User Guidelines for Wireless Access				
	Guideline No	ITS-1015-G	Rev	C
	Owner	IT Security and Compliance		
	Approved by	Sheryl Okuno, Director IT Security and Compliance		
	Issued	2-18-09	Revised	5-17-17
				Page 1 of 6

Table of Contents

User Guidelines for Wireless Access				
	Guideline No	ITS-1015-G	Rev	C
	Owner	IT Security and Compliance		
	Approved by	Sheryl Okuno, Director IT Security and Compliance		
	Issued	2-18-09	Revised	5-17-17
				Page 2 of 6

1. Purpose

Wireless access to the University 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, tablets, cell phones and any other form of wireless communication device capable of transmitting data.

2. Related California State University Policies and Standards

The following documents of the latest issue in effect represent the criteria against which University information security audits shall be based and shall apply to the extent specified herein. Standards provide detailed supporting and compliance information for policies.

ID/Control #	Description	Title
8045.0	**Policy**	**Information Technology Security**
8045.S200	*Standard*	*Malicious Software Protection*
8045.S302	*Standard*	*Remote Access to CSU Resources*
8045.S400	*Standard*	*Mobile Device Management*
8050.0	**Policy**	**Configuration Management**
8050.S200	*Standard*	*Configuration Management – High Risk/Critical Workstation*
8060.0	**Policy**	**Access Control**

In support of the CSU policies and standards, the University publishes **standards** (define the minimum requirements necessary to meet CSU policy) and **user guidelines** (provide general recommendations and instructions for users to comply with the policy). These supporting documents are available on the IT Security website under the policy title noted above.

3. Entities Affected by These Guidelines

All students, faculty, staff, affiliates and sponsored guests are expected to comply with these guidelines.

4. Definitions

a. 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.

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

c. 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.

d. 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, University-Student Union, College of Professional and Global Education and the University Bookstore.

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

f. 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.

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

5. Guidelines

5.1 Appropriate Use for Wireless Access

Students, faculty, staff and sponsored guests are expected to comply with all laws, policies, standards and user guidelines that govern access to and use of the University's networks, accounts and data.

All communication using University networks must be appropriate, ethical, professional and lawful.

All signed Certifications of Appropriate Use, Acknowledgements of Confidentiality, and Appropriate Use of Account statements apply to wireless access to University networks.

Unauthorized peer-to-peer file sharing of copyrighted works, including music, pictures, movies, games and other published copyrighted materials is prohibited.

Unauthorized access points and wireless devices are prohibited.

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.

Unauthorized access to a University network is prohibited.

5.2 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 "Networking" heading.

b. Computers and laptops must have:

- One of these operating systems:
  i. Windows 7 with Service Pack 2 (SP2)
  ii. Windows 10
  iii. Macs OS 10.12, OSX 10.8 or higher
- Anti-virus software with anti-virus definitions dated within 8 days of logging into the network
- A wireless card standard that is 802.11ac or 802.11g/b/n compliant

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.

5.3 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/Email Account Request, available online at http://www.calstatela.edu/its/forms under the Network/Email 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.

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 email the ITS Help Desk at helpdesk@calstatela.edu with the name of the original requestor(s), guest user ID(s) and the number of extension days requested. The ITS Help Desk will email 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 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.

5.4 Wireless Security Tips

a. Configure your laptop settings for optimum security.

b. Enable a software firewall. [Note: Windows 7, Windows 10, Mac OS and OS X have 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.

6. Contacts

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 (323) 343-6170, or email helpdesk@calstatela.edu.

c. For general information and answers to frequently asked questions (FAQ) about 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, standards and user guidelines are available on the ITS Guidelines and Policies website at: http://www.calstatela.edu/its/policies.

7. Applicable Federal and State Laws and Regulations

Federal	Title
Family Educational Rights and Privacy Act (FERPA)	**Family Educational Rights and Privacy Act (FERPA)** http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html This is a federal law that protects the privacy of student education records.
State	**Title**
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.8** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that, as amended by SB 1386 (2003), AB 1298 (2007) and SB 24 (2011), provides information on safeguarding personal information, requires notification to California residents whose personal information was or is reasonably believed to have been acquired by unauthorized individuals and requires notification to the Attorney General if more than 500 residents are involved.