E-Mail practices are prohibited:
  - Sending jokes
  - Generation or forwarding of chain letters
  - Using disclaimer clauses within an E-Mail, unless approved by Company policy
  - Accessing other Employee's E-Mail files, except as specifically authorized by their supervisors in connection with their work for the Company.

PLEASE NOTE: Email is governed by the Company's Email Policy, listed at the beginning of this document, as well. Employees are required to read and adhere to the Email Policy in addition to this Policy.

## Phones, Faxes, and Voice Mail

Telephones, faxes and fax machine, and voice mail are commonly used to receive or disseminate business information, and Users need to be aware of and respect the confidentiality of that information.

- Users must ensure that telephone conversations, faxes, and voice-mails are appropriately safeguarded. Users should be particularly careful with confidential information, ensuring they do not speak too loudly, be aware of speakerphone use, and do not leave faxes in public areas.
- Phone calls, faxes, and Voice-Mails are considered Company records and should be shared only with individuals with a business need to receive them. Those who have personal confidential matters to communicate should, to assure privacy, not use Company equipment, including fax machines and telephone systems.
- As Company records phone calls, faxes, and Voice-Mail records are subject to disclosure to law enforcement or government officials or to other third parties through subpoena or other processes. They may also be considered written documentation, and thus become a part of Company records and are subject to public disclosure in litigation. Consequently, you should always ensure that the business information contained in these messages is accurate, appropriate, professional, and lawful.
- Consistent with the above, Users may not expect or assert a right of privacy in connection with any Company-owned assets. Stored voice mail messages and printed

faxes are to be treated like paper files, with the expectation that anything in them is available for review by authorized Company representatives. Users should also be aware that deleted files remain retrievable for an indeterminable period of time.
- The Company reserves the right to conduct random reviews of Company owned phones, fax machines, and voice-mail systems for the purpose of ensuring that equipment is being used for the intended business purposes and not for any improper purpose, subject to restrictions imposed by law.
- Project specific fax print outs shall be treated as incoming mail and filed as appropriate with other project documents.

## Internet

The Company will provide access to the Internet primarily for business purposes and as such access to non-business sites blocked by the company Internet filtering tool is prohibited, except where specifically approved by the Information Services Director and the appropriate Director or Vice President. Sites may be blocked or filtered for any number of reasons including, but not limited to: content, known virus generation, known ad generation. Sites are blocked to prevent possible loss or corruption of Company information as well to provide a safe and professional working environment.

- All Internet records and files are considered Company records and as such are subject to disclosure to law enforcement or government officials or to other third parties through subpoena or other processes.
- Consistent with the above and applicable laws, Employees may not expect or assert a right of privacy in connection with any Company provided Internet access.
- Wherever possible, the Company will employ an Internet filtering tool for the purposes of restricting access to certain sites. Making any attempt to bypass this tool is prohibited.
- Users or groups of Users will be given access to restricted entertainment or sports sites, approved by their business manager, only to satisfy specific business needs.
- All access to the Internet will be automatically recorded and log files reviewed periodically.
- Any license conditions related to the commercial use of software available on the Internet must be observed.
- Access security between the Company's internal network and the Internet is provided by a firewall. Bypassing this firewall is not permitted.
- Employees are reminded that the use of Company systems to receive, view or transmit content that may be considered offensive is expressly prohibited and may render the individuals involved subject to disciplinary action.
- Personal (non-Company) Internet-based E-Mail accounts must not be accessed from Company computers.
- Use of Instant Messaging software not provided by the Department of Information Services is prohibited.

## Monitoring

The purpose of monitoring is to ensure that the policies herein are being followed and to validate enforcement of necessary action for any breach of this policy. All monitoring is conducted in accordance with applicable state and federal laws.

## Data Protection

Neither the act of storing information in electronic format, nor the tools currently available to monitor and protect computer networks, can prevent loss or misuse of Company information in all situations. Users are required to practice caution and good judgment with regards to all forms of Company information and data.

- Sensitive or restricted data files on servers must be stored in appropriately protected folders. Care must be exercised to ensure such data files are not stored in folders accessible to Users not authorized to access such data.
- Sensitive or restricted data files should not be stored on a local workstation. In those cases where this is unavoidable, such files must be stored in appropriately protected folders. For computers running Windows NT/2000/XP operating systems, the default 'My Documents' folder and its sub-folders will suffice. For computers running all other operating systems, including Windows 95/98/ME, Macintosh or UNIX, guidance must be sought from the Department of Information Services.
- Should you be uncertain as to the security of your files you should immediately contact the Department of Information Services.
- Computer software programs may not be removed from the Company, or reproduced or duplicated, unless specifically authorized by the Information Services Director and the appropriate Director or Vice President.
- Entering information into a computer or database that is known to be false and / or unauthorized, or altering an existing database, document or computer disk with false and / or unauthorized information is prohibited.
- Accessing restricted data and files by non-authorized personnel is prohibited.
- Making any modification to Company computer equipment, systems files or software without specific authorization by the Information Services Director and the appropriate Director or Vice President is prohibited. Modification includes the installation of any software on any Company equipment.
- Users must regularly review, to the best of their ability, their personal file store for unrecognized files that may present a potential threat to system security. Users must immediately report the existence of such files to the Department of Information Services.
- Managers must ensure that Company records are stored and disposed of in accordance with relevant legal, contractual and operational requirements.

## Anti-Virus Protection

Viruses, Trojans, and worms are a significant source of risk to the confidentiality and integrity of Company information and data. Sources of malicious programs can be deceiving, and when there is doubt utmost caution should be used.

- Approved virus protection software must be installed and used on all computers and network servers.
- Where possible, anti-virus software will be periodically updated automatically. Interfering with this automated process is prohibited.
- No data or software must be exported from or input into the Company without validation by a Company-approved virus checker.
- Users must ensure that all virus incidents are reported to the IS Regional Services Representative.

## Software Installation

Software itself, even if seemingly innocent, can also be a source of malicious programs and / or corrupt local or network applications and data.

- Users must not knowingly attempt to download, load, or execute software on, or copy any software from or with, any Company computer without the authority of the Department of Information Services.
- Non-Company software may only be installed for business purposes. In such cases the original license documentation must be sent to the Department of Information Services.
- Under no circumstances should illegal software be loaded on to any Company computer. Should there be any doubt as to the legality of a particular product the Department of Information Services should be contacted.
- The copyright laws protect software and breaches of these laws not only hold the Company liable, but also hold liable any Director, Manager or other Officer of the Company who is deemed to have consented to such a breach. Copyright violations can result in both civil and criminal penalties and must be avoided.
- In order to ensure that unlicensed, illegal, or potentially dangerous software is not installed on Company equipment, audits of the software installed on Company assets will be performed regularly.

## Exclusions

Any requests for deviation from this policy as stated must be submitted to the Department of Information Services by a Director. Service Request personnel will assess the validity of the request prior to forwarding to the appropriate party in Information Services.