LIMPOPO GAMBLING BOARD
INFORMATION TECHNOLOGY UNIT

ICT Information Security Policy

Prepared by:	Recommended by:	Approved by:
Yvonne Mathabatha Chief Financial Officer	Serobi Maja Chief Executive Officer	Mashile Mokono Chairperson of the Board

Version	April 2016	
Effective date		

TABLE OF CONTENTS

1. ACRONYMS

CEO: Chief Executive Officer

ICT: Information and Communication Technology

IT: Information Technology

LGB: Limpopo Gambling Board

PC: Personal Computer

SMS: Senior Management Services

WSUS: Windows Server Update Services

2. INTRODUCTION

This document provides guidelines for the effective management of ICT in the Limpopo Gambling Board (LGB).

Information and Communication Technology (ICT) is a key enabler (tool) in enhancing organisational efficiency in any work environment. Like any other tool, it is necessary to manage and maintain it effectively so that we are able to derive maximum value from it. As the Information Technology (IT) unit, we are tasked with the responsibility of ensuring that the LGB ICT environment is in sync with the needs of users, while at the same time ensuring that all our IT assets are well maintained and pro-actively managed.

LGB as an employer is committed to enhancing the efficiency- capacity of its employees by providing qualifying members of staff with the necessary ICT equipment for the performance of their duties. Such equipment is provided on requisition through the normal procurement process and is furthermore subject to procedures as defined by the Supply Chain Management (SCM) Framework.

Information and Communication Technology (ICT) in any organisation has the potential to unlock immense value within the organisation and has the ability to positively empower employees to fulfil both their work related and individual goals. Access to ICT, however, carries with it responsibility for both the provider and the user in terms of how it is made available, used and managed.

To this extent, LGB will endeavour to subscribe to the broad principles of Corporate Governance of Information and Communications Technology (CGICT) as contained in the LGB CGICT Policy Framework that was instituted by the Limpopo Gambling Board of Public Service and Administration (DPSA) in November 2012; and subsequently adopted by the Limpopo Provincial Administration in 2013.

The policies contained within this package have been developed for the purpose of ensuring that the application of ICT within the Limpopo Gambling Board (LGB) is managed in a way that protects the privacy, confidentiality and integrity of information, while at the same time maintaining the physical ICT assets of the Limpopo Gambling Board in good working order.

3. PURPOSE AND OBJECTIVES

3.1 Purpose

To establish the basic policy for the Limpopo Gambling Board that will guide the use, procedures, principles, norms, standards, rules and regulations for the protection, and preservation of all ICT equipment and information in any form, which is generated by, owned by or otherwise in possession of the Limpopo Gambling Board.

3.2 Objectives

- To protect Limpopo Gambling Board's business information and any public information in its custody by safeguarding the confidentiality, integrity, authenticity and availability.
- To develop principles to protect the Limpopo Gambling Board's information resources from theft, abuse, misuse, distortion and any form of illegal damage.
- To enforce responsibility and accountability for information security in the Limpopo Gambling Board.
- To encourage management and staff to maintain an appropriate level of awareness, knowledge and skills to allow them to minimize information risk.
- To ensure Limpopo Gambling Board continuity with its activities resulting from unforeseen events.
- To voluntarily comply with minimum security information requirements as set out in National and Provincial ICT and Information Policy Frameworks

4. AUTHORITY OF THE POLICY

The policy is issued under the authority of the CEO of LGB.

5. LEGAL FRAMEWORK

This policy has been developed within the following applicable legal frameworks:

a. The Constitution of the Republic of South Africa Act, 1996 (Act no. 108 of 1996).

b. White Paper on the Transformation of the Public Service 1997.

c. Electronic Communication and Transactions Act, 2002 (Act No. 3 25 of 2002).

d. Minimum Information Security Standards.

e. Limpopo Provincial E-Government Strategy.

f. Public Service Act, 1994 (Act no. 103 of 1994) as amended.

g. Public Service Regulations, 2001.

h. Public Finance Management Act, 1999 (Act no. 1 of 1999) as amended.

i. Treasury Regulations,2001

j. Protection of Information Act, 1982 (Act no. 84 of 1982).

k. National Information Security Regulations.

l. SITA amendment Act, 2002 (Act no. 38 of 2002).

m. Electronic Communications Security Act, 2002 (Act no. 68 2002).

n. Public Service IT Policy framework of February 2001.

o. Minimum Interoperability Standards (MIOS) for Information Systems in Government

p. South African Government-Wide Enterprise Architecture Framework (GWEA).

q. Control Objectives for Information and Related Technology (COBIT).

r. International Standards Organization (ISO 9000).

s. Information Technology Infrastructure Library (ITIL).

t. South African National Standards, 85300.

u. King III Report.

v. Corporate Governance of ICT (CGICT).

6. SCOPE OF APPLICATION

This Policy set applies to all permanent employees of the Limpopo Gambling Board (LGB) as well as part-time employees, interns, volunteers, contractors, service providers, and any other individual/s conducting business with or using LGB ICT infrastructure.

