Information Technology (IT) End User Policy

Statement from Executive Management Team

Axiomatic has a long and proud tradition of conducting business in accordance with the highest ethical standards and in full compliance with all applicable laws. The Information Technology (IT) End User Policy was developed at the direction of Axiomatic Executive Management to provide clear guidance to all Axiomatic employees and to ensure a consistent approach to business practices throughout Axiomatic expanding operations.

Axiomatic Executive Management is fully committed to conduct business with the highest level of integrity and we expect your strict adherence to the Information Technology (IT) End User Policy and the law. There will be zero tolerance of non-compliance and any violations will result in swift corrective action, including possible termination of employment from Axiomatic Consultants.

Thank you for your commitment to comply unequivocally with the highest standards of integrity and business ethics.

Purpose for this Policy

To effectively manage and safeguard the use of all IT equipment, data, infrastructure and facilities by Axiomatic IT users and Representatives.

Statement of Responsibilities

The Company employees may access the Internet and/or email through the Company's network for the purpose of conducting Company business. Creating, viewing, copying, storing or sending content outside of the scope of the Company employment is prohibited. The Company provides Internet and e-mail access to all of the employees as a privilege that is based on adherence to the Company's policies and rules regarding Internet and/or e-mail access. In addition to being responsible to abide by the conditions as set out in, but not limited to this end-user policy, an employee who uses the Internet and/or e-mail shall:

- Ensure that no communication interfere with the employees productivity;
- Be responsible for the content of all text, data, audio, video or images that the employee creates, place on or send over the Internet and/or e-mail.
- Not transmit copyrighted materials without permission of the author thereof, and without defining and acknowledging the owner thereof.
- Avoid, where possible, transmission of information confidential to the Company or any of its clients/representatives. If it is absolutely necessary to transmit confidential information, employees are required to ensure that information is delivered to the proper intended recipient and any attached information should be password protected.

Internet and E-Mail Usage

Access to the internet is provided to employees for the benefit of the Company and its business.

Employees using the Internet, including e-mail, are representing the Company. Employees are responsible for ensuring that the Internet is used in an efficient, ethical and lawful manner. The following indicate examples of acceptable use:

- Accessing databases for information as needed for the Company's business.
- Utilizing the Internet, including e-mail, as a tool to advance the business objectives of the Company.

Employees and/or other Company Representatives may not use the Internet or e-mail for purposes that are illegal, unethical, harmful, or contrary to the Company's interests. The following examples indicate unacceptable use:

- Creating, viewing, accessing, intercepting, retaining, copying, processing or transmitting any content or material that is offensive, harassing, fraudulent, illegal or obscene including any pornography, hate mail, racist remarks or hoaxes to any company employee, client or any other individual or entity whether a Company Representative or not.
- Sending or receiving large non-business related e-mails – acceptable size is 5MB or less.

- Misrepresenting personal opinions as that of the Company via e-mail, or publication of unauthorized statements onto web sites, bulletin boards, forums, discussions areas.
- Using a third party e-mail provider, i.e. “Hotmail”, “Yahoo mail”, “Free mail”, “Gmail” or any other e-mail service provided by any outside Internet Service Provider or party, to send Company information or any files emanating from within the Company to external recipients. This INCLUDES any Company work or Data forwarded to personal e-mail addresses for working at home, unless explicitly approved by the Company.
- Providing computing or storage resources, including file sharing or swapping, to external parties through parties such as “Napster” and “Gnutella”, or any other torrent networks.
- Breaking through or even attempting to break through security controls, whether on the Company’s official equipment, personal Laptop or on any other computer system connected to the/a Company network;
- Intentionally or recklessly accessing or transmitting computer viruses and similar software;
- Forwarding internal e-mail distribution lists to outside agencies and organisations;
- Political lobbying of any kind;
- Downloading games, programs, shareware or freeware or data not intended for Company use.
- Any activities which could cause congestion and disruption of networks and systems;
- All e-mails are retained on a central server and will be backed up automatically subject to Company policy.
- Private email addresses must be used, outside business hours, outside the Company network, to register with online social networking services such as Facebook, MySpace, Bebo or Friendster, etc.

