Tombigbee Communications LLC
Policy and Procedure – Consumer Protection Policy

I. INTRODUCTION

This document contains our policies and procedures for complying with the obligation to protect the confidentiality of its telecommunications customers consistent with applicable law, including the regulations governing identity theft. All Tombigbee Communications LLC employees are required to understand and comply with these policies and procedures. Note that all customer and employee information is entitled to legal protection for reasons separate and apart from the FTC's regulations. Questions concerning these policies and procedures should be directed to the Tombigbee Communications LLC Director of Regulatory Affairs or Identity Theft Task force. It will be the responsibility of the task force to coordinate and oversee the plan. The Consumer Protection Policies are intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Tombigbee Communications LLC without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

Information is categorized into three main classifications:

- Customer or Employee
- Company, i.e. Tombigbee Communications LLC
- Public

Public information is information that has been declared public knowledge by someone with the authority to do so and can freely be given to anyone without any possible damage to Tombigbee Communications LLC.

Information outside of public should be treated as confidential. It is a continuum, in that it is understood that some information is more sensitive than other information and should be protected in a more secure manner. Tombigbee Communications LLC employees, service providers and vendors have access to a variety of sensitive customer or employee information, such as credit cards, debit or saving account numbers, social security numbers, Tombigbee Communications LLC trade secrets, financial, marketing and some technical. Tombigbee Communications LLC has established these policies and procedures, which establish the protection of sensitive information. Included under confidential treatment would be other information integral to our success.

A subset of Tombigbee Communications LLC Confidential information is "Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Tombigbee Communications LLC by that entity under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into our network to support our operations.

Tombigbee Communications LLC personnel are encouraged to use common sense judgment in securing Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager.

Any individual who is found to have misused confidential information is in violation of this Policy and Procedure and will be subject to disciplinary action up to immediate dismissal as outlined in the Tombigbee Communications LLC Employee Handbook.

II. DEFINITION OF RED FLAG RULES

1. Customer personal information is information Tombigbee Communications LLC obtains or creates in the normal course of providing telecommunications services to its customers or by its employment of personnel. A "Covered Account", are those accounts used mostly for personal, family or household purposes and involve multiple payments or transactions. Covered accounts that Tombigbee Communications LLC would have access to would be credit card accounts, saving or checking accounts, telecommunication accounts including cell phone accounts. This also extends to employee information that is sensitive in nature and which Tombigbee Communications LLC maintains.

2. A covered account is also an account for which there is a foreseeable risk of identity theft.

3. A "RED FLAG" is a pattern, practice, or specific activity that indicates the possible existence of identity theft. We will demonstrate within our policies and procedures how we comply with the Red Flag rules. The plan will address the following requirements:

1. Establish a written policy/program to protect against Identity Theft

2. Detect Red Flags:

i. Verify identity of person opening a covered account
ii. Obtain identifying information about a customer –password
iii. Authenticate customers
iv. Monitor customer transactions
v. Verify change of address requests

3. Respond to Red Flags:

- Identify factors leading to identity theft
- Security of sensitive information
- Response to unauthorized access to account information

The company's policies and procedures will further define responses to Red Flag Indicators, which will address the following:

i. Describe how we will monitor a covered account.
ii. Describe the process of when and how a customer should be contacted
iii. Describe how often we change passwords or security codes and what type of "strong password" program do we have in place
iv. Describe how closing an existing account and then reopening the account is handled.
v. Describe our procedure on using a debt collection agency
vi. Describe the process of when and how local law enforcement should be notified
vii. Describe the process to determine when no response is warranted.
viii. Describe the type of data security that is used within our information system
ix. Describe how monitoring and testing of our policies and procedures will take place
x. Describe sensitive information retention policy

4. Describe how the Federal Trade Commission's five established Categories of Red Flags will be used:

- Alerts, notifications, warnings from a consumer reporting agency
- Suspicious documents
- Suspicious personal identifying information
- Unusual use of, or suspicious activity related to a covered account
- Notice from customers, victims, or law enforcement

We will within our policies and procedures define how we will use the five categories of Red Flags.

III. WHAT ARE THE RED FLAG REQUIREMENTS

Tombigbee Communications LLC is required to develop a written information security plan that describes our program to protect customer information. The plan will contain the following elements:

- Identify one or more employees who will coordinate its information security program
- Identify and assess the risks to customer information in each relevant area
- Evaluate the effectiveness of current safeguards for controlling these risks
- Regular monitoring and testing of the plan's effectiveness
- Incorporate Red Flag safeguards in contracts with service providers
- Adjust the program as changes occur within the business or operations

The plan will incorporate "Red Flag" indicators, which are used to protect, trigger inspection or direct the reaction to the misuse of personal information.