7. DEFINITIONS

a. **"Exchange server"** is a collaborative enterprise server application that offers electronic mailing, contacts and tasks, calendaring, web-based and mobile information access;

b. **"Proxy server"** is a computer system or an application that acts as an intermediary for requests from clients seeking resources from other servers, e.g. internet;

c. **"Map production"** is a process of arranging map elements on a sheet of paper for interpretation; and

d. **"Meta data"** means Information about the information product such as who captured the data, the manner in which it was collected, date collected etc.

8. POLICY PRONOUNCEMENTS

This policy is available for access through the LGB Intranet and all users who have access to the LGB domain are required to confirm that they have read and understood the provisions of this policy prior to logging-on to the system.

As such, all permanent employees, part-time employees, interns, volunteers, contractors, service providers and any other individual/s conducting business with or using LGB ICT infrastructure utilising LGB ICT infrastructure are personally responsible for understanding and following the terms of the policies contained herein, and shall be held personally accountable for the consequences arising from

any security violation resulting from a failure to observe such policies. The Limpopo Gambling Board shall identify and provide appropriate information security awareness tools and awareness sessions to support this process.

User Awareness

Personnel are encouraged to familiarize themselves with the policies contained herein. Improved awareness of Information Security issues and procedures does not only reduce the risk of information accidents, but also increases the likelihood of suspicious activities being reported and preventative measures being implemented.

8.1. ICT ACCEPTABLE USAGE POLICY

8.1.1. Purpose

The ICT Acceptable Usage Policy sets out the basic responsibilities of users and system providers with regard to system access and password management issues. **This Policy should be read in conjunction with all other LGB ICT Policies.**

8.1.2. System access

The selection of passwords, their use and management as a primary means to control access to systems is to be strictly adhered to according to best practice guidelines. Users are responsible for all activities done in or from their assigned account.

8.1.3. Lock-out mechanisms

Software lockout mechanisms in case of failed attempted log inns shall be established and enforced.

8.1.4. Passwords

Passwords should be of such a combination that it includes a combination of alphanumeric (upper and lower case) and special characters and should consist of minimum of six characters length. Passwords must be kept strictly confidential and must be changed whenever there is any indication of possible system or password compromise. Passwords should be changed every 30 days. Temporary passwords must be changed at first logon.

8.1.5. Clear screen policy

All users of workstations, PCs or laptops are to ensure that all applications are closed when equipment is left unattended alternatively our system logs out the user after five minutes the equipment is left unattended; and systems should be shut-down after hours.

8.1.6. Software updates

All users must ensure that all workstations/notebooks are logged-on to the LGB domain to ensure that all necessary software updates are completed.

8.2. ICT BACKUP POLICY

8.2.1. Purpose

The ICT Backup policy sets out the basic responsibilities of users and system providers with regard to data storage and backup procedures. This Policy should be read in conjunction with all other LGB ICT Policies.

8.2.2. Workstations (All users)

8.2.2.1 Individual computers (Desktop and Notebook Computers)

Important files and data on individual computers must[1] be backed up to the shared directory on the LGB File Server. Each user is assigned storage space on the LGB File Server. This space is assigned only to the designated user and cannot be accessed by any other user. It is the responsibility of the user to ensure that this storage space is managed and regularly maintained.

8.2.2.2 Retention periods and disposal of data

Users are responsible for ensuring that the archiving of electronic data files is archived in accordance with legal and regulatory requirements as stipulated in the LGB Financial Regulation, Accounting Policies & Delegation of Authority Section 15 file plans, process manual, Paia, 2000, SDI Act, and ECT Act.

8.2.3. Servers (System Administrators)

8.2.3.1. File servers

The following files categories must be backed up daily and monthly on an incremental basis:

- Data stored on home (shared) directory.
- System State backup

8.2.3.2. Application server

The following files categories must be backed up daily, weekly and monthly on incremental basis:

- System State backup
- Database backup

8.2.3.3. Exchange server

The following files categories must be backed up daily, weekly and monthly on incremental basis:

- System State backup
- Exchange configuration
- User mail boxes

8.2.3.5. Software update services

The following updates must be implemented when they are released:

- Windows Software Update Services
- Symantec and Sophos Live Updates

8.2.3.6. Backup monitoring

- Backup logs must be monitored monthly.

8.2.3.7. Restore procedure testing

- Restore testing procedures must be conducted annually.

8.2.3.8. Managing On-Site and Off-Site data stores

- Data storage media is filed off-site on a monthly basis.
- Off-site and On-site locations where data is stored must provide access controls and protection which reduce the risk of loss or damage.
- Own Cloud mechanism will be used as another form of back up.

8.3. ICT EMAIL POLICY

8.3.1. Purpose

The ICT e-mail policy sets out the basic responsibilities of users and system providers with regard to sending, receiving and management of electronic mail. Emails are now the primary means of business communication.

However, email also presents a significant risk if it is not used responsibly. Users must be cautioned against accepting and opening unsolicited emails from sources unknown to them. These emails often contain code that is used to gain access to personal information of the user and may be used to commit fraud and other illegal activities. **This Policy should be read in conjunction with all other LGB ICT Policies.**

8.3.2. Electronic mail (E-mail)

LGB e-mail should **ONLY** be used for official purposes, using terms and branding which are consistent with other forms of LGB communication.

