CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject:	**Remote Access Policy**		
Department:	**Information Technology Services**	Reference No.:	
Division:	**Administration and Finance**	Issue Date:	**March 2010**
References:	•	Revision Date:	**N/A**
Web Links:	• **http://daf.csulb.edu/forms/its/procedures**	Expiration Date:	**N/A**

I. PURPOSE

The purpose of this policy is to define standards for connecting to the California State University, Long Beach (CSULB) network from any remote host, untrusted host, and remote network. These standards are designed to minimize the potential exposure to the University from damages that may result from unauthorized access to CSULB's administrative network through a non-CSULB controlled network, device, or medium. Damages include the loss of confidential or internal use data, intellectual property, damage to public image, or damage to critical CSULB computing network and information systems.

II. SCOPE

This policy applies to:

- All users of Information Technology (IT) systems and resources, including but not limited to CSULB students, faculty and staff;
- All systems, networks, and facilities administered by Information Technology Services (ITS) and individual colleges, departments, units, and other University-based entities;
- All equipment used to connect to the CSULB network, including but not limited to photocopy machines, small portable hard drives, flash memory cards, handheld communication devices and privately owned devices not managed or maintained by CSULB.
- Remote access connections used to do work on behalf of CSULB or personal business, including but not limited to, reading or sending e-mail and viewing web resources.

III. POLICY STATEMENT

All individuals using information technology devices connected to the CSULB network are required to manage the security of those devices in accordance with the CSULB information security policy and standards including, but not limited to, security standards for desktops, servers, authentication/passwords, data, applications and middleware.

All individuals accessing CSULB confidential or internal use data from a non-campus location, or transporting such data off-campus on electronic devices, must be authorized to do so and must comply with all University ITS security standards.

IV. COMPLIANCE

Any person found to have violated this policy may have their remote network access privileges temporarily or permanently revoked.