



## CIENA IT ACCEPTABLE USE POLICY

**Revision**

E

**Document Number**

CO1-INF-26

**Page**

1 of 10

**1.0 Purpose:** The purpose of this policy is to outline the acceptable use of Ciena's Network and IT Equipment. Inappropriate use of Ciena's Network or IT Equipment may expose Ciena to risks such as malware attacks, loss or theft of corporate information, compromise of systems and services, and legal and reputational issues.

**2.0 Scope:** This policy applies to employees of Ciena and its subsidiaries and Contingent Workers who operate IT Equipment or make use of Ciena's Network.

### **3.0 Policy Statement:**

#### **3.1 General Statement**

**3.1.1** Data that resides on IT Equipment or Ciena's Network is the property of Ciena. IT Equipment and Ciena's Network are to be used for business purposes in serving the interests of the company, our clients and customers. Users of IT Equipment or Ciena's Network are responsible for the physical security of the equipment and the security of the information held on such equipment.

**3.1.2** This policy is intended to supplement the Ciena Code of Business Conduct and Ethics to provide a standard of conduct for the use of IT Equipment and Ciena's Network.

**3.1.3** Violations of this policy should be reported to the Chief Information Officer or the Senior Director - IT Strategy, Governance & Information Security.

**3.1.4** Information Security may update this policy as business process and technology change, or as IT services change. Any change in this policy will be communicated to employees using the Corporate Policies and Procedures section of Inside Ciena and also with security awareness training.

#### **3.2 Access to Ciena Systems and Networks**

**3.2.1** Ciena will provide access to IT Equipment and Ciena's Network for all employees as required to perform their job responsibilities.


**3.2.2** Contingent Workers may be provided access as required for business purposes. The employee managing the Contingent Worker assumes responsibility for the identification of access requirements and use of the account.

**3.2.3** Guests to Ciena who require temporary access to IT Equipment or Ciena's Network may be provided with access as required for business purposes.

Unless otherwise specified, information shown on this document is proprietary and is not to be reproduced wholly or in part without the expressed permission of the Ciena Corporation. Before using, verify this copy is the correct revision by accessing the controlled document on the network.

UNCONTROLLED IF STORED OUTSIDE REPOSITORY OR PRINTED

DOCUMENT TEMPLATE CO4-QSG-07 – REV: D

	<b>CIENA IT ACCEPTABLE USE POLICY</b>		
	<b>Revision</b>	<b>Document Number</b>	<b>Page</b>
	E	CO1-INF-26	2 of 10

By default, guests will be provided with access to external sub-networks which prevent access to Ciena data but allows for Internet access. Guest access requests for IT Equipment or to Ciena's Network must be requested from the Service Desk.

- 3.2.4** IT Equipment connecting to Ciena's Network must have IT mandatory software installed and operational; this includes, but is not limited to, encryption, anti-virus, and Corporate Systems Management software.


### **3.3 Privacy and Ownership**

- 3.3.1** Any data stored or accessed on IT Equipment or Ciena's Network, including electronic mail, are considered the property of Ciena. There should be no expectation of privacy in data sent, received, accessed or stored, whether for business or personal purposes, while using Ciena's IT Equipment or Network.
- 3.3.2** Electronic mail messages are considered written communications and may be subject to subpoena as part of legal proceedings. Ciena may inspect the contents of electronic mail messages in the course of an investigation and will fulfill any legal obligations as required.
- 3.3.3** Authorized individuals within Ciena may monitor IT Equipment and traffic on Ciena's Network, at any time, for any reason, and without notice. In addition, authorized individuals may access IT Equipment without notice for the purposes of system repair, update, analysis or investigation.
- 3.3.4** Ciena reserves the right to audit the Network and IT Equipment on a periodic or continuous basis to ensure compliance with policies.
- 3.3.5** Any data not deemed necessary for a user's job responsibilities may be removed from IT Equipment or Ciena's Network at any time and without notice to the user. IT is not required to move, copy or transmit any non-business or personal data during maintenance activity to IT Equipment or the Network; such as reimaging or refresh of equipment.

