Security Requirements II
Goods Security Provision

This Security Requirements II Attachment is governed by, and made a part of, the Master Purchase Agreement dated August 23, 2019 between Charter Communications Operating, LLC ("**Charter**") and Ciena Communications, Inc. ("**Supplier**" or "Vendor"), as may be amended from time to time pursuant to its terms (collectively, the "**Master Agreement**"). Capitalized terms used and not defined herein shall have the meanings ascribed to such terms in the Master Agreement.

Security Requirements

1. Supplier will, consistent with current leading industry accepted standards and practices, undertake and maintain physical, administrative, and technical safeguards and other security measures necessary to ensure the security and confidentiality of (i) Charter's Confidential Information, (ii) Supplier supplied assets, systems and software of its network utilized in performance of this Agreement ("Assets, Systems, and Software" or "Network") and (iii) Charter's network and equipment. These measures will include, but are not limited to, the following requirements:

a. Supplier will update any third party assets, systems and software included in or used in conjunction with Supplier's operating systems/platform, network or related hardware/software ("Third Party Element(s)") that are utilized to render any Services or provide any capitalized deliverable, under this Agreement, to the current or to the prior major release of such Third Party Element, unless otherwise agreed in writing between the parties. Supplier shall not use a version of any such Third Party Elements for which support is no longer available from any entity or for which code fixes addressing vulnerabilities are no longer developed.

b. Supplier shall ensure that all Supplier supplied Assets, Systems and Software are protected from known, discovered, documented, and/or reported vulnerabilities to at least critical and high external threats to functionalities or security by installing applicable and necessary security patches within a reasonable timeframe. As a baseline for reasonableness, after the vulnerability is confirmed and a solution has been identified, Supplier must provide to the Network critical security patches immediately (or at least 10 days), high security patches within 1 month of release, medium security patches within a reasonable number of days, and low security patches within the same. Supplier shall not be responsible for delays caused by third parties. Security patch severity will be categorized using the Common Vulnerability Scoring System.

c. Supplier must test the security of its Assets, Systems and Software used in connection with this Agreement as frequently as necessary to confirm that system integrity and security are consistent with current leading industry accepted standards and practices. Supplier is responsible for and shall conduct penetration testing of its own products, assets, systems and software to identify and remediate vulnerabilities in its own environment based on current leading industry accepted penetration testing approaches, and to communicate to Charter a page from the testing report evidencing such testing. Supplier shall:

i) Conduct the penetration testing using appropriately qualified assessors.

ii) Perform penetration testing based on current leading industry accepted penetration testing approaches (for example, NIST SP800-115) at least annually and also after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a major release of the application).

iii) Correct exploitable at least critical vulnerabilities, triaging on those with known malware and/or exploits discovered during penetration testing and then others as reasonably practicable, with follow up testing to verify the effectiveness of the corrections. For any vulnerabilities for which the corrections were not effective, Supplier shall undertake additional measures to correct the vulnerabilities and restart this verification and testing cycle (this step to be repeated until effective corrections are implemented).

2. For any software development processes related to this Agreement, Supplier must address common coding vulnerabilities as follows:

Vendor will, consistent with current leading industry accepted standards and practices, undertake and maintain physical, administrative, and technical safeguards and other security measures necessary to ensure the security and confidentiality of (i) Charter's Confidential Information, (ii) Vendor supplied assets, systems and software and (iii) Charter's network and equipment. These measures will include, but are not limited to, the following requirements:

a At time of delivery, Vendor shall ensure that all products supplied in this agreement are protected, as reasonably determined by Vendor, from known, discovered, documented, and/or reported vulnerabilities to external threats to functionalities or security. Additionally, Vendor shall provide applicable and necessary security patches, new release(s), or other remediation within a reasonable timeframe. As a baseline for reasonableness, Vendor must provide a notification to Customer as described in Section 2.b.iii below. Security vulnerability severity will be categorized using the Common Vulnerability Scoring System and the timeframes begin upon the earlier to occur of (i) the date Charter notifies Vendor at www.ciena.com/support/ or 800-CIENA24 (243-6224) of a vulnerability, or (ii) the date Vendor otherwise becomes aware of the vulnerability.

b. Vendor must test the security of its Products with Embedded Software supplied with this Agreement ("Product(s)") as frequently as it reasonably considers necessary to confirm that system integrity and security are consistent with current industry best tier of standards and practices. Vendor should test the security using representative or adequate infrastructure as it recommends to support the Products being supplied with this agreement. Vendor is responsible for and shall conduct penetration testing of its Products to identify and remediate vulnerabilities in its own environment based on industry-accepted penetration testing approaches. Vendor shall:

   i. Conduct the penetration testing using appropriately qualified assessors.

   ii. Perform penetration testing based on industry-accepted penetration testing approaches (for example, NIST SP800-115) at least upon request (which may be up to annually) and also prior to any significant Product releases.

   iii. Assess the penetration test results to determine risk level, its recommended remediation, and the likelihood that similar vulnerabilities are present in Charter's deployment of the Vendor's Product. Recommended remediation may include but is not limited to the creation of security patches and should not materially impair the functionality of the Product. If through assessment it is likely that Charter's deployment of the Product is vulnerable and without limiting the requirements in Section 1 above, the vendor will 1) notify Charter with vulnerability summary and recommended remediation plan within 20 business days of Vendor discovery of vulnerability, and 2) for critical vulnerabilities use good faith efforts to release a patch, dot release, or mitigation within a reasonable time (e.g. 10 days after a solution has been identified for most critical vulnerabilities when such remediation timing is within Supplier's policy).

c. For any Products provided under this Agreement, Vendor must address common coding vulnerabilities as follows:

   i. Use secure coding guidelines and latest industry best practices for vulnerability management, such as the Open Web Application Security Project (OWASP) Guide, and CERT Secure Coding.

   ii. Make training available for developers, for at least annually in up-to-date secure coding techniques, including, but not limited to, how to avoid common coding vulnerabilities.