Senior Management, reserves the right to recommend the following remedies, in case of any breach of policy, involving use of the Company’s network/systems/data:

- Immediately and without notice withdraw and revoke temporarily/permanently the employee’s access to any/all computer systems and communication services, including e-mail, if it is found that an employee is using e-mail in breach of this document, subject to disciplinary action, in line with the Company’s disciplinary procedures as governed regarding Personnel, in addition to being required to pay any appropriate part of costs and/or damages incurred.

Senior Management may recommend the following response to violations of usage policies by any combination of:

- Informal warning;
- Disciplinary action, potentially for gross misconduct, through the normal disciplinary process;
- Provision of information to the police and law authorities, for possible criminal proceedings.

Copyrights and Downloads

Employees using the Internet are not permitted to illegally and/or wrongfully copy, transfer, rename, add, modify or delete protected works, information or programs. Employee are responsible for observing copyright and licensing agreements that may apply when downloading or distributing files, documents and software. Any copyrighted martial attached to a message should identify the author and acknowledge his/her copyright.

Monitoring and Privacy

All messages created, sent or retrieved over the Internet and e-mail are the property of the Company and may be regarded as public information and the Company reserves the right to intercept, retain, read and inspect the same if the Company believes, in its sole judgment, that it is justified to so in order to protect its business. Should any private information of the employee be contained in such message, the Company agrees to honor such privacy, it being recorded that any messages which may be personal by nature may be accessed and used by the Company where such message may cause harm to the Company and has the potential of causing harm and where the nature or content of the message is or is suspect to be contrary to this policy, or is otherwise unlawful.

All communications, including text, video or audio clips and images, can be disclosed to law enforcement authorities, or other third parties without prior consent of the sender or the receiver.

Computer Viruses

The following responsibilities to computer viruses prevention rest with each of the company's employees:

- Employees shall not knowingly introduce a computer virus into Company computers;
- Employees will not make use of any USB devices;
- Any employee who suspects that his/her workstation has been infected by a virus shall immediately power off the workstation and notify their Manager to take corrective action.

User Accounts and Passwords

The confidentiality and integrity of data stored on Company computers systems must be protected by access controls to ensure that only authorized employees have access. The access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

In addition employees shall access the Internet in a manner that does not compromise the Company's network security. This includes the employees keeping his/her username and password secure, prohibiting access to intruders or viruses, and reporting any suspicious activity to their Manager. Employees that want to download Internet content from a non-Company source must observe Company security procedures.

Password Policy

- If the security of a password is in doubt, the password must be changed immediately;

- Computing devices must not be left unattended without logging of the device or enabling a password protected screensaver.

Employee responsibilities

Each employee:

- Shall be responsible for all computer transactions that are made with his/her User ID (username) and password.
- Shall not disclose password to others. Passwords must be changed immediately if it is suspected that it may have become known to others.
- Should log out when leaving a workstation unmanned, or for an extended period.

Data Storage

The employee will exclusively store Axiomatic Consultants related information on his/her system as well as on network servers to ensure appropriate security protection and backup.

An Audit may be conducted at any time and without notice to ensure compliance with the agreement.

Software Copyright and License Agreements

All software acquired for or on behalf of the Company or developed by Company employees/representatives or contract personnel on behalf of the Company shall be deemed Company property. All such software must be used in compliance with applicable licenses, notices, contracts and agreements.

Non-compliance with legislation dealing with intellectual property, including copyrights, such as the Copyright Act and with license agreements can expose the Company and the responsible employee(s)/representatives to civil and/or criminal liability. Unless otherwise provided in the applicable license, notice, contract or agreement any duplication of copyrighted software, except for backup and archival purposes, may be violation of law.

This policy applies to all software that is owned by the Company, licensed to the Company, rented to the Company including SaaS (Software as a Service) or developed using the Company's resources by employees/representatives.

Home and Mobile Use

Employees should take care when traveling, especially in aircraft, buses and any other mass transport, that external parties cannot read information off computer screens or iPads and tablets. Employees should therefore exercise the necessary care when working on Company related information in public or non-Company areas.

In the event of an iPad, tablet, workstation or laptop being stolen, this should be reported immediately to your Manager, to arrange for all security access to be suspended.