**GEORGIA HIGHSPEED COUNTRY INTERNET, LLC**

**COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM (CWISP)**

I. OBJECTIVE:

Our objective, in the development and implementation of this comprehensive written information security program (“CWISP”), is to create effective administrative, technical and physical safeguards for the protection of personal information. The CWISP sets forth our procedure protecting personal information of customers of Georgia Highspeed Country Internet, LLC. For purposes or evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, an of this CWISP, “personal information” means a customer’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such customer: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident’s financial account; provided, however, that “personal information” shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

It is also our objective to utilize this CWISP to ensure FCC compliance with safeguarding the Customer Proprietary Network Information (“CPNI”) we may have access to as an Broadband Internet Access Service Provider (BIAS). Specific CPNI protection procedures include, but are not limited to: Enabling strict controls regulating the use and access to CPNI; notifying customers about access to CPNI; training employees about safeguarding CPNI; protecting CPNI used in sales and marketing campaigns; notifying the FCC and law enforcement agencies of unauthorized CPNI access; establishing “opt-in/ opt-out” procedures for the use of CPNI by third parties.

II. PURPOSE:

The purpose of the CWISP is to:

(a) Ensure the security and confidentiality of personal and CPNI information;

(b) Protect against any anticipated threats or hazards to the security or integrity of such information;

(c) Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE:

In formulating and implementing the CWISP, (1) identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information; (3) evaluate the sufficiency of existing policies, procedures, and other safeguards in place to control risks; (4) design and implement a CWISP that puts safeguards in place to minimize those risks; and (5) periodically monitor the effectiveness of those safeguards:

IV. Information Security:

We have designated Zach Boulton as supervisor of the following:

a. Initial implementation of the CWISP;

b. Training employees;

c. Requiring each of our third party service providers to implement and maintain appropriate security measures for the personal and CPNI information to which we have permitted them access, consistent; and requiring such third party service providers to implement and maintain appropriate security measures;

d. Reviewing the scope of the security measures in the CWISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information;

e. Providing annual training material for all owners, managers, employees and independent contractors, including temporary and contract employees who have access to personal and CPNI information on the elements of the CWISP.

V. INTERNAL RISKS:

Internal Threats

1. A copy of the CWISP must be distributed to each employee.
2. Mandatory disciplinary action to be taken for violation of security provisions of the CWISP (The nature of the disciplinary measures may depend on a number of factors including the nature of the violation and the nature of the personal and CPNI information affected by the violation).
3. The amount of personal and CPNI information collected should be limited to that amount reasonably necessary to accomplish our legitimate business purposes, or necessary to us to comply with other state or federal regulations.
4. Access to records containing personal and CPNI information shall be limited to those persons who are reasonably required to know such information in order to accomplish our legitimate business purpose or to enable us to comply with other state or federal regulations.
5. All security measures shall be reviewed at least annually, or whenever there is a material change in our business practices that may reasonably implicate the security or integrity of records containing personal and CPNI information. The Information security Manager shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review.
6. Terminated employees must return all records containing personal and CPNI information, in any form, that may at the time of such termination be in the former employee’s possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.)
7. A terminated employee’s physical and electronic access to personal information must be immediately blocked. Such terminated employee shall be required to surrender all keys, IDs or access codes or badges, business cards, and the like, that permit access to the firm’s premises or information. Moreover, such terminated employee’s remote electronic access to personal information must be disabled; his/her voicemail access, e-mail access, internet access, and passwords must be invalidated.
8. Current employees’ passwords must be changed periodically.
9. Access to personal and CPNI information shall be restricted to active users and active user accounts only.
10. Employees are encouraged to report any suspicious or unauthorized use of customer information.
11. Whenever there is an incident that requires notification there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of personal information for which we are responsible.
12. Employees are prohibited from keeping open files containing personal information on their desks when they are not at their desks.
13. At the end of the work day, all files and other records containing personal and CPNI information must be secured in a manner that is consistent with the CWISP’s rules for protecting the security of personal information.
14. Physical records and data will be stored in locked facilities, secure storage areas or locked containers. Access will be granted to authorized personnel only. Authorized personnel should routinely assess physical records to determine if such records can be disposed of.
15. Access to electronically stored personal information shall be electronically limited to authorized personnel, having a unique log-in ID.
16. Visitors’ access must be restricted to one entry point for each building in which personal information is stored. Visitors shall not be permitted to visit unescorted any area within our premises that contains personal information.
17. Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information shall be disposed of only in a manner that complies.
    1. Georgia Highspeed Country Internet, LLC, does not collect any of the following information: Social Security Number, Drivers License or state issued identification card number, financial account number, credit card number or debit card number with or without required security code, access code, personal identification number or password, that would permit access to a residents financial account.

