Frontier Data Privacy and Security Policy

I. Protection of Confidential Information

Confidential information includes all nonpublic information that might be of use to Frontier's competitors, or could be harmful to Frontier or its customers or suppliers, if disclosed. It includes all nonpublic Frontier financial information. Confidential information may also include information that a supplier or customer has entrusted to us.

You must safeguard confidential information by following company policies and procedures, including but not limited to Frontier's Code of Business Conduct and Ethics, Electronic Communications Policy, policies regarding the protection of Customer Proprietary Network Information (CPNI) and contractual agreements for identifying, using, retaining, protecting and disclosing this information. You may not release nonpublic Frontier financial information to the public or third parties unless specifically authorized by Frontier's Chief Financial Officer. You may not release other confidential information to the public or third parties unless you are specifically authorized by a vice president or higher-level supervisor to do so. You may only disclose confidential information to employees who have demonstrated a legitimate, business-related need for the information. If you receive a subpoena or court order that requires the disclosure of confidential information, you must coordinate your response with Frontier's Security and Legal Departments. You may never disclose confidential information to Internet forums (including "blogs", chat rooms or electronic bulletin boards), selected shareholders or financial analysts.

When outside parties request confidential information, you must inform your supervisor and refer the requesting party to Frontier's Security or Legal Department. Even after the company releases information, you should be mindful that related information may still be confidential and must be protected. Your obligation to safeguard confidential information continues after your employment with the company terminates. Without Frontier's specific written prior authorization, you may never disclose or use confidential information. If you suspect or are aware of any improper disclosure of confidential information, you must report it to Frontier's Security Department immediately.

This prohibition applies specifically (but not exclusively) to inquiries about Frontier that may be made by the media, investment analysts, or others. It is important that all such communications on behalf of Frontier be made through an appropriately designated official. Unless you are expressly authorized to the contrary, if you receive any inquiries of this nature, you should politely decline comment and refer the inquiry to Frontier's Corporate Communications Department.

You cannot accept confidential information belonging to a third party (including information from a former employer) unless the person disclosing the information is authorized to do so, Frontier has the owner's written permission to receive it, and the information is provided according to a written agreement that has been approved in advance by your supervisor and Frontier's Legal Department.

II. Customers' Confidential Information.

Federal and state laws also impose obligations on Frontier and its employees to protect information about customers and the services they purchase from Frontier and its affiliates. The Federal Communications Commission has implemented rules imposing obligations on Frontier to protect information about customers and the services they purchase from Frontier (called customer proprietary network information or CPNI). Only authorized Frontier employees can access CPNI. Frontier personnel so authorized must follow all Frontier's procedures regarding access to, use of, and disclosure of CPNI. Frontier cannot disclose CPNI to unaffiliated third parties (including vendors and third parties engaged in marketing or sales efforts on behalf of Frontier) except as authorized by the customer or as compelled (e.g. a subpoena) or authorized by law in consultation with Frontier's Legal Department. When disclosing confidential customer information in connection with a request from a customer or customer representative, employees should confirm that the party requesting records or information associated with an account is the customer or an authorized customer representative on the account. Additional requirements apply to the disclosure of "Call Detail Information" over the telephone or in person. Additional details are provided in Frontier's comprehensive policy on CPNI which is attached hereto. All employees must follow the requirements of this policy.

Employees should assume that all customer information included in the customer's account records and on the customer's Frontier bill, other than the information published in Frontier directories or available publicly through Frontier Directory Assistance is confidential. Questions regarding what is confidential should be directed to Frontier's Legal Department.

Employees must not — or permit others to — access, listen to, monitor, record, tamper with or intrude upon any customer conversation or non-voice communication, or divulge their existence, except as required for business purposes in response to a verified service or installation order, to comply with a valid legal order or law, or when authorized by Frontier's Security or Legal Department.

III. Protection of Property and Confidential Information.

You must always protect Frontier's tangible and intangible property and any property entrusted to your care by customers or business providers. Frontier property and the property of co-workers, customers, and business providers may not be taken, sold, loaned, given away or otherwise disposed of, regardless of its condition or value, without specific authorization. Property includes, but is not limited to, tangible property, data, records, and all communications.

It is never appropriate to use Frontier machinery, switching equipment or vehicles for personal purposes, or any device or system to obtain unauthorized free or discount service.

Frontier's operations must be appropriately secured from sabotage and espionage to protect our customers and each other. This includes customer and employee personal information, network operations and facilities, computer systems and passwords, security procedures, company facilities and their locations, technical and marketing research data, product development information and business plans and strategies. You must take all appropriate precautions to protect Frontier's systems and premises. Do not leave visitors unescorted or sensitive areas unattended or unlocked. When on Frontier property (or, if appropriate, while on Frontier business) wear your identification badge and request identification from others whom you do not recognize. Most importantly, you must report all suspicious activity to Frontier's Security Department immediately.

Frontier's, third parties' and customers' confidential information must be kept secure. Physically or electronically stored confidential information must be protected by security measures appropriate to the type of information. Employees must not take confidential information away from Frontier premises unless required by business needs, and these circumstances should be minimized. All Frontier computers and other data storage devices such as Blackberrys should be password protected. Where appropriate the information should be encrypted. Employees in possession of confidential information must avoid situations where loss or theft of the information is likely.

