Chazy Westport Communications
Westelcom Networks Inc.
Teo Communications Inc.

Data Management and GLBA Policy

A. Overview

The Gramm-Leach-Bliley Act, (GLBA) effective May 23, 2003, addresses the safeguarding and confidentiality of customer information. GLBA and other emerging legislation could result in standards of care for information security across all areas of data management practices both electronic and physical. Therefore, Chazy Westport Communications, Westelcom Networks Inc. and Teo Communications Inc. has adopted this Data Management and GLBA Policy for certain highly critical and private financial and related information. This policy applies to customer financial information (covered data) that Chazy Westport Communications, Westelcom Networks Inc. and Teo Communications Inc. receives in the course of business as required by GLBA.

B. Purpose

In order to continue to protect private information and data and to comply with the provisions of the Federal Trade Commission's safeguard rules implementing applicable provisions of the Gramm-Leach-Bliley Act (GLBA), Chazy Westport Communications, Westelcom Networks Inc. and Teo Communications Inc. has adopted this Data Management and GLBA Policy for certain highly critical and private financial and related information. This policy applies to customer financial information (covered data) that Chazy Westport Communications, Westelcom Networks Inc. and Teo Communications Inc. receives in the course of business as required by GLBA. This policy describes many of the activities that Chazy Westport Communications, Westelcom Networks Inc. and Teo Communications Inc. currently undertakes, and will undertake, to maintain covered data according to legal requirements. This Data Management and GLBA Policy is designed to provide an outline of the safeguards that apply to this information, specifically in compliance with GLBA.

C. Definitions

Customer - means any individual who receives a service from Chazy Westport Communications, Westelcom Networks Inc and/or Teo Communications Inc.

Non-public personal information - means any personally identifiable financial or other personal information, not otherwise publicly available, that Chazy Westport Communications, Westelcom Networks Inc and/or Teo Communications Inc. has obtained from a customer in the process of offering a service. Examples of personally identifiable financial information include names, addresses, telephone numbers, bank and credit card account numbers, income and credit histories, tax returns, asset statements, and social security numbers, both in paper and electronic form.

Covered data and information - for the purpose of this Policy, includes non-public personal information of customers required to be protected under GLBA. In addition to this required coverage, Chazy Westport Communications, Westelcom Networks Inc. and Teo Communications Inc. chooses as a matter of policy to also define covered data and information to include any bank and credit card account

numbers, income and credit information, and social security numbers received in the course of business. Covered data and information includes both paper and electronic records.

D. Security Program Components

The GLBA requires that Chazy Westport Communications, Westelcom Networks Inc. and Teo Communications Inc. develop, implement, and maintain a comprehensive information security program containing the administrative, technical, and physical safeguards that are appropriate based upon the size, complexity, and the nature of its activities. This Information Security Program has five components:

1. Designating an employee or office responsible for coordinating the program;
2. Conducting risk assessments to identify reasonably foreseeable security and privacy risks;
3. Ensuring that safeguards are employed to control the risks identified and that the effectiveness of these safeguards is regularly tested and monitored;
4. Overseeing service providers;
5. Maintaining and adjusting this Information Security Program based upon the results of testing and monitoring conducted as well as changes in operations or operating systems.

E. Information Security Officer

The Chazy Westport Communications, Westelcom Networks Inc. and Teo Communications Inc. 's Information Security Officer will be responsible for implementing the Information Security Program. The Information Security Officer shall be appointed by the President and work closely with other offices and units that may have interface with or have control over covered data.

The Information Security Officer will ensure that risk assessments and monitoring are carried out for each area that has covered data and that appropriate controls are in place for the identified risks.

The Information Security Officer will work with responsible parties to ensure adequate training and education is developed and delivered for all employees with access to covered data. The Information Security Officer will, in consultation with other offices, verify that existing policies, standards and guidelines that provide for the security of covered data are reviewed and adequate. The Information Security Officer will make recommendations for revisions to policy, or the development of new policy, as appropriate.

The Information Security Officer will update this Information Security Program, including this and related documents, from time to time. The Information Security Officer will maintain a written security plan and make the plan available to all employees and business entities as required by GLBA.

F. Risk Assessment

The Information Security Program will identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of covered data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information and assess the sufficiency of any safeguards in place to control these risks. The Information Security Officer will work with all relevant

areas to carry out comprehensive risk assessments. Risk assessments will include system-wide risks as well as risks unique to each area with covered data.

G. Information Safeguards and Monitoring

The Information Security Program will verify that information safeguards are designed and implemented to control the risks identified in the risk assessments set forth above. The Information Security Officer will ensure that reasonable safeguards and monitoring are implemented and cover each unit that has access to covered data. Such safeguards and monitoring will include the following:

1. Employee Management and Training

Safeguards for security will include management and training of those individuals with authorized access to covered data. Chazy Westport Communications, Westelcom Networks Inc. and Teo Communications Inc. has adopted (or will adopt) comprehensive policies, standards and guidelines setting forth the procedures and recommendations for preserving the security of private information, including covered data.

The Information Security Officer will, working with other responsible offices, identify categories of employees or others who have access to covered data.

2. Information Systems

Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal. Network and software systems will be reasonably designed to limit the risk of unauthorized access to covered data. This may include designing limitations to access, and maintaining appropriate screening programs to detect computer hackers and viruses and implementing security patches.

3. Managing System Failures

Chazy Westport Communications, Westelcom Networks Inc. and Teo Communications Inc. will maintain effective systems to prevent, detect, and respond to attacks, intrusions and other system failures.

4. Monitoring and Testing

Monitoring systems will be implemented to regularly test and monitor the effectiveness of information security safeguards.

H. Service Providers

In the course of business, Chazy Westport Communications, Westelcom Networks Inc. and Teo Communications Inc. may from time to time appropriately share covered data with third parties. Such activities may include collection activities, transmission of documents, transfer of funds, destruction of documents or equipment, or other similar services. This Information Security Program will ensure that reasonable steps are taken to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and requiring service providers by contract

to implement and maintain such safeguards. The Information Security Officer, by survey or other reasonable means, will identify service providers who are provided access to covered data. The Information Security Officer will make certain that service provider contracts contain appropriate terms to protect the security of covered data.

I. Program Maintenance

The Information Security Officer, will evaluate and adjust the Information Security Program in light of the results of testing and monitoring described in Section G, as well as, in response to any material changes to operations or business arrangements and any other circumstances, which may reasonably have an impact on the Information Security Program.

J. Roles and Responsibilities

1. Directors, Department Heads and other Managers

The department head, director or other manager responsible for managing employees with access to covered data will designate a responsible contact to work with the Information Security Officer to assist in implementing this program. The designated contact will ensure that risk assessments are carried out for that unit and that monitoring based upon those risks takes place. The designated responsible contact will report the status of the Information Security Program for covered data accessible in that unit to the Security Program Officer.

2. Employees with Access to Covered Data

Employees with access to covered data must abide by Chazy Westport Communications, Westelcom Networks Inc. and Teo Communications Inc. policies and procedures governing covered data as well as any additional practices or procedures established by their immediate supervisor.

3. Information Security Program Officer

The Chazy Westport Communications, Westelcom Networks Inc. and Teo Communications Inc. Information Security Officer will designate individuals who have the responsibility and authority for information technology resources, establish and disseminate enforceable rules regarding access to and acceptable use of information technology resources, establish reasonable security policies and measures to protect data and systems, monitor and manage system resource usage, investigate problems and alleged violations of Chazy Westport Communications and Westelcom Networks Inc. information technology policies and procedures, and refer violations to appropriate management.