### **3.4 Software**

- 3.4.1** Only legally licensed software may be installed on IT Equipment and Ciena's Network. Users are expected to read, understand and conform to the license requirements of any software product(s) they use, re-distribute or install. Individuals must not install free and open source software (FOSS) where the terms of use exclude corporate environments.

Unless otherwise specified, information shown on this document is proprietary and is not to be reproduced wholly or in part without the expressed permission of the Ciena Corporation. Before using, verify this copy is the correct revision by accessing the controlled document on the network.

	<b>CIENA IT ACCEPTABLE USE POLICY</b>		
	<b>Revision</b>	<b>Document Number</b>	<b>Page</b>
	E	CO1-INF-26	3 of 10

**3.4.2** If a Ciena employee has individually procured software, the user must retain the license agreement, license key or activation code from the software vendor which provides assurance that the installed software is legally licensed and that Ciena is compliant with copyright obligations.

**3.4.3** Users are prohibited from disabling or deleting software on IT Equipment that is mandated by IT without prior approval. This includes, but is not limited to, encryption, anti-virus, and Corporate Systems Management software. For Mobile Device management software policy restrictions, refer to the Ciena Mobile Device Policy ([CO1-INF-17](#)).

### **3.5 Physical Security**

**3.5.1** It is the responsibility of the user to take appropriate precautions to prevent damage to, or loss or theft of IT Equipment. Damage or loss determined to be caused by neglect, careless use or intentional misconduct may result in disciplinary action up to and including termination. Furthermore, a user's department may be responsible for any repair or replacement costs associated with the damage or loss of such IT Equipment.

**3.5.2** IT Equipment must be controlled while outside of Ciena facilities. In vulnerable situations (e.g. public areas such as airports, hotels and conference centers) IT Equipment should never be left unattended.


**3.5.3** Users are responsible for IT Equipment issued to them or in their possession and control. All IT Equipment must be returned to IT immediately upon request or upon termination of employment.

**3.5.4** The manager of a terminated employee or Contingent Worker is responsible for ensuring that IT Equipment is returned to IT either by taking possession of the IT Equipment on or prior to the last day of employment or making arrangements for the collection and return of the IT equipment.

Any monies owed to the terminated employee may be withheld until all Ciena property has been returned except where prohibited by law. The terminated employee's department may be charged the replacement cost for IT provided Equipment which is not returned.

**3.5.5** If an IT asset is lost or stolen, the user is responsible for notifying the Service Desk, Information Security or their Manager immediately.

Unless otherwise specified, information shown on this document is proprietary and is not to be reproduced wholly or in part without the expressed permission of the Ciena Corporation. Before using, verify this copy is the correct revision by accessing the controlled document on the network.


	<b>CIENA IT ACCEPTABLE USE POLICY</b>		
	<b>Revision</b>	<b>Document Number</b>	<b>Page</b>
	E	CO1-INF-26	4 of 10

- 3.5.6** Any IT Equipment that is suspected to be stolen should be reported to local police. The police report number must be provided to Ciena's Corporate Security Officer within 24 hours or as soon as available.

### **3.6 Data Protection**

- 3.6.1** It is the responsibility of users of IT Equipment and the Ciena Network to take appropriate precautions to prevent data leakage and unauthorized access to non-public Ciena data. The Information Security Policy ([CO1-INF-01](#)) describes the process for securing the availability, integrity and confidentiality of data on IT Equipment and the Ciena Network.
- 3.6.2** When temporarily leaving IT Equipment unattended, users should manually lock the screen. Idle lockout is specified in the IT Password Policy ([CO1-INF-02](#)).
- 3.6.3** Users must configure strong passwords in compliance with the Ciena IT Password Procedure ([CO2-INF-20](#)).
- 3.6.4** Authorized users are responsible for the security of their user credentials for access to Ciena systems. Users are prohibited from revealing account login information or allowing use of an account by others, including family, friends, or other Ciena employees.
- 3.6.5** Information that is stored on IT Equipment should be uploaded to a supported IT business application (e.g. SharePoint) for secure service and storage.
- 3.6.6** Sharing and exchange of information using Cloud applications is permitted only for authorized users and only with IT Authorized cloud storage or cloud file sharing applications.

