Little Traverse Bay Bands of Odawa Indians
Tribal Court

Tribal Court Client Laptop Acceptable Use Policy

1.0 Overview

LTBB Tribal Court is providing laptop computers to clients participating in specialty court programming. The purpose of providing laptops to clients is to reduce barriers to clients' ability to participate in programming and fulfill programming requirements. The Court's intentions for publishing an Acceptable Use Policy is to ensure that laptops issued to clients are utilized in a manner that is consistent with the Tribal Court's mission and the values reflected in specialty court programming. This Acceptable Use Policy sets forth limitations, restrictions and permissible uses of Court issued laptops and preventing Court issued laptop from being compromised by malware, ransomware and cyber-attacks.

Court issued laptops are the property of LTBB and are loaned to clients participating in specialty court programming. These laptops are to be used for purposes consistent with a client's participation in specialty court programming and fulfilling program requirements.

Effective security is a team effort involving the participation and support of specialty court clients who are using and accessing Court issued laptops. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of laptops issued to LTBB Tribal Court specialty court clients. These rules are in place to protect the client and the Tribal Court. Inappropriate use exposes LTBB to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to Tribal Court clients who have been issued laptops. This policy applies to all equipment that is owned or leased by LTBB Tribal Court.

4.0 Policy

4.1 General Use and Ownership

1. While Tribal Court's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the laptops remains the property of Tribal Court. Because of the need to protect LTBB's network,

management cannot guarantee the confidentiality of information stored on any network device belonging to LTBB Tribal Court.

2. Clients are responsible for exercising good judgment regarding the reasonableness of personal use. Clients **SHALL NOT** utilize the laptops for any of the following purposes:
    a. Planning, committing, or conspiring to commit, a criminal act.
    b. Viewing, publishing, producing or distributing pornography.
    c. Visiting, viewing or creating a website or webpage that promotes drug use or addiction.
    d. Visiting, viewing or creating a website or webpage that promotes, discusses, sells products or provides methods for circumventing drug testing or drug/alcohol monitoring.
    e. Downloading any programs that are designed to mask, conceal, or delete user activity.
    f. Downloading any programs or files that are not related to the completion of, or participation in, specialty court programming requirements.
3. LTBB Tribal Court recommends that any information that users consider sensitive or vulnerable be encrypted. LTBB Tribal Court cannot guarantee that information sent or created on laptops issued by the Tribal Court is secure.
4. For security and network maintenance purposes, authorized individuals within LTBB and the Tribal Court may monitor equipment, systems and network traffic at any time, per LTBB MIS's Audit Policy. This policy is available upon request.
5. LTBB Tribal Court reserves the right to audit laptops, networks and systems on a periodic basis to ensure compliance with this policy. This means that Tribal Court staff may access and review files, programs, browser history and cookies on laptops issued by the Tribal Court.

4.2 Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every sixty days. Tribal Court clients must provide their username and password to the Specialty Court Coordinator and must inform the Specialty Court Coordinator of any changes to their username and password.
2. All PCs, laptops and workstations should be secured with a password-protected screen saver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Windows users) when the host will be unattended.
3. Use encryption of information in compliance with MIS's Acceptable Encryption policy.
4. Because information contained on portable computers is especially vulnerable, special care should be exercised.
5. Clients must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

Under no circumstances is a client of LTBB Tribal Court authorized to engage in any activity that is illegal under tribal, local, state, federal or international law while utilizing LTBB-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by LTBB.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which LTBB or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a LTBB Tribal Court computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services on a Tribal Court issued laptop.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to MIS is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within LTBB's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by LTBB or connected via LTBB's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement
Any client found to have violated this policy may be subject to a probation violation, loss of the device and any other sanction that the Tribal Court may deem appropriate.

6.0 Damage or destruction of laptop. Clients who receive a court-issued laptop agree that they are responsible for any damage to, or the destruction of a Court issued laptop. Clients agree that they are responsible for any costs associated with the repair, or replacement of, a Court issued laptop that they have been issued.

7.0 Definitions

Term	**Definition**
“Spam”	Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History
1. The first version of this policy was adopted on May 12, 2022.

Client Acknowledgment of Policy

I acknowledge that I have read the above policy, that I understand it and agree to follow the terms of the policy. I understand that using the laptop issued by Tribal Court in manner that violates this policy may be considered a program violation and that I may receive a program sanction for violations of this policy.

Date: _____ _____

Client Name: