Institute of Jamaica

Information Technology Policies & Procedures

Revised: February 22, 2010

1. Requirement for Good Judgment and Reasonable Care

1.1 *Precaution against contaminant:*

1.1.1 Users must take the necessary precautions to avoid introducing computers to harmful contaminants, for example, viruses, Trojan horses, and other malware onto IOJ's computer hardware, software and other I.T. devices. Precautionary measures include but are not limited to the practice of:

1.1.1.1 Installation of up-to-date anti-virus software on all laptops and desktop computers;

1.1.1.2 Extreme care when opening e-mail attachments (especially documents with uncommon file extensions) or unauthorized downloading of software (especially trial or beta versions);

1.1.1.3 Scheduling of periodical run of virus scans on computers;

1.1.1.4 Doing an anti-virus scan on thumb drives / flash disk/ other external storage media before connecting to computers / laptops;

1.1.1.5 The setup of automated services by the I.T. Unit to monitor the computers on the network, and setup safe guards to discourage users from disabling these services.

1.2 *Protection against theft and damage:*

1.2.1 Users must take the necessary and reasonable precautions to protect I.T. equipments or systems assigned to them and or their division/department, and will be held liable for I.T. equipment/systems that have been damaged, lost due to theft, destroyed and / malfunctioned due to unsupervised alterations of any kind, including but not limited to:

1.2.1.1 The removal of installed software or machine configurations;

1.2.1.2 The removal of power supplies and / UPS from designated equipment, which are used to prevent / protect against damage resulting from electrical surges;

1.2.1.3 The installation or addition of malicious or unapproved software, hardware, macros or files that interfere with the equipment's productivity or operations.

1.2.1.4 Unauthorized removal of all I.T. equipment from IOJ premises is strictly prohibited and will be regarded as theft and dealt as a criminal offense.

1.2.2 I.T. equipment that has been lost or irrecoverably damaged due to user's negligence must be restored to IOJ. IOJ must receive the same make/model/type of equipment that was lost, stolen or damaged. If the same make/model/type is not

possible, the cost of the equipment as stated by the Accounts department must be paid.

1.3 *Prevention against physical loss of I.T. Equipments:*

1.3.1 In collaboration with the Asset Dept, all I.T. fixed asset (newly acquired and already existing) must be entered into the Asset Database.

1.3.2 Permanent movement of all I.T. fixed asset must be tracked in the Asset Database.

1.3.3 Laptops assigned to staff, must remain within the division / department if that staff member goes on any type of leave – vacation, study, maternal etc., and the I.T. unit notified of the start and end date of the leave period. The I.T. unit will do random spot check to verify the equipment is on the premises and in the correct location.

1.3.4 Authorization from Head of Division (HOD) and I.T. Manager must be given before temporary movement of IOJ's I.T. fixed assets takes place. An entry in the I.T. log (located in the respective division / department) must be done to track temporary movement, indicating the equipment to be moved, the person requesting the move, date of request, date of movement, I.T. staff assigned to move equipment (if applicable), date of return and department where the equipment was moved to and from.

1.3.5 HOD must identify personnel responsible for log and communicate this to the I.T. manager.

1.4 *Prevention against data loss:*

1.4.1 It is the responsibility of the department to request in writing a full backup of critical data on their computers' local drives onto CD / DVD (or other storage devices), or setup a backup schedule with I.T. to do incremental backup of files on local hard drives on to other storage devices.

1.4.2 In the event that IOJ acquires a file server, data deemed mission critical to the division / department / section should be backed up on the server in the folder(s) assigned. Personal data should not be stored on IOJ's servers.

1.4.3 Automatic backup of certain databases are done daily and stored on the existing application server. A full backup of the application server is done on a weekly basis and sent to an off-site location.

1.5 *Protection against excessive degradation of operation:*

1.5.1 It is the responsibility of the users to periodically remove unnecessary or unused files from their computers to prevent using up disk space and negatively affecting the operation of the computer.

1.5.2 I.T. department will be responsible for routine computer maintenance. Maintenance of any I.T. equipment outside the scope of the I.T. department will be deferred to an outside contractor pending availability of funds.

2. Prohibition against Unauthorized Access or Release of Private Information

2.1 *Unauthorized Access:*

2.1.1 The unauthorized access and usage of any I.T. equipment is strictly prohibited.

2.1.2 The data stored on individual's computer (laptops, desktops etc.) or user accounts is deemed confidential, and issues such as exemption stated in section 21(1)a-d of the Access to Information Act(ATI), privacy, stated in section 22(1) of the ATI, and intellectual property rights must be protected.

