California Western School of Law
Remote Access Policy

Updated July 2014

1.0 Overview

It is often necessary to provide access to CWSL information resources to employees or others working outside the school's network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.

2.0 Purpose

This policy is provided to define standards for accessing CWSL information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium.

3.0 Scope

The scope of this policy covers all employees, contractors, and external parties that access school resources over a third-party network, whether such access is performed with school-provided or non-school-provided equipment.

4.0 Policy

4.1 Prohibited Actions

Remote access to CWSL systems is only to be offered through a school-provided means of remote access in a secure fashion. The following are specifically prohibited:

- Installing a modem, router, or other remote access device on a school system without the approval of the IT Executive Director.

- Use of non-school-provided remote access software except for vendors who may have their own remote software. All outside the school community must have a non-disclosure document on file before remote access is granted by IT.

- Split Tunneling to connect to an insecure network in addition to the CWSL network, or in order to bypass security restrictions.

4.2 Use of non-school-provided Machines

Use of non-school-provided machines to access the CWSL network is permitted as long as this policy is adhered to and the user exercises discretion.

4.3 Client Software

The school will supply users with remote access software that allows for secure access and enforces the remote access policy. The software will provide traffic encryption in order to protect the data during transmission as well as a firewall that protects the machine from unauthorized access.

4.4 Network Access

The level of access will not exceed the access a user receives when working in the office.

4.5 Idle Connections

Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to the school's network must be timed out after 2 hour of inactivity.

4.6 Applicability of Other Policies

This document is part of the school's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the Executive Director of IT and/or the Cabinet. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of school property (physical or intellectual) are suspected, the school may report such activities to the applicable authorities.

6.0 Definitions

Modem A hardware device that allows a computer to send and receive digital information over a telephone line.

Remote Access The act of communicating with a computer or network from an off-site location. This is often performed by home-based or traveling users to access documents, email, or other resources at a main site.

Split Tunneling A method of accessing a local network and a public network, such as the Internet, using the same connection.

Timeout A technique that drops or closes a connection after a certain period of inactivity.