Users must refrain from using the "reply to all" response to avoid congestion on the network. Distribution lists should be created to direct emails to relevant recipients.

Users must refrain from sending mass mailings ("send to all"). All such mailings must be channelled through Communications Services for consideration and distribution.

8.3.3. Legal issues around emails

Users are requested to take note that email communications are considered to be legally binding and should therefore be treated as such. Limpopo Gambling Board emails carry a legal-disclaimer and users are cautioned that they may be held individually liable in cases where email is used to misrepresent the Limpopo Gambling Board.

8.3.4. Receiving electronic mail (E-mail)

Incoming e-mail must be treated with the utmost care due to its inherent information security risks. E-mail from an unknown source should be deleted. The opening of file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code.

8.3.5. Retaining or Deleting Electronic Mail

Data retention periods for e-mail should meet legal and business requirements and must be adhered to by all staff.

8.3.6. Receiving Misdirected Information by E-mail

Unsolicited or 'spam' e-mail is to be treated with caution and deleted immediately.

8.3.7. Forwarding E-mail

Ensure that information you are forwarding by e-mail (especially attachments) is correctly addressed and only being sent to appropriate persons. Any security risk (virus, content) associated with the original mail to you will also apply to the forwarded e-mail.

8.3.8. Filtering E-mail content

The organisation will use software filters and other techniques whenever possible to restrict receiving or sending of inappropriate information using email.

8.3.9. Email misuse

Mass mailings are strictly prohibited. Notices of acting delegations, events, bereavements, etc. should be forwarded to Chief Executive Officer for upload onto the LGB intranet.

No private marketing or selling for personal or private gain or for gain of a private company shall be undertaken using the email facility.

Every official shall take extreme care not to be duped into the distribution of chain e- mails, which are e-mails that require a recipient to send an email to one or more persons upon a promise of some or other reward, whether direct or indirect, or upon a threat in the event of a failure to forward or transmit the e-mail.

8.4. ICT INTERNET USAGE POLICY

8.4.1. Purpose

The ICT Internet Usage Policy sets out the basic responsibilities of users and system providers with regard to the availability and the accessing, surfing and downloading of content from the internet. **This Policy should be read in conjunction with all other LGB ICT Policies.**

8.4.2. Setting up Internet access

The System Administrator must ensure that the LGB network is safeguarded from malicious external intrusion by deploying a configured firewall.

8.4.3. Access to Internet

Access to the Internet is provided to all users but may be restricted to certain times and/or to certain users should it be deemed fit to do so. Sites which contain content which is deemed to be inappropriate or offensive or which may pose a security risk may also be blocked.

8.4.4. Downloading files and information from the Internet

Users must exercise care when accessing unknown websites and/or downloading content and files from the Internet to safeguard against malicious code, viruses and inappropriate material. The accessing of prohibited sites using bypass techniques is not allowed.

8.4.5. Downloaded software

Downloading of unlicensed software is prohibited. All software on a user's system must be licensed prior to installation. The downloading of movies, music and other entertainment is prohibited.

8.4.6. Downloaded information

Information on the Internet may be inaccurate, invalid or deliberately misleading, and any decisions based upon it must be considered carefully before use.

8.4.7. Filtering inappropriate material from the Internet

The organisation will use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet.

8.5. ICT USER ACCOUNT MANAGEMENT POLICY

8.5.1. Purpose

The ICT User Account Management Policy sets out the basic responsibilities of users and network administrators with regard to account management. **This Policy should be read in conjunction with all other LGB ICT Policies.**

8.5.2. User registration

All users must complete a domain user account management form to request access to the Limpopo Gambling Board network and must be approved by the user`s supervisor.

8.5.3. Modifications or changes

The IT Office must be informed by the relevant supervisor, in writing, of any amendments in the job function, role and responsibilities of any user where such an amendment may compromise the integrity of the LGB ICT environment.

8.5.4. User deregistration

Human Resources shall be responsible for notifying the IT Office of employees and others, such as independent contractors, who will be leaving the Limpopo Gambling Board`s employment or otherwise (through reassignment, extended absence, and so forth) and will no longer need access to ensure that all IT equipment belonging to the Limpopo Gambling Board is retrieved and the access rights of the said user can be terminated.
Upon termination of an employee or other person with access, the IT Office will immediately take the following actions:

Revoke and disable access privileges, such as usernames and passwords, to systems, data resources and networks. Retrieve all hardware, software, data, access control items, and documentation issued to or otherwise in the possession of the user.

Sixty (60) days after the account is revoked and disabled, the account will be deleted along with all related home directories and mailboxes unless the directorate has submitted a specific request to IT Office for an extension. Any such request must clearly indicate the specific length of the extension being requested and the final date of account termination that is being requested.

It is the responsibility of the departing employee to delete or transfer all files and email messages that are of a personal nature. These may be transferred to a CD or flash storage drive.

8.5.5. Review of user access rights

User access rights should be reviewed by the relevant supervisors and any amendments should be communicated to the IT Office as follows:

- As and when necessary.
- After any changes such as promotion, demotion or termination of employment.
- When moving from one section or business unit to another.
- Authorisations for special privilege access rights should be reviewed as and when necessary.