d. For any third party assets, systems, hardware, and software (Third Party Elements), used or embedded in the products being supplied with this agreement, Vendor will ensure that these Third Party Elements are the latest or reasonably secure major version available and supported by the third party where reasonably available, or if not so, Supplier will apply its vulnerability management process (such as remediation and/or mitigation) to account for risks to such third party software components. Vendor shall not use a version of any such Third Party Elements for which support is no longer available from any entity (including, without limitation, for which code fixes addressing vulnerabilities are no longer developed), except as specified above, or except as mutually agreed in writing.

e Vendor warrants that any Vendor subcontractor engaged in the performance of Vendor obligations or activities for development of software relevant for security, on behalf of Vendor, under this Agreement, will adhere to and abide by security requirements that meet or exceed the security requirements found in this Section. Additionally, upon request, Vendor shall certify that all such subcontractors are adhering to or complying with security requirements that meet or exceed the security requirements found in this Section.

f Charter reserves the right to audit Vendor to the extent specified in the Agreement, to evaluate the Vendor's security program as it relates to the requirements found in this Section, including policies, processes, and internal controls. This may include, where applicable, determining whether the Vendor's or third party subcontractor's internal audit

function operates independently, effectively tests and reports on the internal security controls, and evaluates security processes for escalating, remediating, and holding management accountable for resolutions of concerns identified during audits or other independent tests and mutually agreed in writing.

g Vendor shall ensure all applicable workforce who will perform functions subject to these security requirements, will have access to appropriate training on the applicable security practices.

Charter Communications Access Agreement

THIS ACCESS AGREEMENT (this "Agreement") is entered into as of the Effective Date listed below (the "Effective Date"), between Charter Communications Operating, LLC, a Delaware limited liability company, with a principal place of business at 12405 Powerscourt Drive, St. Louis, Missouri 63131 ("Charter"), and the Accessing Party listed below, its parent, subsidiaries and affiliates ("Accessing Party").

COMPLETE ALL FIELDS | PLEASE WRITE LEGIBLY

Effective Date:	August 28th, 2017
Accessing Party: Full Legal Name (e.g., ACME Products Company, LLC.) and Primary Mailing Address	Ciena Communications, Inc. 7035 Ridge Road Hanover, MD 21076
Charter Sponsor: Name, Department, Phone Number and Email Address	
Accessing Party Primary Contact: Name, Address, Phone Number, Email Address	Keith Principe 5445 DTC Parkway, Suite 900 Greenwood Village, CO 80111 3032827979 kprincip@ciena.com
Accessing Individuals	As specified in **Exhibit A**, as amended, hereby incorporated by reference
Terms & Conditions	As specified in **Exhibit B**, hereby incorporated by reference
Acceptable Use of Technology Policy	As specified in **Exhibit C**, hereby incorporated by reference

This Agreement is approved and accepted as of the Effective Date.

ACCESSING PARTY

By: Erik J. Lichter 8/28/2017

Name:

Title: Vice President & Deputy General Counsel

CHARTER COMMUNICATIONS OPERATING, LLC
By: Charter Communications, Inc., its Manager

By: Steve Nocella
Steve Nocella (Oct 13, 2017)

Name: Steve Nocella

Title: Vice President (or higher)

EXHIBIT A

ACCESSING PARTY USERS LISTS

CHARTER SPONSOR AND ACCESSING PARTY: RETAIN COPY IN YOUR RECORDS.
CHARTER SPONSOR: USE BELOW INFO WHEN COMPLETING IT REMEDY TICKET.

Please provide the following information for each individual user from/with Accessing Party that will need access to the Charter Network. For additional Users please insert additional copies of this page. Sign, date and label each page.

Accessing Party: _____ (signature)

Date: _____

Sheet: ___ of ___

COMPLETE ALL FIELDS | PLEASE WRITE LEGIBLY

First & Last Name:	**Pin Code** (self selected 4-digit Pin)	**Contact Info**: (phone number and email address)	**Access Needed**: (**BE SPECIFIC**, Need to know specific applications, tools, drives, servers, etc.)
EXAMPLE John Doe	***EXAMPLE*** 1776	***EXAMPLE*** 314-555-1212 john.doe@company.com	***EXAMPLE*** Charter Tools, Up To Speed, COIN and Charter Email Address

FAILURE TO PROVIDE REQUESTED INFORMATION COULD DELAY ACCESS

For additional Users please insert additional copies of this form.

EXHIBIT B

GENERAL TERMS AND CONDITIONS

The Parties hereby agree as follows:

1. Grant of Access

Charter grants access to and use of the certain Charter and Charter affiliate networks, computer systems, applications, software and/or data (the "Network") set forth on **Exhibit A** to this Agreement, as amended from time to time, and which is hereby incorporated by reference. The Accessing Party shall not attempt to access or use any Charter or Charter affiliate networks, computer systems software and/or data other than those expressly authorized by Charter.

2. Scope

This grant of access applies only to the Accessing Party's employees, contractors, vendors and agents specifically designated by the Accessing Party (each a "User"). Before allowing a User to access the Network, the Accessing Party shall cause such User to (i) review this agreement and verify in writing that the User has done so and (ii) review and comply with Charter's Acceptable Use of Technology Policy, attached hereto as **Exhibit C** and hereby incorporated by reference. The Accessing Party shall be liable for the actions or omissions of Users in using the Network. Users will use the Network only for legitimate business purposes in furtherance of the Accessing Party's defined business relationship with Charter or its affiliates and for no other purpose. Users' access to the Network, as well as utilization of access codes, passwords and access procedures, may be denied, changed or terminated, at any time, at the sole discretion of Charter, without cause or liability to the Accessing Party or Users.

3. Terms of Use

a. The Accessing Party agrees to follow the then-current Charter Acceptable Use of Technology Policy as applicable, the current version of which is attached hereto as **Exhibit C** and incorporated herein by reference, as well as all other applicable Charter information security policies, standards or procedures that Charter has provided to Accessing Party, and to prevent improper access to the Network or applications on the Network by Users. Charter reserves the right to revise its Acceptable Use Policy, Password Policy and its other information security policies, standards or procedures at any time, at which time Charter will provide such revised policies to Accessing Party.

b. Charter has the right to strictly control access to the Network to ensure security of its data.

c. It is the responsibility of the Accesing Party to ensure that all its Users with virtual private network ("VPN") privileges do not enable access to the Network by unauthorized users.