Employees must ensure that business providers, such as contractors and vendors, make appropriate arrangements to protect confidential information. If you are aware of or even suspect an improper disclosure of confidential information or a breach of customer privacy — including a loss of customers' personal identifying information — you must report the situation immediately. See "Reporting of Loss, Theft or Improper Access to or Disclosure of Confidential Information" below.

Employees must not make any personal recordings (audio or video) or transmit data by recorder, camera, cellular telephone or otherwise, of any meeting, conference or individual discussion without the knowledge and consent of all other participants in such meeting, conference or discussion, except with prior approval from Frontier's Security or Legal Department. Frontier may record any employee conversations conducted over Frontier's corporate telephone equipment or service. Prior approval has been granted for the Frontier's recording of certain Call Center and telemarketing calls with notice to the customers. Questions regarding approval for recording should be directed to the employee's supervisor or to Frontier's Legal Department.

Unless you have obtained prior approval from Frontier's Security or Legal Department, or are authorized as part of carrying out your managerial responsibilities to do so, you may not access another employee's systems, records or equipment without that employee's knowledge and approval.

Employees must not access or attempt to access confidential information for any purpose other than a valid Frontier business purpose, and must not attempt to access confidential information that they have not been authorized to access. Questions regarding what information an employee is authorized to access should be directed to the employee's

supervisor. Questions regarding physical security should be directed to Frontier's Security Department. Questions regarding electronic security should be directed to Frontier's Information Services Department.

As noted in the Frontier Customer Operations Reference Guide, employees may not make any adjustment to their own Frontier service account. Any adjustment made to the account of an employee's family member, friend, or another Frontier employee must be approved by a supervisor.

IV. Subpoenas, Court Orders and Classified or National Security Information.

Frontier may receive subpoenas or court orders seeking information about its customers. You may neither confirm nor deny to any unauthorized person the existence of, or any information concerning, a subpoena, warrant or court order. You should immediately refer to Frontier's Security or Legal Department any documents, inquiries or requests of this kind.

The U.S. Espionage Act and other regulations govern our work with U.S. classified and national security information and impose stringent penalties for misuse or unauthorized disclosure of this information. You must take all necessary steps to protect classified and national security information and you must coordinate all activities related to this information with Frontier's Security Department personnel who have appropriate clearance. It is never appropriate to disclose this information to another person without explicit approval from Frontier's Security Department.

V. Information Provided to the Company Over the Internet.

Frontier's Privacy Policy with respect to information provided to Frontier over the Internet is available at http://www.frontier.com/policies/privacy/. A current copy of this policy is attached hereto, and employees must comply with it. CPNI provided to Frontier over the Internet is also subject to Frontier's policy on CPNI, attached hereto.

VI. Reporting of Loss, Theft, or Improper Access to or Disclosure of Confidential Information.

Any employee believing that confidential information has been lost, stolen, or improperly accessed or disclosed, or who has a good faith concern that such a loss, theft, access or disclosure may have taken place, must immediately report all relevant facts in one or more of the following ways: (1) to his or her supervisor; (2) to Frontier's Legal Department; (3) to Frontier's Security Department; or (4) through Frontier's Ethics Hotline (877-773-8325). It is Frontier's policy not to allow retaliation for reports of misconduct by others that are made by employees in good faith. Supervisors receiving such reports will forward them to Frontier's Legal and Security Department.

Under the FCC's rules, customers impacted by a CPNI security breach cannot be notified of the security breach involving customer information for least seven days after law

enforcement notification. There are limited exceptions that may allow customer notification in certain circumstances before the expiration of the seven-day period. Before a customer is notified of any security breach involving CPNI, please contact Frontier's Legal Department.

VII. Process to Respond to Reports of Suspected Loss, Theft or Improper Access to or Disclosure of Confidential Information.

Any report involving physical security will be directed to Frontier's Director – Environmental, Safety and Security. Any report involving electronic security will be directed to Frontier's Chief Information Officer. Any report involving suspected employee misconduct will be directed to Frontier's Executive Vice President – Human Resources. All reports will also be provided to Frontier's General Counsel and to Frontier's Vice President – Internal Audit. These individuals may designate others in their departments to receive reports. The investigation will be led by Frontier's Human Resources, Security, or Information Services Department depending on the nature of the reported issue, with advice from Frontier's Legal Department. In circumstances identified by Frontier's General Counsel where it is appropriate to maintain attorney-client or attorney work product privilege, the investigation will be led by an attorney in Frontier's Legal Department or by outside counsel. Employees are required to cooperate in internal investigations.

Frontier's Legal Department will determine whether external reporting of the incident is required. Frontier's Security and Legal Department will determine whether law enforcement agencies should be notified. If it appears likely that the incident will receive public attention, Frontier's Corporate Communications Office will be notified and will develop appropriate responses and talking points in consultation with the other involved departments. If it appears likely that the incident will involve questions from or filings with Frontier's regulatory agencies, Frontier's Regulatory Department will be notified and will develop appropriate responses and filings in consultation with the other involved departments.

Any material risk to Frontier identified by the investigation will be reported to Frontier's Senior Leadership Team. If the investigation leads to a conclusion that a process change is appropriate, the change will be reviewed with Frontier's Senior Leadership and then reviewed with and implemented by the affected departments, in consultation with Frontier's Internal Audit Department.

VIII. Violations.

Violations of this Policy will result in disciplinary action up to and including termination of employment with Frontier.