8.5.6. Privilege management

- The access privileges associated with each system product, e.g. operating system, database management system and each application, as well as the users to which they need to be allocated should be identified.
- Privileges should be allocated to users on a need to use basis and on an event by event basis, i.e. the minimum required for their functional role and only when needed.
- An authorisation process and a record of all privileges allocated should be maintained by the Network Administrator.
- Privileges should not be granted until the authorisation process is complete. Temporary privileges should be assigned to a different user ID than that used for normal business activities.

8.6. ICT EXTERNAL SERVICE PROVIDERS/CONTRACTORS

8.6.1. Purpose

The policy sets out the basic principles necessary for the secure use and management of LGB information systems and infrastructure. **This Policy should be read in conjunction with all other LGB ICT Policies.**

8.6.2. Access Control

Access to LGB Information Systems, hardware, software, applications and communications shall be by express permission of the data owner and the Information Technology business unit. Contractors must not attempt to enter, unescorted, any LGB area that houses computer processing or communications equipment. This applies to data centres, patch rooms, switch rooms and any other rooms housing IT processing equipment.

8.6.3. Acceptable use

All contractors working in a LGB environment and accessing LGB Information Systems shall abide by the policies set out in the LGB ICT and Information Security Policy. Contractors must adhere to this Policy. Failure to comply with the above policy shall be considered a security breach.

The External Service Providers must ensure that all subcontractors and/or third parties engaged in the fulfilment of its contract with LGB are aware of and agree in writing to adhere to all provisions contained in this ICT and Information Security policy.

8.6.4. Security Clearance to work in a LGB facility

Any contractor or service provider working on system containing sensitive information may be required to obtain the relevant clearance where it is deemed necessary.

8.7. ICT EQUIPMENT POLICY

8.7.1. Purpose

The ICT Equipment Policy sets out the basic responsibilities of users and system providers with regard to the provision, allocation, requisition, procurement, usage and management of ICT equipment. **This Policy should be read in conjunction with all other LGB ICT Policies.**

8.7.2. Equipment Allocation

The processing of **all** requests for ICT equipment is subject to the following:

- The availability of funds.
- Adherence to Supply Chain Management (SCM) guidelines with special emphasis on demand management and asset management.
- A written request or motivation from the head of the requesting unit.

8.7.3. Desktop Computers

- Desktop computers are provided to employees who are, by the nature of their jobs, office bound and who are permanently employed in positions where the performance of their duties will be enhanced by the provision of a personal computer. Such duties will normally fall within the scope of administrative work.
- Desktop computers may also be provided as a shared resource for use by employees whose posts do not require them to have full-time access to a computer, but would enable such employees to access email, internet and general word processing functions.

8.7.4. Notebook Computers

- Only the members of the Management qualify for a notebook computer as well as employees who are not office bound.
- Employees who fall outside the categories listed above, but who may require a notebook computer on the basis of specialised work related duties may be provided with a notebook computer provided that the responsible Manager provides a detailed motivation outlining the specific functions that requires a portable computer approves the request.
- Where a notebook computer is required by a non-qualifying employee on a temporary basis, the IT Office may, on written request by the relevant Manager, make available a notebook computer on loan on a temporary basis as explained in 8.7.10 under Pool equipment.

8.7.5. Printers and other peripheral devices

- Standalone desktop printers are issued to the CEO and the Executive Management.
- Employees working with confidential information e.g. Bid/SCM Office, Labour Relations, Job Evaluation, etc. may also qualify for a standalone desktop printer, provided that the relevant Manager provides a written motivation for the request.
- Employees that do not qualify for a standalone desktop printer will be connected to a network printer closest to their office.
- Memory sticks are classified as stores items and all requests for these items must be directed to supply chain business unit.
- Data projectors, plotters, scanners and digital cameras may be issued to sections that require them. A written request with motivation by the relevant Manager must be made to the supply chain office outlining the need for such a device.

8.7.6. Custodianship of equipment

- All ICT equipment remains the property of Limpopo Gambling Board. ICT equipment is allocated to individual employees as a tool for fulfilling duties and functions as determined by a particular post. The employee occupying that post is personally responsible for the equipment that has been assigned to that post until such time the employee is transferred to another post or Limpopo Gambling Board or resigns.
- The Manager is the overall custodian of all equipment allocated to his or her business unit and should maintain an inventory of all ICT equipment in their respective business units.
- All employees that have been allocated ICT equipment must take the utmost care in preventing theft, damage or loss of the equipment.
- In the unfortunate instance where any equipment has been lost or stolen, the responsible employee must report the matter to the South African Police Services (SAPS) within 24 hours. A case number and a report detailing the incident must be submitted to the Limpopo Gambling Board, supply chain unit.
- Should any equipment be lost due to the employee's negligence, the employee may be required to pay for the lost item.
- No person other than the employee to whom equipment has been allocated may have access to the computer equipment. The exception is the support technicians and the contracted third party hardware maintenance and software support service provider.
- Users are encouraged to handle all equipment with care. Mobile equipment should be transported in their appropriate carry bags.
- Users are also reminded to ensure that equipment is not left unattended and that offices where equipment resides are kept under lock and key. Equipment is to be used only for the purpose for which it was issued.