4. Term

This Agreement will commence on the Effective Date and continue until terminated by either party hereto, at any time, without cause, five (5) days after receipt of written notice thereof, or as otherwise provided in this Agreement. Accessing Party's failure to comply with any of the provisions of this Agreement is a material breach of this Agreement. In such event, Charter may terminate the Agreement effective immediately upon written notice to the Accessing Party without prejudice to its rights or remedies available at law or in equity or further liability or obligation to Charter. Upon termination or expiration of this Agreement, the Accessing Party will cease and will ensure that Users will cease all attempts to access the Network. Termination or expiration of this Agreement will not relieve the Accessing Party of its obligation to hold Confidential Information (defined below) confidential.

5. Confidentiality

a. Generally.

1. In connection with this Agreement, Accessing Party may receive or have access to certain non-public information that is marked or otherwise specifically identified or which by its contents and the underlying circumstances, a reasonable person would consider proprietary or confidential ("Confidential Information"). In addition, Accessing Party acknowledges that it and its personnel may have access to data, records and documents pertaining to such Confidential Information. This Confidential Information may include, among other things, the personally identifiable information of current, former or prospective Charter customers or employees (also referred to as "Charter PII"), computer software, computer hardware, computer passwords, computer access information, computerized data, licenses, agreements, permits, specifications, designs, business plans, schematics, drawings, software, data, prototypes, or other business, marketing and/or technical information. For purposes of this Section, the party that discloses Confidential Information is

referred to as the "Charter" and the party that receives Confidential Information is referred to as the "Accessing Party". Notwithstanding anything to the contrary, any and all Charter PII shall at all times be considered to be "Confidential Information."

2. With respect to Confidential Information disclosed under this Agreement, the Accessing Party and its employees shall: (a) secure and hold the Confidential Information in confidence, exercising a degree of care not less than the care used by the Accessing Party to protect its own proprietary or confidential information that it does not wish to disclose (but in no event shall such care be less than that which is commercially reasonable), and specifically, the Accessing Party shall maintain and secure any Confidential Information in electronic data format using security measures that meet or exceed either the ISO/IEC 27002 information security controls standard or the NIST 800-53 framework; (b) restrict disclosure of the Confidential Information solely to those of its employees to whom further disclosure is necessary for Accessing Party to perform its obligations under this Agreement, and not disclose the Confidential Information to any other person or entity without the prior written consent of the Charter which shall not be unreasonably withheld; (c) secure in writing the agreement of such employees to keep Confidential Information confidential in accordance herewith; (d) use the Confidential Information only in connection with the performance of this Agreement, except as Charter may otherwise agree in writing; and (e) segregate all such Confidential Information from the confidential materials and information of Accessing Party or others to prevent commingling.

3. Confidential Information shall be deemed the property of Charter during the term of this Agreement and afterwards in perpetuity, subject only to the exceptions expressly stated herein. Upon written request of Charter, the Accessing Party shall return all Confidential Information received in tangible form, except that each party's legal counsel may retain one copy for its files solely to provide a record of such Confidential Information for archival purposes.

4. Each party will keep this Agreement and its terms confidential and will make no press release or public disclosure, either written or oral, regarding the transactions contemplated by this Agreement without the prior consent of the other party hereto, which consent will not be unreasonably withheld; provided that the foregoing will not prohibit any disclosure that is required by law or the rules of any stock exchange or other entity where a party's securities are traded.

5. Except to the extent of Charter PII for which the confidentiality obligations shall remain intact unless otherwise required by court order, the Accessing Party shall have no obligation to preserve the proprietary nature of Confidential Information that (a) was previously known to the Accessing Party free of any obligation to keep it confidential; (b) is or becomes publicly available by means other than unauthorized or illegal disclosure; (c) is developed by or on behalf of the Accessing Party independently of any Confidential Information furnished under this Agreement; or (d) is received from a third party whose disclosure does not violate any confidentiality obligation.

6. If the Accessing Party is required to disclose Charter's Confidential Information by an order or a lawful process of a court or governmental body, the Accessing Party shall, if legally permitted, promptly notify Charter, and shall cooperate with Charter in seeking reasonable protective arrangements before the Confidential Information is produced.

7. Each party agrees that a breach of any of the terms of this "Confidentiality" Section by the Accessing Party or its representatives will result in irreparable harm for which there is no adequate remedy at law, and in the event of any such breach Charter may seek a preliminary or permanent injunction and/or specific performance which shall be granted upon a finding of a breach (or substantial likelihood of a breach in the case of a preliminary injunction). Such remedies shall not be deemed to be the exclusive remedies for a breach of the terms of this "Confidentiality" Section, but shall be in addition to all other remedies available at law or in equity.

8. Upon reasonable request from Charter, Accessing Party shall provide access to, and the right to inspect, all records relating to (i) the collection, processing, or transfers of data relating to Charter's Confidential Information and (ii) the information security measures used by Accessing Party to secure Confidential Information. Unless otherwise agreed, any such inspection shall occur only at the business offices of Accessing Party during normal business hours and shall be conducted by a mutually acceptable third-party inspector. Accessing Party further agrees to cooperate in any regulatory investigation or in any internal investigation by Charter (and in responding to any inquiry relating to Charter PII). In the event of any such investigation or inquiry, upon notice to Accessing Party, Charter may suspend any further transfers of Confidential Information for so long as may be necessary to obtain assurances that any additional transfers will not provide the basis for further regulatory action or possible liabilities. Any such suspension will not relieve either party for any liability arising from this Agreement or any other commercial agreements with Charter.

10. The provisions set forth in this Section, shall survive the expiration or earlier termination of this Agreement.

b. ADDITIONAL REQUIREMENTS WITH RESPECT TO CHARTER PII.