Unless otherwise specified, information shown on this document is proprietary and is not to be reproduced wholly or in part without the expressed permission of the Ciena Corporation. Before using, verify this copy is the correct revision by accessing the controlled document on the network.

	<b>CIENA IT ACCEPTABLE USE POLICY</b>		
	<b>Revision</b>	<b>Document Number</b>	<b>Page</b>
	E	CO1-INF-26	5 of 10

### 3.7 Unacceptable Use


**3.7.1** Ciena's IT Equipment and Network may not be used for any of the following purposes:

- 3.7.1.1** Accessing, storing or transmitting explicit material in formats such as text, imagery, video or audio.
- 3.7.1.2** Offensive, demeaning, discriminatory, harassing, or disruptive material or messages that are inconsistent with Ciena's core values as standardized in the Code of Business Conduct and Ethics.
- 3.7.1.3** Storing or downloading copyrighted material such as music, movies or other media unless you have legally purchased the media and/or have permission to use.
- 3.7.1.4** Accessing cloud storage or cloud file sharing applications for exchange of information, unless the IT Authorized cloud storage or cloud file sharing application is used.
- 3.7.1.5** Streaming of music, video, free and/or subscription based services or other high bandwidth non-business related media over Ciena's Network.
- 3.7.1.6** Installation of "cracking" applications to install or use software without purchasing a license or "jail break" applications to allow the use of features or a service from a service provider without purchasing the service.
- 3.7.1.7** Conducting any activity that is illegal under local, federal or international law, including export control regulations and intellectual property laws.
- 3.7.1.8** Sharing of Ciena information that is not expressly approved by Ciena's legal and/or public relations department. This includes print media as well as posting to blogs and social media sites.
- 3.7.1.9** Use of a Ciena email account to attribute personal statements, opinions or beliefs to Ciena.
- 3.7.1.10** Initiating security breaches or disruption of the Ciena Network.
- 3.7.1.11** Intentional introduction of malicious programs into the Ciena Network.

Unless otherwise specified, information shown on this document is proprietary and is not to be reproduced wholly or in part without the expressed permission of the Ciena Corporation. Before using, verify this copy is the correct revision by accessing the controlled document on the network.

UNCONTROLLED IF STORED OUTSIDE REPOSITORY OR PRINTED

DOCUMENT TEMPLATE CO4-QSG-07 – REV: D

	<b>CIENA IT ACCEPTABLE USE POLICY</b>		
	<b>Revision</b>	<b>Document Number</b>	<b>Page</b>
	E	CO1-INF-26	6 of 10

- 3.7.1.12** IT Equipment and Ciena Network vulnerability scanning and penetration testing unless prior notification and approval from the Chief Information Officer or Information Security is obtained.
- 3.7.1.13** Executing any form of network monitoring which will intercept data not intended for the employee, unless prior approval from Information Security is obtained.
- 3.7.1.14** Circumventing user authentication or security of any IT Equipment, Ciena Network or user account, including the use of any other user's account.
- 3.7.1.15** Retrieving or reading any email messages for which they are not the intended recipient or using a password to retrieve any information unless authorized to do so. Notwithstanding the company's right to retrieve and read any e-mail messages, such messages should be treated as confidential by other employees.