2.1.3 To access and / alter email messages or files stored on another user's computer or storage device including USB / flash drives, without permission, even if data is not password protected, is prohibited. This does not include network administrators and / I.T. personnel who will need access to carry out their assigned duties.

2.1.4 It is the responsibility of the user to safe guard the password to their computer, databases and / files.

2.2 *Release of Private Information:*

According to the Access to Information ACT (ATI) section 22(1) –

"...a public authority shall not grant access to an official document if it would involve the unreasonable disclosure of information relating to the personal affairs of any person, whether living or dead."

It is prohibited to disclose any data that would be a breach of confidence or copyright as stated in section 33(1)b of the ATI, whether via e-mail, website, in print form or via unauthorized access to stored files on computers.

3. Prohibited Use

3.1 Obscene , sexual explicit or pornographic subject matter:

It is strictly prohibited to use IOJ owned or leased I.T. equipment to download, view, access, store, print, replicate or broadcast any material deemed obscene, immoral or unlawful by Jamaican law or policies of the Institute of Jamaica. Exemption maybe given in the case of cultural research, collection or for educational activities by authorized personnel.

3.2 Unauthorized Software Downloads:

The list of prohibited software is endless and ever growing. Nevertheless, a few are identified on IOJ's Intranet at http://ioj.com/Documents/IT%20Policy.pdf. Any of the software listed, if already installed on IOJ computers shall be removed by an I.T. staff upon discovery. Any other software deemed harmful or counter-productive by the Head of Division and / the I.T. Department will also be removed by an I.T. staff upon discovery.

4. Compliance with Laws and Policies

4.1 Software Licensing:

4.1.1. The use of unlicensed software on any of IOJ's computers is strictly prohibited. Persons are strongly discouraged to install/download any software prior I.T.'s knowledge and / approval.

4.1.2. I.T. shall perform random audit of software on IOJ's computer systems. Unauthorized software shall be removed and a report submitted to the HOD.

4.2 Intellectual Property/ Copyright:

[1]Work created using IOJ's computers, network and / equipment, during the course of duty are the property of IOJ, see staff manual under "copyright".

[1] http://www.jipo.gov.jm/pages/copyright.htm

5. Communication via email, website and the Internet

5.1 Email:

5.1.1. This medium of communication is being used with such frequency and is engrained in IOJ's business processes that regardless of the intent, status or location of an email, once IOJ's computers and / network are used to create and send it, that email is the property of IOJ and no different from any other document. [2]Therefore, individuals have no personal privacy rights in materials created or communicated on IOJ's computer systems.

5.1.2. [3]Email is not just a medium by which we communicate with our internal and external customers, but is considered a legal document of record and can be used as evidence in the court of law.

5.1.3. Emails sent from IOJ computers are considered to be done on behalf of IOJ and as such indecent/obscene/sexual/pornographic language and / content is strictly prohibited. Additionally, emails used to promote or solicit non-IOJ business and do not benefit IOJ in any way; include content of a harassing nature and / content deemed unproductive are prohibited.

5.1.4. It is the responsibility of each IOJ employee to use with care and proper decorum email as a communication tool, and be aware that they are representatives of IOJ and that emails sent from any IOJ computer is the property of IOJ, is a legal document of record and is a reflection of IOJ and the individual.

5.2 Website:

5.2.1. The use of IOJ's computers and / network to browse, access, download, upload, and or otherwise disseminate pornographic, sexual explicit, distasteful, unproductive material – audio, video, pictorial and / text, outside of authorized research is strictly prohibited. If content, URL and any other tags are found on any of IOJ's I.T. or audio-visual equipment, the information will be deleted upon

[2] http://estorian.dciginc.com/2009/04/emailnot-just-communication-bu.html

[3] http://www.deltabravo.net/custody/email.php

discovery and person(s) assign, if not authorized, shall be reported for disciplinary actions.

5.2.2. Excessive Internet surfing of non-work material using IOJ's computers and / network, especially during work hours is strictly prohibited and person(s) shall be reported for disciplinary actions.

6. Password and User Network Account Policy:

6.1 Change password:

Automatic alerts will be set to prompt users to change their passwords every 3-4 months. Changing password frequently is a security measure to discourage unauthorized access of person's computers.

6.2 Delete / suspend user's network and / email accounts:

6.2.1. HR to send a list to I.T. Manager including all persons who are no longer working for IOJ per month, so that their email and user accounts can be locked and / deleted within 7 – 10 working days of receipt of list.

6.2.2. HR to send a list of persons whose contracts will expire within the next 1 – 2 months, so that I.T. may suspend their user and email accounts until their contracts are renewed.