IV. DETECTING AND RESPONDING TO RED FLAGS

Policies and procedures will define how we intend to detect and respond to Red Flag Indicators to prevent and mitigate the potential risk of Identity Theft within our organization. All employees will be required on an annual basis to attend training on the Tombigbee Communications LLC's Identity Theft Policies. New hires will be required as part of their orientation to review the Identity Theft Policies in conjunction with CPNI Policies and Procedures. The Tombigbee Communications LLC's policies and procedures are design to aid employees in understanding, detecting and preventing the potential risk of identity theft. The Tombigbee Communications LLC policies will further define how we will adhere to the Red Flag rules by implementing the following procedures.

AUTHENTICATING CUSTOMER INFORMATION:

It will be the responsibility of employees who deal directly with sensitive customer information to verify the customer. We currently do this as part of our CPNI practices, however, the Red Flag rules now require that before any information is given or changes are made to an account, the customer must be authenticated by use of a password. Each customer will receive a pre-assigned password that will serve as their customer authentication for Identity Theft and CPNI. We use the same CPNI procedure for establishing or changing passwords. Customers who use electronic bill payment will use passwords they have chosen. The verification process also includes being on guard for any suspicious looking documents or other information requests. This may include identification or information that appears to have been altered. We use Equifax as our third-party source to verify customer information. When suspicious activity identified will be reported immediately to a supervisor and then to the Identity Theft Coordinator.

Specific customer verification steps will be used in the following instances:

OPENING A COVERED ACCOUNT:

When customer opens or changes an account it will be the responsibility of the Customer Service Representative and Installation Technician to verify the identity of the person.

IN-STORE VISIT: When a customer comes into any retail facility to sign up for services, part of the process will be to:

a. asks to see a valid driver's license or other photo identification;

PLACING ORDER BY PHONE: When a customer opens or changes an account by phone, the following process will be used:

a. the customer will be advised that at the time of the installation, the service technician will ask to see a valid driver's license or other photo identification. The installer will be responsible to check the validation box on the service order;

b. the customer will also have the option to stop into the office prior to installation to present a valid photo ID.

CLOSING AND REOPENING A COVERED ACCOUNT:

Closing an account: There are two ways an account can be closed: voluntary and in-voluntary.

Voluntary: When a customer chooses to cancel service with us. The customer's closed account should have sensitive information removed or the account purged after a three year period or after the final payment has been made. Sensitive information that is retained from customers who cancelled service will be kept secure.

Involuntary: When Tombigbee Communications LLC has suspended or canceled a customer's account for non-payment or malicious/illegal use of services. The same identity theft guidelines apply in that a customer must be verified prior to services being reactivated by supplying their password.

Customer death – A death certificate must be presented in order for the account to be closed. Sensitive information will be destroyed.

Customer incapacitation – The customer's personal representative or power of attorney will be presented as proper documentation before changes or closing of the account can be processed.

SUSPICIOUS ACTIVITY RELATED TO A COVERED ACCOUNT:
It will be the responsibility of Customer Service, the Broadband Service Center, the Help Desk and the Finance department to use these indicators to assist in monitoring and reporting suspicious activity. However, all employees should be aware of and using these indicators to help identify suspicious activity. This will include:

1. verifying change of address activity;
2. nonpayment when there is no history of late or missed payments;
3. unusual phishing for credit card or bank information, personal information related to the account;
4. a material change in telephone calling patterns in connection with a phone account;
5. an account that has been inactive for a long period of time is used;
6. mail sent that is repeatedly returned as undeliverable even though transactions continue to occur on the customer's account;
7. customer notification they are not receiving their paper account statements;
8. customer notification of unauthorized charges or transactions in connection with a customer's account.

RETENTION OF SENSITIVE INFORMATION:
It will be our policy and procedure to retain relevant sensitive information for no more than three years in accordance with our Data Retention Policy. The following guidelines apply:

DISPOSAL OF SENSITIVE INFORMATION:
Deposit outdated paper information in specially marked disposal bins on company premises; electronic data will be expunged/cleared. Reliably erase or physically destroy outdated materials. Each department will be equipped with or have easy access to

shredders. At NO TIME should sensitive information be included in recycle bins if not properly shredded.

USE OF DEBT COLLECTION AGENGIES:
It is our policy to use an outside debt collection agency once a customer's account is 90-days past due. After 90-days of non-payment, Accounts Receivable sends all the pertinent information on the customer to the specified debt collection agency. Pertinent information may include name, Social Security number, addresses, phone numbers, account information, and amount due. The contractual agreement with the service agency must ensure it requires them to maintain safeguards. It will be our responsibility to oversee their handling of customer information.