1. All Charter PII (e.g. without limitation, names, addresses, telephone numbers, social security numbers, driver's license numbers, payment card/bank account information, etc.) will be maintained by Accessing Party as confidential and will not be used for any purpose other than the completion of these specific duties undertaken in this Agreement. Any collection, maintenance, and/or use of Charter PII by Accessing Party shall be undertaken (a) subject to the then current documented subscriber information collection business practices and written customer privacy policies of Charter (which practices and policies are described more fully at www.charter.com, and may be amended in Charter's sole discretion from time to time); (b) in all cases, in compliance with all applicable local, state and federal laws, rules and regulations governing Charter's collection, maintenance, transmission, dissemination, use and destruction of Charter PII, including, but not limited to, (i) the provisions of 47 U.S.C. § 551, *et seq.*, as if Accessing Party were deemed a "cable operator", (ii) any state and federal security breach notification laws, (iii) any state and federal law requiring the protection of personally identifiable information, and (iv) the rules, regulations and directives of the Federal Communications Commission and the Federal Trade Commission, as amended from time to time; and (c) in compliance with the Payment Card Industry Data Security Standards (PCI DSS), including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS at Accessing Party's sole cost and expense, to the extent the recipient has access to any system that contains Charter customer's payment card information.

2. Accessing Party acknowledges that Accessing Party is responsible for the security of any Charter customers' payment card information to which it has access (whether stored, transmitted, processed, or otherwise accessible or in its possession), including without limitation to the extent to which Accessing Party's acts or omissions could impact the security of such payment card information. Accessing Party shall maintain all information and records related to the specific PCI Standards requirements applicable to Accessing Party and its treatment of cardholder information and shall provide such information or records to Charter upon request.

3. Accessing Party shall retain all Charter PII only for so long as is reasonably necessary to complete the purposes for which the Charter PII has been disclosed to Accessing Party, unless otherwise specified by a mutual written agreement of the Parties. Thereafter, Accessing Party shall, at Charter's election, permanently destroy or return such information to Charter with a certification signed by an officer of Accessing Party that all such Charter PII has been destroyed or returned. Accessing Party shall comply with all reasonable directions provided by Charter with respect to the return or disposal of Charter PII.

4. Under no circumstances shall Accessing Party disclose Charter PII to any third party (even if under contract to that party) or to any personnel of the party responsible for publicity or for end-user sales or marketing.

c. Breach of Confidential Information

1. For the purposes of this Section a "Security Incident" is defined as any actual or reasonably suspected compromise, unauthorized use or disclosure of Confidential Information or Charter PII, or any other breach of this Section.

2. Accessing Party shall: (i) provide Charter with the name and contact information for an employee of Accessing Party who shall serve as the primary security contact and shall be available to assist Charter twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a Security Incident; (ii) notify Charter of a Security Incident as soon as practicable, but no later than twenty-four (24) hours after Accessing Party becomes aware of it; and (iii) notify Charter of any Security Incident by telephone at the following number at **1-866-894-0103** and written communication by e-mailing Charter with a read receipt at **dlsecurityincidents@charter.com** and with a copy by e-mail to Accessing Party's primary business contact within Charter.

3. Immediately following Accessing Party's notification to Charter of a Security Incident, the parties shall coordinate with each other to investigate the Security Incident. Accessing Party agrees to fully and reasonably cooperate with Charter in Charter's handling of the matter, including, without limitation: (i) assisting with any investigation; (ii) providing Charter with physical access to the facilities and operations affected; (iii) facilitating interviews with Accessing Party's employees and others involved in the matter; and (iv) making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise reasonably required by Charter.

4. Accessing Party shall take reasonable steps and use best efforts to immediately remedy any Security Incident and prevent any further Security Incidents at Accessing Party's expense in accordance with applicable privacy rights, laws, regulations and standards. Accessing Party shall reimburse Charter for actual reasonable costs incurred by Charter in responding to, and mitigating damages caused by, any Security Incident, including all costs of notice and/or remediation.

5. Accessing Party agrees that it shall not inform any third party of any Security Incident without first obtaining Charter's prior written consent, other than to inform a complainant that the matter has been forwarded to Charter's legal counsel. Further, Accessing Party agrees that Charter shall have the sole right to determine: (i) whether notice of the Security Incident is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others as required by law or regulation, or otherwise in Charter's discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation.

6. Accessing Party agrees to reasonably cooperate, at its own expense, with Charter in any litigation or other formal action deemed reasonably necessary by Charter to protect its rights relating to the use, disclosure, protection and maintenance of Charter PII.

6. Laws

In addition to the requirements of Section 5, the Accessing Party will abide by all applicable laws, statutes, rules, ordinances and regulations including U.S. export control laws and regulations. This Agreement will be governed by the laws of the State of Missouri without giving effect to its conflict of laws principles.

7. Warranties and Limitations of Liability

CHARTER MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, TITLE, OR AGAINST INFRINGEMENT, ARISING OUT OF THIS AGREEMENT OR THE USE OF THE NETWORK BY THE ACCESSING PARTY OR USERS. CHARTER WILL NOT BE RESPONSIBLE FOR ANY CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES ARISING OUT OF THIS AGREEMENT. Any loss or damage occurring to the Accessing Party or Users arising from the use of the Network will be the sole responsibility of the Accessing Party or Users, unless and except to the limited extent such loss or damage was caused by Charter's acts or omissions. Without limiting the foregoing, Charter will not be liable to the Accessing Party or Users for: (i) any loss or corruption of Accessing Party data stored in or transmitted through the Network; (ii) any incorrect results obtained by using the Network; (iii) any interruption of access or use of the Network for whatever reason; (iv) access of any Accessing Party data by third parties; or (v) toll fraud in accessing, using or egressing the Network.

8. Ownership and Use

Except for information or data input into the Network by the Accessing Party ("Accessing Party Information"), all information, including data, created or contained in the Network, including messages, is the property of Charter or one or more third parties ("Information"). The Accessing Party hereby assigns to Charter, to the extent it has the right so to do, all of its right, title, and interest in and to Information created on the Network. Except as otherwise required by law, Charter hereby grants to the Accessing Party a non-exclusive, perpetual, royalty free license to use such Information for legitimate business purposes in furtherance of the Accessing Party's business relationship with Charter or its affiliates and for no other purpose. Except as otherwise required by law, the Accessing Party hereby grants to Charter a non-exclusive, perpetual, royalty free license to use Accessing Party Information for any legitimate business purposes in furtherance of the Accessing Party's business relationship with Charter or its affiliates and for no other purpose.