### **3.8 Enforcement**

- 3.8.1** The Ciena IT Acceptable Use Acknowledgment Form Appendix A ([CO1-INF-26](#)) must be completed and signed by employees and Contractors who operate IT Equipment or make use of the Ciena Network.
- 3.8.2** It is expected that individuals who are Partner Employees or Consultants will be subject to the terms of this Ciena IT Acceptable Use Policy under the terms of the agreement between Ciena and the Partner Employee's employer, or between Ciena and the Consultant or the Consultant's employer.
- 3.8.3** Any employee found in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

### **3.9 Exception**

- 3.9.1** Compliance with this policy is expected for all Ciena employees, Contingent Workers and guests. If an Exception to this policy is required on the basis of a valid business justification, an Exception request must be sent to Information Security using the Information Security Exception Form ([CO4-INF-06](#)).

Unless otherwise specified, information shown on this document is proprietary and is not to be reproduced wholly or in part without the expressed permission of the Ciena Corporation. Before using, verify this copy is the correct revision by accessing the controlled document on the network.

	<b>CIENA IT ACCEPTABLE USE POLICY</b>		
	<b>Revision</b>	<b>Document Number</b>	<b>Page</b>
	E	CO1-INF-26	7 of 10

## A. Applicable and Reference Documents

Document Name	Document Number
INFORMATION SECURITY POLICY	<a href="#">CO1-INF-01</a>
CIENA IT PASSWORD POLICY	<a href="#">CO1-INF-02</a>
CIENA IT PASSWORD PROCEDURE	<a href="#">CO2-INF-20</a>
CIENA MOBILE DEVICE POLICY	<a href="#">CO1-INF-17</a>
CIENA CODE OF BUSINESS CONDUCT AND ETHICS	<a href="#">CO1-LEG-03</a>
INFORMATION SECURITY POLICY EXCEPTION FORM	<a href="#">CO4-INF-06</a>

## B. Standard and Reference Elements


Std / Req	Ref No./ Cycle	Description / Title	Relevant Paragraph Within This Document
N/A	N/A	N/A	N/A

## C. Definitions

Process Term / Acronym	Definition / Explanation
<i>Information Security</i>	The Ciena Information Security group is responsible for developing and implementing the information security program. Information Security will implement security policies, procedures and guidelines; conduct security awareness training; and co-ordinate a response to security incidents, suspected or actual breaches in the availability, integrity and confidentiality of Ciena data.
<i>Malware</i>	Short phrase for malicious software, is software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems. While it is sometimes software, it can also appear in the form of script or code.
<i>Cracking Applications</i>	Software or applications which enable the installation or use of features or applications without purchasing a license.

Unless otherwise specified, information shown on this document is proprietary and is not to be reproduced wholly or in part without the expressed permission of the Ciena Corporation. Before using, verify this copy is the correct revision by accessing the controlled document on the network.




	<b>CIENA IT ACCEPTABLE USE POLICY</b>		
	<b>Revision</b>	<b>Document Number</b>	<b>Page</b>
	E	CO1-INF-26	8 of 10

<i>Jail break Applications</i>	Software or applications that enable the use of features or a service from a service provider without purchasing the feature or service.
<i>Multifunction device</i>	Office machine which incorporates the functionality of multiple devices in one. A typical device may act as a combination of some or all of the following devices: Printer, Scanner, Photocopier, Fax, E-mail.
<i>Reimage/refresh</i>	To re-install a computer's operating system, and possibly other software, by writing a disk image to the hard disk, replacing the entire contents.
<i>Free and open-source software (FOSS)</i>	Software that gives users the right to use, copy, study, change and improve its design through the availability of its source code. FOSS is licensed and not necessarily free of charge.
<i>Data leakage</i>	Intentional or unintentional release of secure information to an un-trusted environment.
<i>Blog</i>	A blog is a journal published on the world wide web consisting of discrete entries on various topics of interest to masses.
<i>Security Scanning/Port Scanning</i>	Scanning for computer or network vulnerabilities/ scanning a computer's ports to identify open doors.
<i>IT</i>	The Ciena Information Technology group is responsible for providing IT Equipment and Network services to support customer business processes.
<i>IT Equipment</i>	IT Equipment may include, but is not limited to, computing devices (laptops and desktops), Mobile Devices and Tablets, Multifunction devices such as Printers, Copiers, Modems and Fax machines, which are owned by Ciena.
<i>IT or Ciena Network</i>	IT or Ciena Network is the private corporate network of Ciena which has specific sub-networks for employees, Contingent Workers, guests, applications and data.
<i>Service Desk</i>	Ciena's IT Service Desk is the central point of contact for IT service incidents and requests. The Service Desk can be contacted at 1-410-694-5888 and <a href="https://ciena.service-">https://ciena.service-</a>