V. DATA SECURITY

PHYSICAL SECURITY:
All office locations have security measures in place that include both the entry to and from the building during non-business hours. It will be the responsibility of senior management to determine which employees require 24x7 access to each building location. Security ID badges with photo identification must be worn especially when entering the building during non-business hours. Personnel who are required to enter customer premises must present photo identification.

Visitors will be required to check in at all times and shall wear a visitor's badge. A list of approved non-company employees permitted into areas outside of the front office will be distributed to all department managers/supervisors. At no time shall a non-company employee be left unattended within the building.

Each employee will be required to sign a confidentiality agreement.
Immediately deny access when employees are no longer employed.

Each department will create a list of employees who have access to sensitive information. Those lists will be given to Human Resources and the Identity Theft Coordinator.

Physical security will also mean having possession of an assigned computer at all times, or locking the computer in an unusable state. Discarded computers should be properly disposed of and information erased. A laptop or other portable computer, should never be left unattended, whether in or out of the office.

ELECTRONIC SECURITY: Employees will be required to use the company's corporate E-mail system for business messages. At no time should sensitive information be sent electronically without the proper encryption or when possible, sent via a private link to approved recipients outside of company premises.

A. PASSWORD PROTECTION:

Passwords are an important aspect of computer security.

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on quarterly basis.

- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

It will be the responsibility of Network Operations to assign each employee a secure network password that will be changed every six months. The following parameters apply.

Not be less than ten characters
Passwords will not contain any common usage word such as:

- Names of family, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns like aaabbb, zyxwvuts, 123321, etc.
- Any of the above spelled backwards.
- Any of the above preceded or followed by a digit (e.g., secret1)

1. Do not use a Tombigbee Communications LLC assigned password for personal access (e.g., personal ISP account, bank account, stock trading, benefits, etc.).

2. Never share passwords with anyone, including other Tombigbee Communications LLC employees unless absolutely required. Employees must use their own passwords when working at a non-assigned workstation. Network Operations will be the exception to individuals within the Tombigbee Communications LLC who have access to Tombigbee Communications LLC-wide system passwords. It will be their sole responsibility to develop, monitor and protect Tombigbee Communications LLC passwords at all times. All passwords are to be treated as sensitive and confidential information.

If an account or password is suspected to have been compromised, please report it immediately to your supervisor, manager or the Identity Theft Coordinator.

B. ENCRYPTION PROTECTION:

Offensive comments about race, gender, hair color, national origin, religion, disabilities, politics, age, sexual orientation or pornography through use of the

Tombigbee Communications LLC E-mail system is prohibited. Employees who receive these type of E-mail
messages from within the Tombigbee Communications LLC should report it to your supervisor.

Tombigbee Communications LLC E-mail messages must contain our confidential clause statement. Including
quotes or other signature lines to external Tombigbee Communications LLC E-mails except for contact
information and confidentiality statement is not acceptable.

TOMBIGBEE COMMUNICATIONS LLC employees shall have no expectation of privacy in anything they store, send or receive on the Tombigbee Communications LLC's E-mail system. The company may monitor messages without prior notice, however it is not obliged to monitor E-mail messages.

Company network security is the responsibility of the Director of Technical Operations and network operations personnel.

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 1 week.
    - Daily incremental tape backups will be retained for at least 1 month.
    - Weekly full tape backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to VP of Technical Operation, who will review logs and report incidents to Identity Theft Coordinator and management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

- Sensitive data transfers should never be sent in a manner that is not secure and should always be encrypted before leaving company premises. At no time should sensitive information be sent within e-mail messages whether the destination is internal or external without proper security measures.

C. VIRTUAL PRIVATE NETWORKS (VPNS):

This policy applies to all employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing a VPN to access the Tombigbee Communications LLC network. This policy applies to implementations of VPNs that are directed through Network Operations.

Approved employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of a VPN, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong pass phrase.
3. When actively connected to the corporate network, a VPN will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by the network operations group.
6. All computers connected to internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.
7. VPN users will be automatically disconnected from the network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not company-owned equipment must configure the equipment to comply with the company's VPN and Network policies.
10. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the company's network, and as such are subject to the same rules and regulations.

D. INTERNAL LAB SECURITY:

This policy establishes information security requirements for labs to ensure that Tombigbee Communications LLC confidential information and technologies are not compromised, and that production services and other company interests are protected from lab activities. This policy applies to all internally connected labs, employees and third parties who access Tombigbee Communications LLC labs. All existing and future equipment, which fall under the scope of this policy, must be configured according to the referenced documents.

The Network Operations must maintain a firewall device between the corporate production network and all lab equipment. All traffic between the company network and the lab network must go through a company-maintained firewall. Lab network devices (including wireless) must not cross-connect the lab and live company networks.

