Protect - Promote - Defend

Lesbians, Gays, and Bisexulas of Botswana
Email admin@legabibo.org
Tel (+267) 316 7425 **Fax** (+267) 316 7465
P.O. Box 5500430 Mogoditshane, Botswana

INFORMATION AND TECHNOLOGY GUIDELINES

1. Introduction

The data stored in manual and electronic systems used by LEGABIBO represent an extremely valuable asset. LEGABIBO relies on information technology to deliver services therefore it is necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion, in addition to paper based records.

1.1. Purpose of the policy/ Intent

This document sets out the LEGABIBO's IT policy for the protection of its information and technology systems and defining baseline responsibilities for security, equipment and file storage. LEGABIBO's IT systems refer to the IT network, hardware including portable media, system and application software, communication components include telephone and WAN systems, documentation, physical environment and other information assets. The policy aims to protect LEGABIBO's information and assets from all threats, whether internal or external, deliberate or accidental.

The equipment covered by this policy includes;

- Network infrastructure- the equipment housed internally to provide the LEGABIBO IT network, including servers, enclosures, racks, cabling, switches/hubs, Routers, wireless access points, firewalls, proxies, authentication systems etc.
- Desktops- Personal Computers (PCs) issued or provided to staff in the course of carrying out their duties
- Laptops- Portable Personal Computers issued or provided to staff in the course of carrying out their duties
- Mobile Phones- Digital communication devices issued or provided to staff in the course of carrying out their duties
- Phones – Telephones/Voice Communication devices connected to the Network Infrastructure including desk telephones, conference telephones etc.
- Electronic Storage Devices such as DVDs, CDs, memory sticks and hard drives issued or provided to staff in the course of carrying out their duties
- External Communications Infrastructure – Equipment used to connect LEGABIBO to the external world including the Wide Area Network, telephone lines, Ethernet, ADSL circuits and all related equipment and services.

To the extent these policies are effectively implemented and upheld, they will provide assurance that Donor and LEGABIBO information, both programmatic and financial, is protected.

As a result, all staff must exercise the necessary discipline to ensure that approved policies and procedures are implemented.

Protect - Promote - Defend

Lesbians, Gays, and Bisexulas of Botswana
Email admin@legabibo.org
Tel (+267) 316 7425 **Fax** (+267) 316 7465
P.O. Box 5500430 Mogoditshane, Botswana

2. General Policy Guidelines

2.1. Data kept on all company computers, which include desktops, servers, organizational laptops and private laptops used for organization business, is confidential and must not be shared with persons or organizations outside LEGABIBO unless approval has been granted by someone in position of authority.

2.2. No unauthorized software may be installed on any computer. All software must be installed by an authorized personnel as approved by management.

2.3. Hard copy records of all critical system settings (passwords, internet user-names, email log on details, network settings etc.) must be made and retained in secure keeping.

2.4. Internet use of a personal nature must be kept to a minimum. This includes personal email and 'web browsing'.

2.5. Application software (such as Microsoft Office) installed on all computers is the sole property of LEGABIBO and must not be copied for personal use.

2.6. A back-up regime for all computer data must be adopted and performed on a regular basis. Employees are responsible for the data they work on.

2.7. All electronic equipment must be signed off in the Assets Register at the Finance and Administration Office.

3. Usage

LEGABIBO IT equipment is used for purposes relevant to organizational mandate. The following acceptable usage are allowable:

- Research
- Administration and management of LEGABIBO business
- Communication

4. Internet

Use of the Internet is permitted where such use supports the goals and objectives of LEGABIBO. Internet passwords and other security log-ins are stored in a secure location and controlled by authorized personnel only.

5. Unacceptable Behaviour

- visiting internet sites that contain obscene, hateful, pornographic or other illegal material
- using the computer to perpetrate any form of fraud, or software, film or music piracy
- using the Internet to send offensive or harassing material to other users
- Creating or transmitting defamatory material

Lesbians, Gays, and Bisexulas of Botswana
Email admin@legabibo.org
Tel (+267) 316 7425 **Fax** (+267) 316 7465
P.O. Box 5500430 Mogoditshane, Botswana

- introducing any form of computer virus into the network Users shall ensure that fax communications are protected at all times and that faxes containing personal or sensitive information are sent, and received in a secure manner.

6. Verbal Communications

Employees are reminded of their obligation to respect the privacy of fellow employees and visitors. This means holding conversations discreetly and with due regard to the sensitivity of the subject under discussion.

7. Fax Security USB Data Sticks or Pen/Flash Drives or External Hard Drive units.

The use of any privately owned equipment or media within LEGABIBO computer system is prohibited.

Confidentiality must always be maintained , this includes information about our donors and staff. Ethical duties of confidence must be observed and extreme caution should be exercised. USB data devices should only be used on an exceptional basis where it is essential to store or temporarily transfer data, in accordance with the Computer Use Policy.
Only LEGABIBO owned or approved USB data devices can be used with LEGABIBO computer equipment.

Any loss of a LEGABIBO owned USB device potentially constitutes a serious breach of security and should immediately be reported to management and recorded as an incident.

Data should always be removed from the USB media when no longer required.