9. Indemnity

The Accessing Party shall defend, indemnify and hold harmless Charter, its parent company and its subsidiaries, affiliates, and their respective officers, directors, employees, agents, successors and permitted assigns (each, a "Charter Indemnitee") from and against all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers, arising out of or resulting from any third-party claim against any Charter Indemnitee arising out of or resulting from Accessing Party's failure to comply with any of its obligations under this Section in performance of this Agreement, including but not limited to Accessing Party's negligence, willful misconduct, breach of contract or violations of applicable law by the Accessing Party or Users.

10. Malicious Code Attacks

The Accessing Party shall be liable for all damage to or loss of computer files or programs, disruption of use of all or any part of the Network or other Charter computer systems, or other loss or damage to Charter, which results in whole or in part, directly or indirectly, from the Accessing Party introducing a computer virus or other code designed to destroy, corrupt, facilitate theft of data or software, or disable or lock software or the Network on Charter computer systems or networks. The Accessing Party shall not be so liable to the extent that such computer virus or such other code was unintentionally introduced on Charter computer systems or networks and the Accessing Party has used reasonable care to detect and eliminate computer viruses using then-current industry standard security and anti-virus tools.

11. Assignment; Relationship of Parties

This Agreement may not be assigned by the Accessing Party without the prior written consent of Charter, which may be withheld by Charter in its sole judgment. Nothing in this Agreement will be construed to make the Accessing Party or any of its employees an employee, agent, joint venturer or partner of Charter. In no event will Accessing Party or User represent that they have authority to bind, or to act for or on behalf of, Charter or any Charter affiliate unless Charter has previously authorized them to do so in writing.

12. Software

In no event will Users copy, download, modify, reverse engineer, decompile, disassemble or create derivative works of Charter software programs, or third party software programs licensed to Charter. Accessing Party will provide, maintain and utilize all necessary software and security programs to secure their hardware, software, network and any other application or device used to connect to any portion of the Network.

13. Entirety

This Agreement embodies the entire understanding between Charter and the Accessing Party and there are no contracts, agreements, understandings, conditions, warranties or representations, oral or written, express or implied, with reference to the subject matter hereof which are not merged herein.

14. Internet Access

Except to the extent access rights are expressly granted by Charter to the Accessing Party, in writing, neither the Accessing Party nor any of its employees, agents, officers or directors not located at a Charter owned or managed site will access or use the Internet through any Charter gateway or other Charter connection to the Internet. Such use by "on-site" Users will only be for legitimate business purposes. Users will not use such Charter connection in violation of any law, statute, regulation, rule or ordinance of any government entity, domestic or foreign, and will not use such Charter connection in a way that will subject Charter to any criminal or civil liability.

15. Authorization, Responsible Parties

It is the responsibility of the Accessing Party to ensure that all Users are familiar with Charter's Acceptable Use Policy and are responsible and appropriate persons to have access to the Network. It is the responsibility of the Accessing Party to ensure that all Users practice secure networking at their location at all times. This Agreement must be signed or authorized by an officer of Charter Communications (vice president or above) or this Agreement shall be null and void.

It is the responsibility of the Accessing Party to immediately notify Charter's IT Help Desk by calling **1-888-415-0012**, or the successor telephone number thereto, when access has expired, when employees who are Users are terminated by the Accessing Party. When the possibility exists that a Security Incident has or will occur, Accessing Party must immediately call your Charter Sponsor and then call Charter's Law Enforcement Hotline at **1-866-894-0103** or e-mail **dlsecurityincidents@charter.com**.

EXHIBIT C

ACCEPTABLE USE OF TECHNOLOGY POLICY

Policy Issuer: Compliance	**Applicable To:** All business units	**Effective Date:** 3/15/2006	**Last Revised:** 10/27/15
Title: Acceptable Use of Technology Policy		**Approved By:** Compliance Committee	**Info Classification:** Internal Only

Table of Contents:

1.0 PURPOSE

The purpose of the Acceptable Use of Technology Policy ("Policy") is to define the standards for the acceptable use of Charter Communications' ("Charter") computing equipment, information and communications. This Policy is to be read in conjunction with the Employee Handbook, Code of Conduct and the Information Classification & Protection Policy.

(back to top)

2.0 SCOPE

This Policy applies to all of Charter's employees, contractors, vendors, agents, consultants, temporary workers and any other person or entity who has access to or connects to any of Charter's electronic, network or other electronic resources (the "Network"), or who utilize any computing or other equipment owned, leased or managed by Charter or any equipment that is connected to the Network ("Equipment"). This Policy governs all access including local, remote, and mobile access to the Network. All capitalized terms are defined in the Glossary.

(back to top)

3.0 POLICY

The requirements contained herein are cumulative and are meant to be read in conjunction with one another and not in isolation