The enable password for all lab owned gateway devices must be different from all other equipment passwords in the lab. The password must be in accordance with company *Password Policies*. The password will only be provided to those who are authorized to administer the lab network.

In labs where non-company personnel have physical access (e.g., training labs), direct connectivity to the corporate production network is not allowed. Additionally, no company confidential information can reside on any computer equipment in these labs.

All lab networks with external connections must not be connected to the company network or any other internal network directly or via a wireless connection, or via any other form of computing equipment.

E. ANTI-VIRUS GUIDELINES:

Recommended processes to prevent virus problems:

- Always run supported anti-virus software from the company download site. Download and run the current version; download and install anti-virus software updates as they become available;
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash;
- Delete spam, chain, and other junk email without forwarding;
- Never download files from unknown or suspicious sources;
- Avoid USB sharing unless there is absolutely a business requirement to do so;
- Back-up critical data and system configurations on a regular basis and store the data in a safe place;
- New viruses are discovered almost every day so periodic updates will be conducted by network operations personnel.

VI. MONITORING OF AND RESPONSE TO UNAUTHORIZED ACCESS

A. DETECTING BREACHES IN SECURITY:

AUDITS & MONITORING - It will be the responsibility of Network Operations to monitor and conduct system information audits on a regular and recurring basis for potential or attempted access to sensitive information within the network. As part of these audits incoming traffic will be monitored for signs of data breech.

The sole purpose of audits will be to:

- Ensure integrity, confidentiality and availability of information and resources;
- Investigate possible security incidents and ensure conformance to security policies;
- Monitor user or system activity where appropriate.

Access may include:

- User level and/or system level access to any computing or communications device;
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on equipment or premises;
- Access to work areas (labs, offices, cubicles, storage areas, etc.);
- Access to interactively monitor and log traffic on company networks.

The Tombigbee Communications LLC Identity Theft measures will be routinely monitored and tested to make sure all employees are in compliance and any failures in the processes are corrected or modified.

Each department will be responsible to reinforce or enhance the policies by creating departmental security programs that correlate with the overall company security measures.

This policy covers all computer and communication devices owned or operated by Tombigbee Communications LLC. This policy also covers any computer and communications device that are present on company premises, but which may not be owned or operated by Tombigbee Communications LLC.

B. ALERTS, NOTICATIONS AND WARNINGS

It will be the responsibility of employees and departments that deal directly with consumers, system information or billing systems to adhere to the following procedure for alerts and notifications that are derived internally or from external sources such as government security or industry alert websites, consumer reports, financial institutions or other creditors. These notifications should be used to alert personnel of activity that could pose as a potential Identity Theft risk or attack. These reports can indicate a pattern of activity that is inconsistent with the history of an applicant/customer or warnings of new electronic or phishing attacks. It will be the responsibility of employees who receive these alerts or warnings to share them immediately with all employees through a staff e-mail alert.

C. RESPONSE TO BREACH OR ATTACK

When a breach in security is identified the following procedure will be in place dependent on the severity of the attack.

Severe breach – unauthorized person(s) have gained access into critical systems or obtain sensitive information, such as Social Security Numbers, bank or credit card account numbers.

Once the breach has been identified an immediate overview of the comprised information or situation will be supplied to senior management by the VP of Technical Operations or the Identity Theft Coordinator. Senior management will then decide based on the severity of the breach whether to alert local law enforcement or federal agencies such as United States Secret Service (USSS) and/or the Federal Bureau of Investigation (FBI) simultaneously employees will be made aware of the situation, which will cause a high alert warning. Customer or public notification will not occur until local law enforcement has been notified or the company is directed by either the FBI or USSS to delay notification. Senior Management will, at its discretion, choose the language and method by which to describe the circumstances to its customers or public. However, the information must clearly describe what is known about the compromise, how it happened, what information was taken and, if we know, how the perpetrators have used the information along with what actions have been taken to remedy the situation. The notification must also explain the appropriate steps customers should take depending on the type of the information taken.

Moderate breach – unauthorized person(s) have made several attempts to gain access or information.

Company personnel should notify their supervisor, who will then notify the Identity Theft Coordinator or VP of Technology as to the nature of the attempts made. A staff alert will be sent by the Identity Theft Coordinator noting the suspicious activity that is occurring and the necessary steps that should be taken to heighten security measures.

B. SECURITY PRACTICES FOR VENDORS OR SERVICE PROVIDERS:

In cases where the company engages a service provider or vendor to perform activities in connection with one or more covered accounts, it will be the company's responsibility to ensure that the activity of the service provider or vendor is conducted in accordance with reasonable policies and procedures, which detect, prevent and mitigate the risk of identity theft.