

FSA Code of Conduct: Corporate Policy on the Use of Information Resources

This Statement of Policy sets forth the guidelines of Financial Security Assurance Holdings Ltd., including Financial Security Assurance Inc. and its other direct and indirect subsidiaries (collectively referred to as “FSA”), for the use of information resources provided to FSA employees, including access to the FSA computer systems, e-mail, and the Internet.

For guidance on the permissible use and dissemination of information, including confidential information, about FSA, its customers and its employees, see the **Code of Conduct, Corporate Policy on Insider Trading and Tipping, Corporate Policy on Fair Disclosure** and **Corporate Policy on Personal Information**.

Policy

Every FSA employee is responsible for safeguarding FSA’s business information resources, by protecting them from misuse or improper modification, ensuring that they remain accessible to their proper users, and generally following FSA’s guidelines for their use.

Employee Use of Information Resources

Information is an important business asset. Because FSA relies on the accuracy of its information in the daily conduct of its business, all FSA employees must ensure that its information resources are reliable and protected from accidental or malicious changes. This Statement of Policy establishes a framework for the use of FSA’s information resources. Although much of this guidance refers to networks and computer systems, the basic principles of information protection apply to all kinds of information, including verbal and written communications.

FSA provides its employees with computer and communications resources for use in accomplishing FSA’s business objectives. FSA permits employees to make limited personal use of e-mail accounts, the Internet and local or toll-free telephone calls for brief personal communications, but it may curtail those privileges at any time if abused.

Any employee who violates FSA’s information resource policies or the guidelines set forth below may be subject to disciplinary measures. International employees should also review the Handbook for International Staff, including Section 1, paragraph 10, “Data Consent” and Section 2, paragraph 16, “Electronic Communications Policy.”

Employee Use of Information Resources is Monitored

All employee use of FSA computers and communications resources, including e-mail, the Internet and, in some areas, phone lines, is logged and may be monitored. All e-mail messages sent or received using FSA network resources and all recorded phone calls are and will remain the property of FSA and may be monitored or disclosed by officers of FSA

to third parties without employee permission. Records from logs and monitoring systems established by MIS may be examined for evidence of employee misconduct.

In order to minimize the risks of unauthorized disclosure of sensitive FSA information, as well as the risks of deliberate attacks through Internet connections, MIS may use technical means to restrict what locations and services FSA network users are able to access through Internet connections. Employees must not attempt to circumvent these access controls. If an employee has a valid business need to access something blocked, he or she may submit a request to MIS for special access. If necessary, group manager approval may be required.

FSA uses software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet. Such filters cover broad categories, including pornographic sites, chat rooms, and other areas. An additional filter blocks access to broad categories of Web sites and protects against sites that may have malicious code. If an employee has a valid business need to access something blocked, he or she may send an e-mail message to MIS to explain the need and request access to the site. If necessary, group manager approval may be required.

Information System User Guidelines

Employees utilizing FSA's business information resources are subject to the following guidelines.

1. Employees may not:
 - access or transmit obscene or harassing materials, including, but not limited to, those evidencing discrimination based on race, national origin, gender, sexual orientation, age, disability, religion or political beliefs;
 - transmit messages of a harassing or threatening nature, including, but not limited to, defamatory, fraudulent, intimidating, abrasive or offensive statements; or
 - access or transmit materials of a pornographic or sexually explicit nature.
2. Employees must not abuse the privilege to use FSA computers and communications resources for limited personal needs, and in particular must not permit their personal use to interfere with their productivity or the availability of FSA's resources for their or others' business needs.
3. Access to computer resources within FSA facilities is controlled to prevent unauthorized access. Before leaving for the day, employees must sign off or lock their computer. An employee must not share his or her user ID and password with anyone else or write them where someone might find them, as the employee will be responsible for anything done by someone else using the passwords.
4. Employees are responsible for the proper protection of all FSA and non-public personal information copied or downloaded to their computer.

5. Employees must not try to access any FSA computer or network resource without permission or attempt any unauthorized probe or test of network security controls.
6. Employees should be wary of any e-mail from unknown senders, as well as of messages with unusual subject lines, as they may contain malicious software. Employees must not:
 - open attachments received with suspicious email messages; or
 - disable the automatic scanning protection settings of the anti-virus software.

Any employee who suspects that his or her workstation has been infected by a computer virus or notices unexplained changes in the behavior of other FSA systems that he or she connects to, should report it immediately to MIS.

7. MIS installs computer equipment with standard software packages for business use. Employees should not attempt to load or otherwise access additional software on their own. If an employee needs special software installed, his or her group manager should send an e-mail message to MIS to explain the need and request installation of the software.
8. Employees must not conduct any actions intended to damage or disrupt computer systems or networks or otherwise misuse FSA computers, including by:
 - relocating workstations or attaching modems or wireless networking adapters without authorization and assistance from MIS;
 - requesting a User ID under false pretenses, attempting to log on as another user, using tools to decode passwords, intentionally misrepresenting the identity of a message sender, hiding the identity of a sender, or altering another sender's message;
 - attempting to disable or by-pass the logging or monitoring of resource use;
 - distributing chain letters or unsolicited advertising;
 - intentionally propagating computer worms or viruses;
 - conducting Internet file-sharing; or
 - knowingly infringing copyright or other intellectual property rights.
9. Authorization from MIS is needed in order to move FSA-owned computer equipment from FSA's facilities.

The Information Security Program

To ensure the integrity, availability, and confidentiality of its information assets, FSA has instituted a company-wide **Information Security Program**. Responsibility for the program lies with company executive management and with each and every FSA employee. The **Information**

Security Officer, under the direction of the CFO and in consultation with business unit managers, holds primary responsibility for assessing information security risks and for the elaboration and implementation of information security and access control policies for computers and networked information systems.

The Management Information Systems Department (“**MIS**”) is responsible for the implementation of appropriate technical controls to protect FSA's automated information resources on its computer systems and networks. MIS develops implementation procedures and standards, enforcement mechanisms, and user guidance for FSA electronic information systems and networks. In its implementation and enforcement of electronic information policies, MIS deploys technology to control the use of FSA information and communications systems, and to log or monitor the use of FSA computers, networks or other electronic systems by employees, contractors, or remote users.

By default, any member of a work group within FSA is granted access to the same set of information resources and programs as all members of that group. Work group managers who need to have exceptions made for one or another employee must communicate that requirement to MIS. Business unit managers should establish criteria for determining who is granted access to the group's information resources. They may not, however, implement any computer or networking technology without MIS involvement.