8.7.7. Replacement and renewal

- IT equipment will be replaced based on the technical assessment by an IT technician. Only equipment that is beyond repair or is older than 36 months will be considered for replacement.
- Equipment retrieved from users will be reallocated to other users. Redundant and irreparable equipment will be disposed of in line with the Supply Chain Management (SCM) disposal principles.

8.7.8. Requisition of equipment

- Equipment requisitions must be made on an official ICT Equipment Request Form (**Attachment**) by the user and approved by the respective Manager.
- No verbal or email requests for equipment will be processed.

8.7.9. Transfer of equipment

- No employee shall move or transfer equipment from one business unit to another.
- In cases where such a transfer is required, the equipment should first be returned to the IT Office for configuration.
- Only after Supply Chain Management has done the proper entries in the asset register will the IT Office release the equipment for reallocation or transfer.
- An employee who vacates or relinquishes a position by virtue of which she or he had been allocated specific computer equipment must hand over the equipment to his or her supervisor prior to departure.
- The supervisor shall accept custodianship of the equipment with effect from the date of vacation or relinquishment by the employee, and return the IT equipment to the IT Office within 14 days.

8.7.10. Pool equipment

- The Limpopo Gambling Board shall make available pool equipment, where possible, to accommodate needs where such needs may not be required on a full-time basis. (E.g. Notebook, Projector, memory device, camera, etc.).
- The equipment will be loaned out by the IT Office upon written request from the head of the borrowing unit on a first come first served basis.
- Pool equipment is a scarce resource and the IT Office does not guarantee that equipment will always be available. Loan of pool equipment is limited to a maximum of 14 days, after which reapplication should to be made.

8.7.11. General

- An asset allocation form must be completed by the assigned user for each allocated device (See annexure 1).
- This form shall contain a detailed description, model and serial number of the said device.
- The user undertakes not to move, transfer, and re-allocate the device without prior written approval from the IT Office.
- Users are strictly prohibited from attempting to conduct repairs or technical modifications on any equipment as this may void any standing warranties or guarantees.
- Employees are advised to ensure physical security and care of their assigned equipment. Special care must be taken in the day to day use of the equipment.

8.8. ANTIVIRUS MANAGEMENT AND MALICIOUS SOFTWARE POLICY

8.8.1. Purpose

The ICT Antivirus Management Policy & Malicious Software Policy sets out the measures that must be taken by employees to help achieve effective virus detection and prevention. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable internet files, and removable media. Their presence is not always obvious to the computer user. A virus infection can be very costly in terms of lost data, lost staff productivity and / or lost reputation.

This policy applies to all computers that run any operating system and are connected to LGB network via a standard network connection, wireless access point or virtual private network connection. The definition of computers includes desktop workstations, laptop computers, handheld computing devices and servers.

8.8.2. Roles and responsibilities

8.8.2.1. IT Office

IT is responsible for executing, monitoring and implementing this policy. While safeguarding the network is the responsibility of every user, IT ensures all known and reasonable defences are in place to reduce network vulnerabilities while keeping the network operating. This responsibility includes the following:

8.8.2.2. User

It is the responsibility of each user to ensure that their devices are regularly connected to the LGB network to ensure that the latest virus definition (signature) files are installed and/or updated.

8.8.2.3. Procedure

Anti-virus software is installed on all LGB desktop workstations and servers running any operating system, following the vendor installation guide provided with the software.

The anti-virus software console window provides complete access to the options available.

The anti-virus software includes the full version of anti-- spyware module, which protects computers from malicious software that is not categorised as a virus. The anti-spyware module blocks spyware, adware, cookies and Trojans.

Real-time Scanning is enabled, and configured so that anti-virus software cannot be disabled on all desktop workstations, laptops, and servers. Real-time Scanning runs automatically and scans a file before opening any file accessed.

The Full Scan option is enabled, so that the anti-virus server will conduct scan of all workstations and servers.

The Full Scan item scans every file on each computer, can be memory-intensive, take several hours to complete and it is run when there are known vulnerabilities over night or at the weekend. To scan a computer hard and flash drive(s) for viruses on an ad- hoc basis, select the Full Scan option in the anti-virus software console window. Antivirus software is configured for live updates to catch new viruses.

This is achieved by ensuring that the anti-virus product is updated in terms of both virus definition (signature) files and the scan engine version being used. The antivirus server is configured to check the vendor's website for updates.

All LGBs servers and workstations are updated from the anti-virus server. If any machine fails an anti-virus update, IT will run a manual update, establish the cause of failure and resolve the issue. Scan engine version patches are only installed onto the anti-virus server when a major version change is implemented. This is done manually from the vendor website, and after being successfully tested, is installed automatically onto all other servers and workstations.

8.9. PASSWORD MANAGEMENT POLICY

8.9.1. Purpose

The purpose of this Policy is to present best practice for the creation of strong passwords, the protection of those passwords, and the frequency of change.

8.9.2. Roles and responsibilities

Users must note that passwords are for their own personal use and must not be shared or disclosed to anyone. It is a breach of this Policy for any user to misuse their own or other user's password. If any such misuse results in a user knowingly elevating their system privileges above those that they have been authorised to use then this will be considered an act of gross misconduct.

