Remote Access Connection Procedure & Agreement

1. Purpose

The purpose of this Procedure is to define standards, procedures, guidelines, and restrictions for connecting to LRCCD's private internal network(s) from any external host(s) via remote access connection technologies. A remote access connection is a secured private network connection built on top of a public network, such as the Internet. Remote access technologies provide a secure, encrypted connection, or tunnel, over the Internet between an individual computing device and a private network (such as the LRCCD private network). LRCCD's resources (i.e. public and private networks, systems, network hardware and appliances, computing assets, databases, file stores, district data, etc.) must be protected from unauthorized use and/or malicious attack that could result in system unavailability, loss of information, damage to critical applications, loss of revenue, harm to our students, or harm to our public image. Therefore, for all LRCCD employees and agents, any remote access or mobile privileges that allow access to LRCCD private resources MUST employ only LRCCD approved connection methods.

2. Scope

This Procedure applies to all LRCCD employees, including full-time staff, part-time staff, contractors, freelancers, and other agents who utilize district-owned or personally-owned computers to remotely access LRCCD private network resources. This procedure is NOT intended to restrict or otherwise limit Internet access to LRCCD's web enabled public network resources (College or District Websites) and/or web enabled private network resources (Outlook Web Access). This procedure is intended to restrict access to LRCCD's secure private network resources from any computing device connected to and/or communicating through any non-LRCCD network link.

Any and all work performed for LRCCD on said computers by any and all employees, through a remote access connection of any kind, is covered by this Procedure. Work can include (but is not limited to) e-mail correspondence, system inspection, maintenance, or troubleshooting, Web browsing, utilizing intranet resources, and any other district application used over the Internet. Remote access is defined as any Connection to any LRCCD private network and/or other secure network applications from off-site locations, which include but are not limited to, the employee's home, a hotel room, an airport, café, satellite office, wireless device, etc. Connections that qualify as remote access connections covered by this procedure include but are not limited to Internet dial-up modems, cable modems, DSL, ISDN, frame relay, VPN, SSH, proprietary remote access/control software, etc.

3. Supported Technology

All remote access will be centrally managed by LRCCD's District Office Information Technology Department (DOIT) and will utilize encryption and strong authentication measures. Any device connecting to any LRCCD network remotely must have currently supported operating systems patched with current security patches. Unpatched systems may be denied access to LRCCD resources.

4. Eligible Users

All employees requiring the use of remote access for business purposes must go through an application process that clearly outlines what access is required, why that access is required and what level of service the employee needs should his/her application be accepted. Application forms must be approved and signed by the employee's unit manager, supervisor, or department head before submission to DOIT.

Employees may use privately owned connections (under 'Supported Technology') for business purposes. If this is the case, DOIT must approve the connection as being secure and protected. However, DOIT cannot and will not technically support a third-party ISP connection or hotspot wireless ISP connection. All expense forms for reimbursement of cost (if any) incurred due to remote access for business purposes (i.e. Internet connectivity

charges) must be submitted to the appropriate unit or department head. Financial reimbursement of costs associated with employee use of remote access technologies is not the responsibility of DOIT.

5. Regulation and Appropriate Use

It is the responsibility of any employee of LRCCD with remote access privileges to ensure that their remote access connection remains secure. It is imperative that any remote access connection used to conduct LRCCD business be utilized appropriately, responsibly, and ethically. Therefore, the following rules must be observed:

1. General access to the Internet by remote users through LRCCD's network is permitted. However, both the employee and his/her family members using the Internet for recreational purposes through district networks are not to violate any of LRCCD's Computer Use Policies or Regulations (See Section 7. Below - P8871 and R8871).

2. Employees will use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with LRCCD's password Regulation (R8871). Employees agree to never disclose their passwords to anyone, particularly to family members if business work is conducted from home.

3. All remote computer equipment and devices used for business interests, whether personally-owned or district-owned, must display reasonable physical security measures and use currently supported software with up to date patch levels. Computers will also have active antivirus software installed and updated with current antivirus definitions.