Unless otherwise specified, information shown on this document is proprietary and is not to be reproduced wholly or in part without the expressed permission of the Ciena Corporation. Before using, verify this copy is the correct revision by accessing the controlled document on the network.



	<b>CIENA IT ACCEPTABLE USE POLICY</b>		
	<b>Revision</b>	<b>Document Number</b>	<b>Page</b>
	E	CO1-INF-26	9 of 10

	<a href="http://now.com/ess/">now.com/ess/</a> .
<i>Contingent Worker</i>	Means a Contractor, Consultant or Partner Employee.
<i>Contractor</i>	Persons engaged through a Statement of Work generally hired through an outside vendor for a specific project or for a specific period of time. The Contractor performs work intended to provide staff augmentation, to replace an employee on leave, or to provide additional resources based on cyclical or seasonal workforce needs.
<i>Consultant</i>	Persons engaged by Ciena to perform a specific task – limited in scope and duration – which is outside the key aspects of Ciena's regular business. Consultants are usually employed by a consulting firm or similar entity which has entered into a contractual relationship with Ciena to perform services outside of Ciena's areas of expertise. They do not perform work that is "substantially similar" to work performed by Ciena employees.
<i>Partner Employee</i>	Persons engaged by Ciena to perform tasks which may be – but are not necessarily – within the key aspects of Ciena's regular business. Partner Employees are engaged by Ciena indirectly, as a result of their employment by a company which has entered into a contractual relationship with Ciena to perform certain services. They do not perform work that is "substantially similar" to work performed by Ciena employees.

Unless otherwise specified, information shown on this document is proprietary and is not to be reproduced wholly or in part without the expressed permission of the Ciena Corporation. Before using, verify this copy is the correct revision by accessing the controlled document on the network.

	<b>CIENA IT ACCEPTABLE USE POLICY</b>		
	<b>Revision</b>	<b>Document Number</b>	<b>Page</b>
	E	CO1-INF-26	10 of 10

## APPENDIX A

### ACKNOWLEDGEMENT OF CIENA IT ACCEPTABLE USE POLICY

The Ciena IT Acceptable Use Acknowledgment Form must be completed and signed by employees and Contingent Workers who operate IT Equipment or make use of the IT Network. This form acknowledges that the employees or contractors have reviewed the Ciena IT Acceptable Use Policy [CO1-INF-26](#). The Ciena IT Acceptable Use Policy [CO1-INF-26](#) outlines the acceptable use of Ciena's IT Network and IT Equipment. Inappropriate use of Ciena's IT Network or IT Equipment may expose Ciena to risks such as malware attacks, data loss, compromise of systems and services, and legal and reputational issues.

I hereby confirm that I have received, read and understood the CIENA IT ACCEPTABLE USE POLICY [CO1-INF-26](#), and agree to abide by all statements within the document. I also understand that policy violations will be enforced by Ciena including disciplinary action up to and including termination of employment or contract.

Name: \_\_\_\_\_

Print Your Name

Signature: \_\_\_\_\_

Sign Your Name

Date: \_\_\_\_\_

Unless otherwise specified, information shown on this document is proprietary and is not to be reproduced wholly or in part without the expressed permission of the Ciena Corporation. Before using, verify this copy is the correct revision by accessing the controlled document on the network.

UNCONTROLLED IF STORED OUTSIDE REPOSITORY OR PRINTED

DOCUMENT TEMPLATE CO4-QSG-07 – REV: D