



Process Issuer: Compliance	Applicable To: All business units	Effective Date: 3/15/2006	Last Revised: 04/27/17
Title: Acceptable Use of Technology Policy		Approved By: Compliance Committee	Info Classification: Internal Only

Acceptable Use of Technology Policy

Table of Contents:

Table of Contents:	1
1.0 PURPOSE	1
2.0 SCOPE	1
3.0 POLICY.....	2
3.1 GENERAL GUIDELINES	2
3.2 EQUIPMENT/HARDWARE.....	3
3.3 PORTABLE STORAGE DEVICES.....	3
3.4 AUTHENTICATION	5
3.5 WIRELESS CONNECTIVITY ON CHARTER PREMISES	6
3.6 ILLEGAL OR PROHIBITED ACTIVITIES	6
3.7 ELECTRONIC COMMUNICATIONS	7
4.0 REPORTING BREACHES IN SECURITY AND VIOLATIONS OF THIS POLICY	8
5.0 ENFORCEMENT	8
6.0 GLOSSARY	8
REFERENCES	11

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](#).

[\(back to top\)](#)

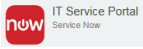
2.0 SCOPE

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](#).

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 a [Service Now ticket](#) by navigating to <https://login.sso.charter.com/nidp/portal> and selecting the IT Service Portal.

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](#).

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. **ALL** Equipment connected to the Network must meet the minimum requirements established by Charter's Information Technology Department, as modified from 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.

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” characters in addition to numbers and letters (e.g., !@#\$%^&*()_+|~), 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 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.

6. **NEVER** introduce sexually explicit or otherwise offensive material into any electronic communication or other Medium unless this activity is a part of the User's authorized job duty.
7. **NEVER** use unauthorized or forged e-mail header information.
8. **NEVER** post to, participate in or host blogs, newsgroups, chat rooms or other similar activities in violation of Charter's Online Public Communications Policy.
9. **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.
10. **NEVER** use non-Charter e-mail, instant messaging or other communications services not approved by Charter's IT Department to conduct company business.
11. **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. You may also submit security events for remediation to DLSecurityIncidentResponse@charter.com.

Reporting Violations of this Policy

Except as otherwise stated herein, violations or noncompliance with this policy should be reported to 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.

6.0 GLOSSARY

Term	Term Description
<i>Charter</i>	Charter Communications, Inc. and its subsidiaries and affiliates.
<i>Charter University</i>	Charter's Online training and education website. Charter University is available at http://cuonline .
<i>Enterprise Support Desk (IT SOC)</i>	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 IT SOC may be contacted by calling 888-415-0012 or by submitting a Service Now ticket by navigating to https://login.sso.charter.com/nidp/portal and selecting the IT Service Portal.
<i>Equipment</i>	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).
<i>EthicsPoint</i>	<p>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.</p> <p>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.</p>
<i>Information</i>	<p>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."</p> <p>See the Records & Information Management Policy</p>
<i>Internal Only Information</i>	<p>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.</p> <p>Examples: internal memos, unpublished marketing materials, competitive analysis, company policies, etc.</p> <p>See the Information Classification & Protection Policy</p>
<i>Medium</i>	<p>Object (such as paper) or device (such as a hard drive, tape or optical disk) upon which Information is stored.</p> <p>See the Records & Information Management Policy</p>
<i>Network</i>	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.

<i>Non-Record</i>	<p>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.</p> <p>See the Records & Information Management Policy</p>
<i>Policy</i>	Employee Acceptable Use of Technology Policy
<i>Portable Storage Device</i>	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
<i>Public Information</i>	<p>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.</p> <p><i>Examples:</i> information in the public domain, released press releases, published marketing materials, publically filed documents, etc.</p> <p>See the Information Classification & Protection Policy</p>
<i>Record</i>	<p>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.</p> <p>See the Records & Information Management Policy</p>
<i>Restricted Information</i>	<p>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.</p> <p><i>Examples:</i> accounting information, proprietary intellectual property, business plans, subscriber or employee information (that is not classified as Sensitive), etc.</p> <p>See the Information Classification & Protection Policy</p>
<i>Security Incident Response</i>	Security incidents may be submitted for remediation with as many details as available to SecurityIncidentResponse@charter.com .

<i>Sensitive Information</i>	<p>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.</p> <p><i>Examples:</i> 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.</p> <p>See the Information Classification & Protection Policy</p>
<i>User</i>	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](#)