 User Guidelines for Wireless Access	Guidelines No.	ITS-1015-G	Rev:	A
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Interim Issued:	11/27/07	Effective:	11/27/07
	Page 1 of 4			

1 Purpose

Wireless access to the campus network is provided as a convenience to students, faculty, staff, and sponsored guests. These guidelines are intended to help users meet the University's accepted standards for such access, and apply to all wireless communication devices/equipment, such as computers, laptops, notebooks, cellular phones, personal digital assistants (PDAs), and any other form of wireless communication device capable of transmitting data.

2 Definitions

Access Point (also known as a Hotspot): "A hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired Local Area Network (LAN)." (Source: 2006. <<http://www.webpedia.com>>) Access points act as central transmitters and receivers of wireless LAN radio signals.

Encrypted Connection: Data transmitted "in the air" (i.e., to and from your computer and the access point) that is scrambled such that unauthorized individuals are prevented from discerning it.

Integrity Check: An assessment performed to verify that the user's operating system and anti-virus definitions meet the minimum standards set by the University.

Revenue Generating Organization: A revenue-generating entity that is not a state-funded institution or organization, but that is funded by grants or charges fees to the University to operate. Examples of revenue generating organizations include: UAS, ASI, Student Union, Continuing Education, Reprographics, and the Campus Bookstore.

Unencrypted Connection: Clear text data transmitted "in the air" (i.e., to and from your computer and the access point). Data transmitted "in the air" without encryption can be easily snooped and captured.


Wireless Access: A connection that allows a computer or device to access a network as if it were connected to the network with a cable plugged into a jack.

Wireless Guest Account: A temporary sponsored account that gives guest users access to the Internet.

3 Guidelines

3.1 Appropriate Use for Wireless Access

- a) Students, faculty, staff, and sponsored guests are expected to comply with all laws, policies, and user guidelines that govern access to and use of the University's networks, accounts, and data.
- b) All communication using campus networks must be appropriate, ethical, professional, and lawful.
- c) All signed Certifications of Appropriate Use, Acknowledgements of Confidentiality, and Appropriate Use of Account statements apply to wireless access to campus networks.
- d) Unauthorized peer-to-peer file sharing of copyrighted works, including music, pictures, movies, games, and other published copyrighted materials is prohibited.
- e) Unauthorized access points and wireless devices are prohibited.

 User Guidelines for Wireless Access	Guidelines No.	ITS-1015-G	Rev:	A
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Interim Issued:	11/27/07	Effective:	11/27/07

Page 2 of 4

- f) Use of a wireless device to form a bridge (connection) or act as a hub between the University's wired and wireless networks is prohibited.
- g) Unauthorized access to a campus network is prohibited.

3.2 Minimum Requirements and Standards for Wireless Access

- a) All users must have a network account or a wireless guest account. Applications for network and wireless guest accounts are located online at <http://www.calstatela.edu/its/forms> under the Network/E-mail and Wireless topics, respectively.
- b) Computers and laptops must have:
 - One of these operating systems:
 - i. Windows XP with Service Pack 2 (SP2) or higher
 - ii. Windows 2000 with Service Pack 3 (SP3) or higher
 - iii. Macs: OSX or higher
 - Anti-virus software with anti-virus definitions dated within 8 days of logging into the campus network
 - A wireless card standard that is 802.11b or 802.11g compliant
- c) For an encrypted connection, the wireless transceiver must support WPA encryption and must be properly configured (WPA2 is preferred).

NOTE

Machines that do not meet operating system, anti-virus, and encryption requirements and standards will be restricted to an open (unencrypted) wireless connection to the Internet.


3.3 Wireless Guest Accounts

- a) Guest accounts must be sponsored; they must be requested by positions with fund authority at the level of associate dean, dean, director, or above. Requests for guest accounts from students, faculty, and staff must be made through a sponsor.
- b) Sponsors must request guest accounts using the Wireless Guest Account Request form, available online at <http://www.calstatela.edu/its/forms> under the Wireless topic.
- c) Guest accounts may be requested for a minimum of one day up to a maximum of seven consecutive days, including extensions.

NOTE

Temporary staff, consultants under contract with the University, or individuals requiring access for more than seven days should not request a wireless guest account. Instead, they submit a Network/E-mail Account Request, available online at <http://www.calstatela.edu/its/forms> under the Network/E-mail topic.

- d) Guest accounts for revenue generating organizations must have the sponsor's and the fiscal officer's approval.
- e) Revenue generating organizations will be charged ten dollars (\$10.00) per day for each guest account requested. A billing statement will be sent to the fiscal officer.