- All system-level passwords (e.g. root, enable, Windows admin, application administration accounts, etc.) Must be changed on at least a quarterly basis.
- Remote access to privileged accounts (e.g. root, enable, Windows admin, application administration accounts, etc.) must not be attempted from insecure locations e.g. open access cluster systems or public terminals.
- All user-level passwords (e.g. email, web, desktop computer, etc.) must be changed at least every six months with a recommended change interval of every four months.
- A user account that has system-level privileges granted through group memberships or systems such as Dynamic Local User must have a password that is unique from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

8.9.3. Guidelines

All users should be aware of how to select strong passwords. A strong password has the following characteristics:

- It is least eight characters long.
- It includes upper and lower case letters (e.g. a-z, A-Z); digits and other characters: @ # $ % A & * () - + 1 - - = \ ' {} [1: II; I < >? I. I)
- It is not a word in any language, slang, dialect, jargon, etc.
- It is not based on personal information, names of family, etc.

Weak passwords have the following characteristics:

- The password contains less than six characters.
- The password is a word found in a dictionary (English or foreign).
- The password uses names of family, pets, friends, co-workers, fantasy characters, etc.
- The password uses computer terms and names, commands, hardware, software.
- The password uses predictable words e.g. 'P@ssword', 'LGB01', 'Administrator01'.
- The password uses personal information such as addresses and phone numbers.
- The password uses word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- The password uses names of any of the above spelt backwards or preceded/followed by a digit (e.g., secret1, 1secret).

8.9.4. Password protection standards

Do not use the same password for LGB domain accounts as for other non-LGB accounts (e.g. personal ISP account, online banking, e-shopping, etc.). Where possible, use a different password for different LGB accounts systems. For example, select one password for your desktop login account and a separate password for your remote access account.
Do not share your LGB domain accounts passwords with anyone, including IT staff, administrative assistants or personal assistant.

Here is a list of 'dont's':

- Don't reveal a password over the phone to ANYONE.
- Don't reveal a password in an email message.
- Don't reveal a password to your line manager.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g. 'my family name').
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on holiday.
- Don't use the 'Remember Password' feature of applications.
- Don't write passwords down and store them anywhere in your office.
- Don't store passwords in a file on ANY computer system (including PDAs or similar devices) without encryption.

If someone demands that you reveal your password, refer them to this document or have them contact IT Office. In the event that an account or password is suspected to have been compromised, the incident must be reported to IT Office, all passwords are to be immediately changed. IT Office or a delegated authority may perform password conformance checks on a periodic or random basis.

ANNEXURE 1

a. Sample Asset-allocation form

LIMPOPO GAMBLING BOARD: LGB AM 01

LIMPOPO GAMBLING BOARD
ASSET TRANSFER FORM

Date Requested			
Asset Barcode			
Asset No			
Asset Description			
Asset Classification			
Condition of Asset			
Reason for Allocation			
Permanent	✓	Temporary	
If Temporary: Duration		Date to be returned	
CURRENT LOCATION		**NEW LOCATION**	
Business Unit		Business Unit	
Location / User		User	
User's Signature		User's Signature	
Date Transferred		Date Transferred	
SUPPLY CHAIN MANAGEMENT		**FINANCE SECTION**	
Asset Checked by		Update by	
Official's Signature		Official's Signature	
Date		Date	

8.10. ICT MAINTENANCE PLAN POLICY

8.10.1. Purpose

The ICT Maintenance Plan Policy sets out routine maintenance activities to be carried out on a regular basis and procedures to be followed in performing this activities. **This Policy should be read in conjunction with all other LGB ICT Policies.**

8.10.2. Environment

The LGB ICT environment can be broadly categorised at three levels:

- Workstation Level
- Server Level
- Network Level

8.10.3. Roles and responsibilities

8.10.3.1. IT Manager and Technician

- Introducing and integrating new technologies into the existing environment.
- Monitor network traffic.
- Performing backups.
- Applying operating system and application software updates, and configuration changes.
- Installing and configuring new hardware and software
- Responsibility for system security.
- Troubleshooting any reported problems at network and server level.
- Ensuring that the network infrastructure is up and running.

8.10.3.2. IT Manager and Technician

- Adding, removing, or updating user account information and resetting passwords.
- Answering technical queries.
- Manage IT infrastructure
- Monitor desktop support.
- Monitor routine maintenance activities at workstation level.

8.10.3.3. IT Manager and Technician

- Installing and configuring new hardware and software at workstation level.
- Diagnose and resolve hardware and software issues at workstation level.
- Escalate unresolved issues to consultants.
- Monitor routine maintenance activities at workstation level.

8.10.3.4. End User

- Operate hardware equipment and software applications as per
- LGB ICT Policies.
- Ensure equipment is used responsible and maintained in good condition.

