Adopted Date: 1.21.20
Effective Date: 2.21.20

POLICY MANUAL

HUMAN RESOURCES POLICIES

ACCEPTABLE USE POLICY

PURPOSE

To establish a policy for the acceptable use of Mississippi Lottery Corporation (MLC) information systems and resources by all employees and supporting entities, including contractors, vendors, and any others deemed as such by the MLC.

BACKGROUND

MLC information systems and resources are provided to support the MLC in its mission and business objectives. Inappropriate use by any employee could jeopardize the integrity, security, and privacy of all MLC employees and supporting entities. Ensuring that information systems and resources are used appropriately is a priority of the MLC.

POLICY

1) Employees shall have no expectation of privacy regarding emails, documents, phone calls, text messages, photos, or other correspondence prepared, stored, sent, or received utilizing the MLC network or devices. All communications can be disclosed to internal personnel, law enforcement, or other third parties without prior consent of, or notice to, the sender or the receiver.

2) MLC email accounts are for business use only and shall not be used for personal email messages. Personal email accounts shall not be used for business purposes and access to personal email is prohibited on MLC devices. MLC email accounts shall not be used to register for personal online accounts and services.

3) Passwords shall not be shared with anyone and must not be publicly displayed.

4) Employees shall lock their computer when leaving the immediate vicinity of their work area.

5) Data stored on the MLC network and devices are and remain at all times property of the MLC. Employees shall not copy, transfer, rename, add, or delete data belonging to other users unless given express permission to do so by the information owner.

6) Software shall not be installed on any MLC device by any employee. Software installations must be approved and completed by the IT Department. This includes but is not limited to freeware, shareware, utilities, browser plugins, toolbars, and games.

7) Software owned or licensed by the MLC shall not be copied to alternate media, distributed by email, transmitted electronically, or utilized on any device other than those authorized by the IT Department. Employees are responsible for using software in a manner consistent with the licensing agreements of the manufacturer.

8) Personal devices and hardware shall not be connected to the MLC network or devices. This includes but is not limited to phones, laptops, tablets, printers, monitors, keyboards, mice, and removable media.

9) MLC devices, except those issued for remote work, shall not be removed from the premises without explicit authorization by the IT Department.

10) Portable devices (laptops, tablets, phones, etc.) issued to employees must be physically secured at all times. These devices shall not be left unattended in public places or stored overnight in vehicles. When traveling by air, devices shall not be stored in checked baggage. If staying in a hotel, devices shall be placed in an inconspicuous and safe location when possible.

11) Employees shall be held financially responsible for any equipment assigned to them that is deemed unusable by the IT Department or is damaged due to willful neglect or abuse. This includes the cost of repairs or replacement up to the full cost of the equipment and its software. Lost or damaged equipment must be immediately reported to the IT Department.

12) MLC cell phones are for business use only and shall not be used for personal text messages, phone calls, or as a hot spot to share internet connectivity with other devices.

13) Non-public information shall not be disclosed to anyone without a legitimate business need, with disclosure to a third party requiring explicit approval by the information owner. Employees are responsible for protecting the information to which they have access. Non-public information includes but is not limited to Personally Identifiable Information (PII), banking and financial information, information covered by non-disclosure agreements, proprietary information, Central Gaming System (CGS) data, and Internal Control System (ICS) data.

14) The MLC network and devices shall not intentionally be used in an illegal, malicious, or obscene manner. This includes but is not limited to disseminating spam, conducting denial-of-service attacks, using peer-to-peer networking services, accessing or storing pornography, participating in political activities, solicitation, and using resources for personal financial gain.

15) The downloading and storage of MCL data to removable storage media (USB drives, portable hard drives, CD/DVD's) is prohibited unless explicitly approved by the information owner and the IT Department. The requesting employee is responsible for protecting the data and tracking the removable media until delivery or destruction.

16) The use of cloud-based applications and storage (Dropbox, Google Docs, ShareFile, etc.) for MLC data is prohibited. MLC currently uses its own Microsoft 365 tenant to provide these services, which is the only approved solution.

17) Internet usage shall be limited to business purposes. Occasional personal use is acceptable during designated break periods, so long as such use is consistent with this policy.

18) Employees who observe actions in violation of this policy should report such incidents to Human Resources, which may include investigation by the Security and/or IT Department for further action.

19) Any employee who violates this policy may be subject to disciplinary actions up to and including termination of employment.