 User Guidelines for Wireless Access	Guidelines No.	ITS-1015-G	Rev:	A
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Interim Issued:	11/27/07	Effective:	11/27/07

Page 3 of 4


- f) The sponsor or named designee must submit the completed and approved request form in person to the ITS Help Desk (LIB PW Lobby) at least two hours before the desired account activation time. Guest accounts will be processed when the request form is submitted.
- g) To extend a guest account, the sponsor, designee, or revenue generating organization's fiscal officer must e-mail the ITS Help Desk at helpdesk@calstatela.edu with the guest user ID(s) and the number of extension days requested. The ITS Help Desk will e-mail a reply after processing the extension request.
- h) Sponsors are responsible for ensuring that guests understand and comply with the University's appropriate use policy. Sponsors must have their guests sign and date the Appropriate Use of Account agreement contained on page 2 of the Account Information Sheet(s), which is given to the sponsor or designee at the time the account(s) is/are picked up at the ITS Help Desk.
- i) Sponsors must return a copy of all signed and dated Appropriate Use of Account agreements to the ITS Help Desk on the day that they distribute the account(s) to their guests.
- j) Guest access bandwidth is limited to 2 megabytes.
- k) Guest account access, whether encrypted or not, is restricted to the Internet only.

3.4 Wireless Security Tips

- a) Configure your laptop settings for optimum security.
- b) Enable a software firewall. [Note: Windows XP and Mac OS X both provide a built-in firewall.]
- c) Disable your laptop's guest account feature.
- d) Disable auto-login.
- e) Disable save password functions.
- f) Prevent user names from being displayed at login, or after logging off and restarting your computer.
- g) Do not store passwords, PINS, and other sensitive or confidential information on your computer.
- h) Do not set your device up as an ad-hoc network that allows other devices to connect to it.
- i) Disable your wireless card when you are offline.
- j) Use secure websites (https://) when entering user IDs, passwords, PINs, credit card numbers, or other financial or confidential information.
- k) See the **Are You Secure?** website at <http://www.calstatela.edu/itsecurity> for more tips.

4 Terms, Conditions, and Sanctions

- a) The wireless system performs an integrity check to verify that machines meet the requirements and standards outlined in section 3.2. Machines found to be out of compliance will not be allowed wireless access.
- b) Computers exhibiting suspicious activity indicative of an intrusion or other unauthorized activity will be disconnected from the network.

 User Guidelines for Wireless Access	Guidelines No.	ITS-1015-G	Rev:	A
	Owner:	IT Security Management and Compliance		
	Approved by:	Peter Quan, VP ITS and CTO		
	Interim Issued:	11/27/07	Effective:	11/27/07
	Page 4 of 4			

- c) Inappropriate or unauthorized actions that jeopardize campus resources will be reported to the University Counsel, Human Resources Management, and the appropriate vice president for review and possible disciplinary and legal action as provided by statute.
- d) Before downloading or uploading uncopyrighted works, users should obtain permission from the copyright holder. Illegal downloading and uploading may carry significant monetary and criminal sanctions.
- e) Users should have no expectation of privacy when connected to a campus network. Using a campus network constitutes consent to monitoring, retrieval, and disclosure for any purpose, including criminal prosecution, of any information stored on the network or locally on a hard drive or other media in use with a campus network or computing resource.
- f) Using a campus network or computing resource constitutes agreement to abide by University policies, user guidelines, and confidentiality agreements. Violations may result in the revocation of University computing resource privileges.
- g) All University employees are subject to California Government Code section 8314, which prohibits the use of public resources for unauthorized purposes, and California Penal Code sections 502 and 502.01, which deal with unauthorized access to computers, computer systems, and computer data.

5 Contacts and Resources

- a) To report a lost or stolen laptop or electronic storage device, contact University Police at (323) 343-3700, Building C.
- b) For technical support, contact the ITS Help Desk (LIB PW Lobby) at extension (323) 343-6170, or e-mail helpdesk@calstatela.edu.
- c) For general information and answers to frequently asked questions (FAQ) about campus wireless services, see <http://www.calstatela.edu/wireless>.
- d) Questions regarding these guidelines should be directed to ITSecurity@calstatela.edu.
- e) Links to relevant laws, policies, and user guidelines are available on the ITS Guidelines and Policies website at: <http://www.calstatela.edu/its/policies>.

6 Related Documents

ID/Control #	Title
AP 709	Computer Center Accounts
ITS-2804	Lost or Stolen Computer or Electronic Storage Device Report form
ITS-8808	Network / E-mail Account Request
ITS-8813	Student Application for Network Information Services (NIS) Account
ITS-1001-G	User Guidelines for Network Traffic Management
ITS-1000-G	User Guidelines for E-mail and Electronic Communications
ITS-1007-G	User Guidelines for Laptop Security
ITS-1005-G	User Guidelines for Portable Electronic Storage Media
ITS-1008-G	User Guidelines for Reporting a Lost or Stolen Computer or Electronic Storage Device
ITS-4815	Wireless Guest Account Request