LOS RIOS
COMMUNITY
COLLEGE
DISTRICT

American River College
Cosumnes River College
Folsom Lake College
Sacramento City College

1919 Spanos Court
Sacramento, CA 95825
Phone: 916 568-3021
Fax: 916 568-3023
www.losrios.edu

July 6, 2016

TO: Vice Presidents of Administration
District and College IT Managers

SLL

FROM: Sue Lorimer, District-wide Information Security Officer (DWISO)

SUBJECT: Protocol to Respond to Compromised Devices on the Los Rios Network

The Los Rios District Office Information Technology (DOIT) department is responsible for the security of the district's network, including responding to compromised devices. A compromised device is one that is no longer fully under Los Rios' control such that another person or entity partially or fully controls the device and may use it to gain access to protected data, attack other devises internal/external to the Los Rios network, send out spam emails, or engage in other harmful activities. Compromised devices can be identified via DOIT security scanning tools or reported to the district by a trusted outside organization (e.g. FBI, REN-ISAC, etc).

Federal and state statues require the notification of affected individuals where there is a reason to believe that legally protected data held by or for Los Rios may have been acquired by unauthorized personnel. Therefore, the district is establishing a protocol to **immediately** remove compromised devices from the network to protect data privacy, other Los Rios computers, and Los Rios' reputation. Immediate network disconnection is required to stop the attack from continuing and prevent additional damage. The protocol is as follows:

1. Once a compromised device is identified anywhere on the Los Rios network that is determined to have access to protected data or is positioned within the same network that stores protected data, DOIT will immediately remove the device from the network.

2. DOIT will then immediately notify the appropriate college or district staff, including IT staff, of the disconnection and work with the appropriate staff to restore the device once it is no longer compromised.

3. The District-wide ISO, in consultation with DOIT and the affected site ISO, will determine if a data breach has occurred which will require implementation of the Los Rios Data Breach Notification Procedures and will implement those procedures as necessary.

NOTE: All members of the Los Rios community are responsible for promptly reporting suspected or known security incidents via the Information Security Incident Form (http://www.losrios.edu/lrc/infosecurity.php). College ISOs are responsible to follow-up on all reported incidents.

Cc: District and College ISOs