3.1 GENERAL GUIDELINES

1. ALWAYS exercise common sense and good judgment
2. Access to the Network is a privilege, not a right. Access may be suspended at any time and for any reason. Charter reserves the right to monitor, audit and police the use of its Network and any content or communication stored on or communicated through the Network. Your use of the Network or the Equipment constitutes your consent to this monitoring.
3. Any data or other Information created or stored on the Network or any Equipment becomes and/or remains the property of Charter.
4. All company Information must be protected according to the requirements of Charter's Information Classification & Protection Policy. Information contained on the Network or Equipment is classified as Public, Internal Only, Restricted or Sensitive. Instructions on how these different types of Information must be accessed, distributed, stored and disposed of are contained in the Information Classification & Protection Policy.
5. Some parts of this Policy may require you to encrypt certain information or transmission paths. If you need assistance encrypting any information or using Charter's approved encryption software, contact Charter's IT SOC by calling 1-888-415-0012 or submitting an IT Remedy ticket at mars.corp.chartercom.com.
6. Charter may modify this Policy without notice.
7. Units, departments, and groups may establish more restrictive policies for their respective users but may not waive or lessen any requirement contained in this Policy without written authorization from the Compliance Committee or its designee. Any such more restrictive policy must be in writing and must be made available to that unit, department or group that is subject to the additional restrictions.
8. In accordance with Charter's Employee Privacy Policy, you should have no expectation of privacy in any location, item, information or communication existing or occurring on or in Charter's property or when using Charter's resources or equipment, even if protected by passwords, access codes, keys, locks or other security devices.
9. At the end of your employment or service, you are required to relinquish all Charter owned, leased or managed Equipment and all files or Information in an unencrypted, non-password protected and readily accessible form. You may not attempt or continue to access the Network or Equipment after the end of your employment or service.
10. ALWAYS take all required training including but not limited to Compliance Awareness, Security & Privacy, Harassment Prevention in the Workplace and Records & Information Management training. Most required employee training courses are available on Charter's training site, Charter University.
11. ALWAYS follow all applicable policies including but not limited to the Employee Handbook, Code of Conduct, Information Classification & Protection Policy and Records & Information Management Policy.

(back to top)

3.2 EQUIPMENT/HARDWARE

1. NEVER connect personal equipment to the Network without authorization from Charter's IT SOC.
2. NEVER remove Equipment from Charter premises without authorization. Employees who are issued laptop computer or other Portable Storage Devices that are intended to be removed from the premises are presumed to have authorization unless otherwise instructed.
3. NEVER knowingly perform an act which will interfere with the normal operation of Charter's Network and Equipment.
4. ALWAYS have up to date anti-virus software installed and running on all Equipment connected directly or remotely to the Network.
5. Never disable Charter's centrally managed anti-virus and anti-malware security software.
6. Always report anti-virus or anti-malware that reports an out of date issue to the IT SOC by calling 888-415-0012.
7. Equipment connected to the Network must meet the minimum requirements established by Charter's Information Technology Department, as modified form time to time.
8. Except as otherwise provided, ALWAYS store all Charter Information on your assigned Charter network "Home Drive," a department network "Shared Drive" or an approved SharePoint/COIN collaboration site.

(back to top)

3.3 PORTABLE STORAGE DEVICES

Portable Storage Devices are especially susceptible to being lost or compromised and additional requirements must be followed. The following are some general requirements followed by additional specifications for particular types of Portable Storage Devices. Portable Storage Devices are divided into five broad categories: (1) laptops and mobile computers, (2) CD/DVD/Disk, (3) external hard drives (including removable hard drives and USB thumb/flash drives), (4) backup tapes, and (5) handheld/wireless devices.

A. General Requirements

1. NEVER leave any Portable Storage Devices unattended and unsecured. When a device is left unattended, it should be protected as much as possible against unauthorized access or removal (e.g., locked in a cabinet, drawer, hotel room safe, cable locked or otherwise protected from unauthorized removal).
2. NEVER leave any Portable Storage Devices in any vehicle overnight. Never leave a device unattended in a vehicle unless it is protected as much as possible against unauthorized access or removal (e.g., locked in the trunk or, if the vehicle does not have a trunk, in a location that is not visible from outside the vehicle).
3. ALWAYS immediately report all lost or stolen Portable Storage Devices to Charter's IT SOC by calling 1-888-415-0012. If the lost or stolen Portable Storage Device contains ANY customer or employee information, immediately alert your supervisor and file a report on EthicsPoint.
4. ALWAYS comply with the instructions and requests of those assigned to investigate the lost or stolen Portable Storage Device.

5. ALWAYS take precautions to prevent your login, password, and any Charter Information from being viewed by others while using a Portable Storage Device.
6. Except as otherwise provided herein, NEVER save Charter Information or other files on your Portable Storage Device other than those files automatically saved on it by the device's applications or necessary to run the Portable Storage Device.
7. NEVER store any unencrypted SENSITIVE Charter Information on any Portable Storage Device, in accordance with this Policy.

(back to top)

B. Laptops and Mobile Computers

1. ALWAYS connect to Charter's VPN if you are going to access the Internet from Charter Equipment while not connected to Charter's Network.
2. Except as provided by B.3., ALWAYS store all Charter Information on your assigned Charter network "Home Drive," a department network "Shared Drive" or an approved SharePoint/COIN collaboration site.
3. You may check-out or create, as applicable, files (other than those containing SENSITIVE Charter Information) using the check-in/check-out procedures if you will not be connected to Charter's Network and unable to use the VPN. Find directions on Panorama to learn more about the check-in/check-out procedures.
4. ALWAYS check-in all files that were previously checked-out as soon as your Portable Storage Device is reconnected to Charter's Network.

(back to top)

C. CD/DVD/Disk

1. ALWAYS encrypt all SENSITIVE Charter Information saved to CD/DVD/Disk in accordance with Charter's Encryption Policy.
2. ALWAYS encrypt or password protect all RESTRICTED Charter Information saved to CD/DVD/Disk.
3. You may store Charter Information that is NOT SENSITIVE or RESTRICTED but has a legitimate business purpose to a CD/DVD/Disk without encryption or password protection.
4. AVOID saving any information that does not have legitimate business purposes to any CD/DVD/Disk using Charter's Network.
5. You may read/access information on a CD/DVD/Disk that does not have a legitimate business purpose with your supervisor's approval so long as such use is consistent with Charter's Employee Handbook and the other requirements of this Policy.
6. ALWAYS save Charter Information to an appropriate network drive and then destroy (pursuant to Information Classification & Protection Policy) or put adequate physical controls (pursuant to Information Classification & Protection Policy) to protect any CD/DVD/Disk you receive that contains RESTRICTED or SENSITIVE Charter Information that has not been encrypted or password protected as required by the above requirements.