8.11. ICT INCIDENT MANAGEMENT POLICY

8.11.1. Purpose:

The ICT Incident Management Policy sets out the procedures to be carried out in the event of failures or errors to prevent recurrence of incidents related to these errors. **This Policy should be read in conjunction with all other LGB ICT Policies.**

8.11.2. First-level incident management processes

1. Incident detection and recording (Incident Register)
2. Classification and initial support
3. Investigation and diagnosis
4. Resolution and recovery
5. Incident closure

8.11.3. Second-level incident management processes

1. Incident ownership, monitoring, tracking and communication
2. Establish incident framework management
3. Evaluation of incident framework management

8.12. PATCH MANAGEMENT POLICY

8.12.1. Purpose

The ICT Patch Management Policy sets out the procedures to be carried out in order to provide a secure network environment for all applications and users. All computer devices (including servers, desktops, laptops etc.) connected to the LGB network have proper virus-protection software, current virus-definition libraries, and the most recent operating system and security patches installed. **This Policy should be read in conjunction with all other LGB ICT Policies.**

8.12.2. Roles and responsibilities

8.12.2.1 IT

- IT is responsible for the overall patch management implementation, operations and procedures. While safeguarding the network is the responsibility of every user, IT ensures all known and reasonable

defences are in place to reduce network vulnerabilities while keeping the network operating.

- IT will monitor security threats, review vendor notifications and websites and research specific public websites for the release of new patches. Monitoring will include, but not limited to, the following: Scanning the network to identify known vulnerabilities, identifying and communicating identified vulnerabilities to appropriate members, Identifying and communicating identified security breaches to the appropriate members.
- IT will ensure that firewall and antivirus is installed and running all the time and that security updates and service packs are automatically deployed to clients computers.
- IT will monitor security, review vendor notifications and websites and research specific public websites for the release of new patches e.g. SAGE. Monitoring will include, but not limited to, the following:

  ✓ Scanning the network to identify known vulnerabilities.
  ✓ Identifying and communicating identified vulnerabilities to appropriate users.
  ✓ Identifying and communicating identified security breaches to the appropriate users

8.12.2.2. User Responsibilities and Practices

- It is the responsibility of each user to ensure that their devices are regularly connected to the LGB network in order for the latest software updates and anti-virus software to be installed and/or updated.

8.13. ICT SERVICE CONTINUITY POLICY

8.13.1. Purpose

The purpose of this document is to ensure that due consideration is given to the access and availability of transversal ICT systems in the event that the ICT services of LGB are in any way compromised in the event of a disaster; and to ensure that alternative access mechanisms can be activated within the shortest possible time so that LGB activities can be resumed normally with minimum citizen discomfort. **This Policy should be read in conjunction with all other LGB ICT Policies.**

8.13.2. Critical Systems

IT System	Business Process	Business owner	Operational responsibility	Infrastructure Requirements
Accpac	Purchase	CFO	IT Manager/Senior Manager Finance	Computer with a secure connection
PASTEL	Acquisition and accountability	CFO	IT Manager/Senior Manager Finance/SCM Manager	Computer with a secure connection
D-bit	Asset	CFO	IT Manager/Senior Manager Finance	Computer with a secure connection
VIP	Salaries	CFO	IT Manager/Senior Manager Finance	Computer with a secure connection
Ess	Leave system	CFO	IT Manager/HR Manager	Computer with a secure connection
HR	Employee Information	CFO	IT Manager/HR Manager	Computer with a secure connection

8.13.3. Recovery Team

Service	Responsibility
Financial System	SAGE
Printing	IT Manager/Technician
Desktop	IT Manager/Technician
Server	IT Manager/Technician
Wide Area Network	IT Manager/Technician
Local Area Network	IT Manager/Technician

8.14. ICT SERVER ROOM POLICY

8.14.1. Purpose

The ICT Environmental Control Policy provides guidelines for the protection of computer server rooms used to store classified and protected information. **This Policy should be read in conjunction with all other LGB ICT Policies.**

8.14.2. Access Control

Access to the Server room is controlled by:

- Activity monitoring register
- Physical door
- Access Control

8.14.3. Environmental considerations

- No combustibles (boxes, paper, chemicals, etc.)
- No food or other contaminants

8.14.4. Climate Control

- Appropriate climate-control must be maintained.

a. Maintenance Plan Detail

Workstations and Peripherals

No	Actions	Activities	Frequency	Responsibility
1	Operating System Updates	Check and Update: • Security Updates • Patch Management • Service Pack Deployment	 Monthly/Live Monthly/Live Monthly/Live	IT Manager/Technician
2	Application Software Updates	Check and Update: • Software Versions	Quarterly/Live	User
3	Anti-Virus Updates	Check and Update: • Virus Definitions • Software Versions	Weekly/Live Quarterly/Live	User User/IT Technician/Manager
4	Workstation Optimisation	Optimise Hard Disk Space by: • Defragmentation of hard drives • Purging Temporary Internet Files • Flush Deleted Items	Quarterly Weekly Weekly	User User User
5	Physical Environment Optimisation	Check and Fix • Cable Connections / Network Points • Dust Accumulation	Quarterly Quarterly	User/IT Manager/Technician User/IT Manager/Technician
6	File and Data Management	• Backup critical data	Daily	User
7	Reporting	Produce Status Report Of Work Performed And Pending Issues.	Quarterly	Manager: IT

b. Servers

No	Actions	Activities	Frequency	Responsibility
1	Operating System Updates	Check and Update: • Security Updates • Patch Management • Service Pack Deployment	As and when necessary	Administrator Administrator Administrator
2	Application Software Updates	Check and Update: • Software Versions • Patch Management	As and when necessary	Administrator Administrator
3	Anti-Virus Updates	Check and Update: • Virus Definitions • Software Versions	As and when necessary	Administrator Administrator
4	Server Optimisation	Monitor and Optimise Storage Space by: • Defragmentation of hard drives • • Flush Deleted Items Monitor server event logs and correct errors.	As and when necess ary	IT Manager/Technician
5	Physical Environment Optimisation	Monitor and Correct: • Cable Connections / management • Dust Removal	As and when necessary	IT Manager/Technician