VI. EXTERNAL RISKS

External Threats

There must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, installed on all systems processing personal information.

1. There must be reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing personal information.
2. To the extent technically feasible, all records and files containing P.I. must be encrypted before being transmitted across public networks or wirelessly. Encryption here means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Office of Consumer Affairs and Business Regulation.
3. There must be secure user authentication protocols in place, including:(1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices; (3) control of data security passwords to ensure that such passwords are kept in a secure location.
   1. Georgia Highspeed Country Internet, LLC, does not collect any of the following information: Social Security Number, Drivers License or state issued identification card number, financial account number, credit card number or debit card number with or without required security code, access code, personal identification number or password, that would permit access to a residents financial account. Therefore, there is no concern of submission of this information or external risks.

**Security threat mitigation policy and procedures**

Computer resources

1. Servers, firewalls, web-filter, anti-spam, anti-virus, phone system, and core infrastructure assets are secured in a locked room with physical access granted to “authorized personnel only”.
2. Management of Servers, firewalls, web-filter, anti-spam, anti-virus, phone system, and core infrastructure assets are restricted to personnel on a hierarchical basis as required.
3. Servers, firewalls, web-filter, anti-spam, anti-virus, phone system, and core infrastructure assets are patched and updated on a regular basis.
4. Desktops and portable devices are configured to accept automatic updates.

External Firewall

1. Company maintains firewall(s) to protect against unauthorized entry into the internal network from WAN access points.
2. Access to firewall configuration is limited to “authorized personnel only”.
3. User level security and auditing of same is limited. Current configuration is one to many.
4. Firewall has security audit capabilities of attacks, providing a base level of threat detection and prevention.

Wi-Fi Security

1. WPA/WPA2 with TKIP/AES
2. Shared secret reset upon termination of employment
3. Restrict to MAC Authorized access list

P.I. and CPNI Security

1. Hard copy containing P.I. and CPNI information is either stored in a locked container/office or scanned to network on a contemporaneous basis and then physical copy is promptly shredded. In no case should P.I. and CPNI be left unattended, including breaks, lunch, and overnight. Physical records containing P.I. may not be removed from premises unless required for lawful or business related purposes.
2. Scanned P.I. and CPNI to be stored on network share with access granted on a hierarchical basis as required.
3. No P.I. and CPNI data is to be copied from network shares to any portable device.

Network Login

1. Passwords must have a minimum of 7 characters and contain alpha, numeric and special characters.
2. Passwords shall be reset upon notification of compromise, and/or any time it is deemed appropriate to maintain the integrity of “password privacy”.
3. Notification of Terminated personnel shall be submitted to I.T. and H.R. immediately upon termination. Terminated personnel’s account(s) shall be deleted unless further access is required in which case account(s) password(s) shall be reset and account(s) disabled.

Remote Access VPN

1. Granted on an as needed basis
2. Secured by PPTP, SSL or IPSec Tunnels
3. Any device accessing corporate network must be running client level anti-virus software with up to date signatures.
4. Any device accessing corporate network must be running client level anti-spyware software with up to date signatures.
5. Any device connecting to corporate network must maintain an engaged firewall that adheres to corporate configuration standards.
6. It is a violation of corporate security policy for PI and/or CPNI data or for any document containing P.I. and/or CPNI data to be copied from the corporate network to any portable device.

Remote Access Web Portals

1. Granted on an as needed basis
2. Communications to be secured by an SSL certificate, self-issued, Internal CA, or Public CA.
3. Documents containing P.I. and CPNI may be viewed only. Corporate policy expressly prohibits the manual recording, screen capturing, or downloading of any P.I. related information to off network device(s).

Document uploading to network

1. No files should be loaded directly onto network by end user using removable media, including but not limited to floppy, CD, DVD, Blu-Ray, Flash, and Portable HDD.
2. Files that need to be uploaded should be sent thru email system, and processed thru Anti-Virus system.

Printed material containing P.I. and CPNI must be promptly removed from all unsecured devices. In no case should material be left on unsecured devices overnight.

Preferred format for all material is secured electronic. Where possible third party service providers and customers are encouraged to transmit records containing P.I. CPNI in an electronic portable document format, via secure transmission methods. Facsimiles containing P.I. and CPNI should be sent to secured devices only.