(back to top)

D. External Hard Drives (including USB thumb/flash drives)

1. NEVER store/save RESTRICTED or SENSITIVE Information to external hard drive without Charter's Corporate Information Technology Department's review and written approval.
2. ALWAYS encrypt all SENSITIVE Charter Information saved to an external hard drive in accordance with Charter's Encryption Policy.
3. ALWAYS encrypt or password protect all RESTRICTED Charter Information saved to an external hard drive.
4. You may store Charter Information that is NOT SENSITIVE or RESTRICTED but has a legitimate business purpose to an external hard drive without encryption or password protection.
5. NEVER save any information that does not have legitimate business purposes to any external hard drive using Charter's Network.
6. You may read/access an external hard drive that does not have a legitimate business purposes with your supervisor's approval so long as such use is consistent with Charter's Employee Handbook and the other requirements of this policy.
7. ALWAYS save the information to an appropriate network drive and then destroy (pursuant to Information Classification & Protection Policy) or put adequate physical controls (pursuant to Information Classification & Protection Policy) to protect any external hard drive you receive that contains RESTRICTED or SENSITIVE Charter Information that has not been encrypted or password protected as required by the above requirements.

(back to top)

E. Backup Media

The use of backup Media is governed by the Electronic Data Backup Policy.

(back to top)

F. Handheld/Wireless Devices

1. ALL Handheld/Wireless Devices must be password protected, including personal devices containing any Information.
2. NEVER send to or save any RESTRICTED or SENSITIVE Charter Information to a Handheld/Wireless Device unless it is protected in accords with Charter's Information Security Policy.

3.4 AUTHENTICATION

1. You are responsible for the security and confidentiality of your passwords and account access. If your password is lost, stolen or if its integrity is compromised immediately alert Charter's IT SOC by calling 1-888-415-0012.
2. ALWAYS change your password(s) at least every sixty (60) days.
3. Account access must be revoked within 48 hours of any reported terminated user.

4. An account review process must identify all unused network accounts every 90 days. Accounts identified as being inactive or unused for this time frame will be disabled unless proper business justification is submitted.
5. When accessing Charter Communications information system resources, any account failing to provide proper credentials six consecutive times must be locked out for a period of no less than 30 minutes or until support personnel can reset the account.
6. Any user computer session inactive for a period of 15 minutes must be re-authenticated by entering network credentials at the logon screen. Charter technology standards enforce this requirement.
7. Shared, group, or generic IDs must be disabled or removed and not used for individual system administration or other critical functions.
8. ALWAYS use a strong password that is at least eight (8) alphanumeric characters in length, uses "special" charters in addition to numbers and letters (e.g., !@#$%^&*()_+1—), and uses both upper and lower case characters (e.g., a-z, A-Z). Do not base password off of any personal information (e.g., date of birth, name) or that are words any language, slang, dialect, jargon, etc. Never use common or generic usernames or passwords (e.g., admin or password).
9. NEVER reveal your password to any other person, at any time, for any reason. This includes your supervisor, co-workers, vendors, or third-parties such as family and other household members. Charter Information Technology staff will NEVER ask for your password.
10. NEVER write down or store your password in an unprotected fashion or transmit it via e-mail or another form of unencrypted communication.
11. ALL passwords must be deleted or changed immediately upon of the end of employment or service any User.
12. ALWAYS review your level of access (including which systems and applications you have access to) whenever your responsibilities, function or position changes. It is the obligation of every User to make sure that their level of access is current.
13. ALL User-, system- and application-level passwords must conform to Charter's Password Policy.

3.5 WIRELESS CONNECTIVITY ON CHARTER PREMISES

1. Onsite Charter employees and contractors must access the network via wired connection unless no wired connection is available. In the event, no wired connection is available "CharterCorp" or a duly authorized alternative must be utilized. "CharterGuest" connections are limited.
2. "Charter_Guest_Wireless" is for the use of Charter guests such as vendor visits. "Charter_Guest_Wireless" must not be utilized by Charter employees or contractors to access the Charter network unless no wired or "Charter_Wireless" connections are available.
3. Only Charter authorized devices are allowed to connect to the Charter Network.

(back to top)

3.6 ILLEGAL OR PROHIBITED ACTIVITIES

1. ALWAYS comply with all applicable laws, the Code of Conduct and all Charter policies.
2. NEVER violate any rights protected by copyright, trade secret, patent or other intellectual property, or similar law or regulations.

3. NEVER make any unauthorized use, duplications, broadcast or sharing of any content, in any form, that is subject to any copyright or other restriction and for which Charter or the User does not have the appropriate license.
4. NEVER allow anyone else to use your username or password to log onto the Network or any application. NEVER use Equipment or an account that you are not authorized to use or obtain a password without the consent of the account owner.
5. NEVER use the Network to gain unauthorized access to any computer system.
6. NEVER attempt to circumvent data protection mechanisms, content filters or uncover security flaws.
7. NEVER use any software/application that has not been approved by Charter's Information Technology department or violate the terms of any applicable software licensing agreements or terms of use.
8. NEVER mask the identity of an account or machine without authorization.
9. NEVER attempt to monitor or tamper with anyone's electronic communications, or read, copy, change or delete anyone's files or software without authorization.
10. NEVER export software, technical information, encryption software or technology to foreign countries or nationals in violation of export control laws.
11. NEVER knowingly introduce or disseminate any malicious programs or code (e.g., virus, worm, trojan horse, e-mail bomb, etc.) into or on the Network.
12. NEVER access, procure or transmit any material or content in violation of Charter's Sexual Harassment or any other Charter policy or that creates a hostile work environment.
13. NEVER use the Network or Equipment to search for, access or otherwise utilize any site, service or content related to gambling or gaming, adult material or content, that disparages any racial, ethnic, religious or other group in violation of Charter's policies, or social unauthorized networking sites (including online dating), in accordance with the Employee Handbook and the Online Public Communications Policy.

(back to top)

3.7 ELECTRONIC COMMUNICATIONS

The following are additional requirements that apply to Electronic Communications. The term Electronic Communications includes but is not limited to e-mail, text messages, instant messages, telephone calls or any other type of analog or digital communication sent over or using the Network or using the Equipment.