No	Actions	Activities	Frequency	Responsibility
		• Environment (temperature) • Fire Safety Measures		Network Administrator Network Administrator
6	File and Data Management	Backup of Data • Monthly (Full) • Weekly (Incremental) • Daily (Incremental)	Monthly Daily	IT Manager/ Technician Administrator Network Administrator
7	User Account Management	Monitor and Manage User Account Logs	Monthly	Manager:IT
8	Reporting	Produce Status Report of work performed and pending issues.	Monthly	Manager: IT

c. Network

No	Actions	Activities	Frequency	Responsibility
1	Maintain Network Infrastructure	Check and Rectify Faults On: Switches Routers Wireless Access Points Network Printers	As and when necessary	Service Provider Service Provider Service Provider Service Provider Service Provider
	Maintain Network Security	Update Firewall Operating System Check Firewall Rules	As and when necessary	Service Provider IT Manager/Technician
		Monitor and Correct: Cable Connections / management Dust Removal Environment (temperature) Fire Safety Measures	As and when necessary	IT Manager/Technician/ HR Manager and supply chain

d. Maintenance Checklist Forms

Networks

NETWORK	LGB ICT Maintenance Checklist								Page 1/2
Location						Name:			
Date:			Time:			Signature :			
Description		**Environmental**				**Security (Firewall)**			**FINAL STATUS**	**Report**
Device	Asset No.	Dust	Cables	Temp	Fire	Logs	Rules	Update		Notes
		[redacted]	[redacted]		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	

NETWORK		LGB ICT Maintenance Checklist								Page 2/2
Description		Environmental				Security (Firewall)			FINAL STATUS	Report
Device	Asset No.	Dust	Cables	Temp	Fire	Logs	Rules	Update		Notes

e. Workstations

WORKSTATION	LGB ICT Maintenance Checklist					Pg. 1/2
Location :			Name :			
Date :		Time :	Signature :			
User Name :			Employee No. :			
Workstation Type:			Asset No. :		S/No. :	
Attached Device 1 :			Asset No. :		S/No. :	
Attached Device 2 :			Asset No. :		S/No. :	
Actions/Activities	**Status**	**Notes/Comments**				**Final Status**
Environment Optimisation						
Remove Dust						
Check Cable Connections						
Operating System Updates						
Verify Security Updates						
Verify Installed Patches						
Verify Service Packs						
Application Software Updates						
Verify Installed Patches						
Verify Versions						

WORKSTATION	LGB ICT Maintenance Checklist		Pg. 2/2
Actions/Activities	**Status**	**Notes/Comments**	**Final Status**
Anti-Virus Updates			
Verify Live Updates			
Perform Scan			
Optimization Tasks			
Purge Temporary Files			
Flush Recycle Bin			
Archive Emails			
Purge Deleted Emails			
Defrag Hard Disk Drives			
File & Data Management			
Perform Manual Backups			
Verify Home (Shared) Directory			

f. Servers

SERVERS	LGB ICT Maintenance Checklist		Pg. 1/2
Location & District :		Name :	
Date :	Time :	Signature :	
Server :		Asset No. :	
Actions/Activities	Status	Notes/Comments	Final Status
Environment Optimisation			
Remove Dust			
Check Cable			
Check Fire & Safety Measures			
Check Temperature			
Operating System Updates			
Perform Security			
Install Patches			
Deploy Service Packs			
Application Software Updates			
Install Patches			
Version Updates			

SERVERS	LGB ICT Maintenance Checklist		Pg. 2/2
Actions/Activities	Status	Notes/Comments	Final Status
Anti-Virus Updates			
Update Virus Definitions			
Perform Scan			
Print Event Logs			
Server Optimisation Tasks			
Purge Temporary Files			
Check User Account Logs			
Flush Deleted Items			
Defrag Hard Disk Drives			
Print Event Logs			
File & Data Management			
Perform Manual Backups			
Verify Automated Backups			
Secure Off-site Backups			
Print Event Logs			

9. DEFAULT

An employee who fails to comply with the provisions of this policy shall be dealt with in terms of the LGB Disciplinary Code and Procedures for the LGB.

10. INCEPTION DATE

The inception date of this policy is 30 days after approval by the Head of Limpopo Gambling Board.

11. REVIEW

This policy shall be reviewed every two years (2).

12. TERMINATION

This policy shall remain in force until and unless it has been withdrawn and/or amended.

13. ENQUIRIES

Enquiries regarding the policy shall be directed to the Chief Executive Officer.