4. Remote users using public hotspots for wireless Internet access must employ for their devices a district-approved personal firewall, VPN, and any other security measure deemed necessary by DOIT. VPNs supplied by the wireless service provider may also be used, but only in conjunction with LRCCD's additional security measures.

    - Hotspot and remote users must disable or disconnect wireless cards when not in use in order to mitigate attacks by hackers, wardrivers, and eavesdroppers.
    - Users must apply new passwords every business/personal trip where district data is being utilized over a hotspot wireless service, or when a district device is used for personal Web browsing.

5. Any remote connection that is configured to access LRCCD resources must adhere to the authentication requirements of DOIT. In addition, all hardware security configurations (personal or district-owned) must be approved by DOIT.

6. Employees, contractors, and temporary staff will make no modifications of any kind to the remote access connection or install any remote control or file-sharing software without the express approval of DOIT. This includes, but is not limited to, split tunneling, dual homing, non-standard hardware or security configurations, etc.

7. Employees, contractors, and temporary staff with remote access privileges must ensure that their computers are not connected to any other network while connected to LRCCD's network via remote access, with the obvious exception of Internet connectivity.

8. In order to avoid confusing official district business with personal communications, employees, contractors, and temporary staff with remote access privileges must never use non-district e-mail accounts (e.g. Hotmail, Yahoo, etc.) to conduct LRCCD business without prior approval from DOIT.

9. No employee is to use Internet access through district networks via remote connection for any purpose that is inconsistent with district policies and regulations (See Section 7. Below), that violates any state or federal law, or that results in any form of obscene behavior or harassment of any kind.

10. All remote access connections must include a “time-out” system. In accordance with LRCCD’s security policies, remote access sessions will time out after [30] minutes of inactivity, and will terminate after [8] hours of continuous connection as appropriate. Both time-outs will require the user to reconnect and re-authenticate in order to re-enter district networks. Should a remote user’s account be inactive for period of [120] days, access account privileges may be suspended until DOIT is notified of the need to re-enable.

11. If a personally-owned or district-owned computer or related equipment used for remote access is damaged, lost, or stolen, the authorized user will be responsible for notifying their manager and DOIT immediately.

12. The remote access user also agrees to immediately report to their manager and to DOIT any incident or suspected incidents of unauthorized access to any electronic district resources, networks, databases, data, etc.

13. The remote access user also agrees to and accepts that his or her access and/or connection to LRCCD’s networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computer connections, monitoring will be done in accordance with P8851and R8851 and will focus on the identification of accounts/computers that may have been compromised by external parties.

6. Regulation Non-Compliance

Failure to follow this Remote Access Procedure, comply with District Policies and Regulations, or failure to comply with relevant state or federal law may result in the suspension or removal of remote access privileges, disciplinary action, and possible termination of employment.

7. Relevant LRCCD Policy & Regulation Reference

LRCCD Policy numbers as follows: P8811, P8831, P8841, P8851, P8861, P8871, P8881

LRCCD Regulation numbers as follows: R8811, R8831, R8851, R8871

Please pay special attention to **P8871** and **R8871** to ensure compliance.

Employee Declaration, Approval and Signed Agreement

The Employee Declaration is on the next page of this document.

Business Requirement

Justification: _____

Employee Declaration

I, _____, have read and understand the above Remote Access
(Print Name)
Procedure and Agreement, and consent to adhere to the rules outlined therein.

_____ _____
Employee Signature Date

Approval

_____ _____
Supervisor/Manager Signature Date

_____ _____
Vice President of Administration Date

_____ _____
ISO Signature Date

Remote Access Connection Granted

_____ _____
Network Security Administrator Date

Remote Access Information:

Remote Access User Information:

First Name: _____ Last Name: _____Location: _____

Emplid #: _____ ☐ Permanent Staff ☐ Class. Temp. ☐ Other: _____

Section 1: Equipment Ownership (Device used to connect to VPN.)

Check all that apply:

☐ District Issued ☐ Non-District Issued

Section 2: Equipment Type (Device used to connect to VPN.)

Check all that apply:

☐ Mac ☐ PC (Windows)