1. ALWAYS exercise caution when opening e-mail attachments received from unknown or untrusted senders.
2. NEVER distribute unsolicited e-mail messages including sending of "junk mail" or other advertising material when outside your scope of responsibility.
3. NEVER distribute "chain letters," "Ponzi" or other "pyramid" schemes of any type.
4. NEVER make or send harassing e-mail, telephone calls or other messages whether through language, frequency, or size of messages.
5. NEVER introduce sexually explicit or otherwise offensive material into any electronic communication or other Medium unless this activity is a part of the Users authorized job duty.

6. NEVER use unauthorized or forged e-mail header information.
7. NEVER post to, participate in or host blogs, newsgroups, chat rooms or other similar activities in violation of Charter's Online Public Communications Policy.
8. NEVER email unencrypted SENSITIVE Information, including but not limited to social security numbers, driver's license or state-issued identification numbers, or financial account numbers or credit or debit card numbers.
9. NEVER use non-Charter e-mail, instant messaging or other communications services not approved by Charter's IT Department to conduct company business.
10. NEVER transmit Records (as defined by Charter's Records & Information Management Policy) via voicemail, text messages or instant messages.

(back to top)

4.0 REPORTING BREACHES IN SECURITY AND VIOLATIONS OF THIS POLICY

Reporting Breaches in Security

If you observe or suspect any type of suspicious, abnormal or unauthorized activity that threatens the integrity, confidentiality or availability of Charter's Network or Equipment; or any activity that compromises or is likely to compromise customer or employee personal information, whether through unauthorized disclosure, access or destruction, you should immediately contact your supervisor and file a report on EthicsPoint. Threats to the Network should also be reported to Charter's IT SOC by calling 1-888-415-0012.

Reporting Violations of this Policy

Except as otherwise stated herein, violations or noncompliance with this policy should be reported your manager, your local human resources representative or to EthicsPoint.

(back to top)

5.0 ENFORCEMENT

Any violation of this Policy may result in termination of your use or access to the Network and/or disciplinary action up to and including termination. Charter may take any legal action it deems appropriate and/or report any suspected unlawful conduct to law enforcement.

(back to top)

6.0 GLOSSARY

Term	Term Description
Charter	Charter Communications, Inc. and its subsidiaries and affiliates.
Charter University	Charter's Online training and education website. Charter University is available at http://cuonline.
Enterprise Support Desk (IT SOC)	A dedicated team of IT professionals that assist with administrating and supporting various Information Technology functions, including but not limited to on- and off-boarding Network access, incident management and resolution, IT alert and notifications, and other back office functions. The Enterprise Support Desk may be reached by calling 1-888-415-0012

	or by submitting an IT "remedy" ticket at mars.corp.chartercom.com.
Equipment	Any computing or other equipment that is owned, leased or managed by Charter or that is connected to the Network, including but not limited to computers, servers, routers, handheld/mobile/wireless devices (e.g., cell phones, personal digital assistants, handheld computers).
EthicsPoint	Charter's reporting mechanism that provides out employees, customers, vendors and suppliers with a simple, anonymous and confidential way of reporting their concerns of unethical behavior, violations or suspected violations of the law and/or the Code of Conduct. EthicsPoint reports may be filed 24 hours a day, 7 days a week by visiting http://www.ethicspoint.com or by calling (866) 384-4277.
Information	All data within Charter's possession or control that is created or received by users during the performance of their duties at Charter. Information can be broken down into two categories that are defined as "Records" and "Non-Records." See the Records & Information Management Policy
Internal Only Information	Information that is not Restricted or Sensitive and which is not approved for general circulation outside of the company, where its disclosure would inconvenience the company, but is unlikely to result in significant financial loss or serious damage. Examples: internal memos, unpublished marketing materials, competitive analysis, company policies, etc. See the Information Classification & Protection Policy
Medium	Object (such as paper) or device (such as a hard drive, tape or optical disk) upon which Information is stored. See the Records & Information Management Policy
Network	Any and all of Charter's electronic, network or other resources, including but not limited to computing equipment, software and applications, databases, electronic mail, the Internet, telephone, voicemail and all telecommunications facilities.
Non-Record	Information that has no business value and which is not subject to statutory or regulatory record-keeping requirements, as specified by Charter's Record Retention Schedules, including, but not limited to, drafts and copies of Records. See the Records & Information Management Policy
Policy	Employee Acceptable Use of Technology Policy
Portable Storage Device	Includes laptops and other mobile computers, compact disks (CDs), digital video disks (DVDs), backup tapes, universal serial bus (USB) thumb drives, wireless handheld devices (such as Blackberries) or other personal digital assistants (PDAs), mobile phones, external hard drives

	and other movable devices that can be used to store or transfer Information.
Public Information	Information that does not fall within one of the more restrictive categories and that can be made available to the public without any financial, legal or other implications to Charter. *Examples:* information in the public domain, released press releases, published marketing materials, publically filed documents, etc. See the Information Classification & Protection Policy
Record	Information recorded on a Medium and intentionally retained and managed as evidence of an organization's activities, decisions, events, actions or transactions because of its ongoing business, operational, legal, regulatory and / or historical value. See the Records & Information Management Policy
Restricted Information	Information that is not Sensitive and which is considered critical to the organization's ongoing operations and could seriously impede or disrupt them if disclosed without authorization or made available to the public. *Examples:* accounting information, proprietary intellectual property, business plans, subscriber or employee information (that is not classified as Sensitive), etc. See the Information Classification & Protection Policy
Sensitive Information	Any highly sensitive internal information about customers, employees or other information which the loss of confidentiality, integrity, or availability could be expected to have a severe adverse effect on the company. The highest levels of integrity, confidentiality, and restricted availability are vital. *Examples:* customer or employee social security or tax identification number, driver's license or state issued identification number, financial or payment card information, information regard impending cable system acquisitions or divestitures, investment strategies, etc. See the Information Classification & Protection Policy
User	Any person or thing that accesses the Network or uses the Equipment.

REFERENCES

All companywide policies may be found on the Policies page of Charter's intranet site, Panorama.

Code of Conduct
Electronic Data Backup Policy
Employee Handbook
Employee Privacy Policy
Encryption Policy
EthicsPoint (compliance and incident reporting website)
Information Classification & Protection Policy
Online Public Communications Policy
Records & Information Management Policy
Panorama
Wireless Device Policy