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

February 7, 2014

TO: Chancellor's Executive Staff, District and College Information Security Officers, Associate Vice Chancellor of Information Technology, and College IT Deans

FROM: Sue Lorimer, District-wide Information Security Officer

SUBJECT: Los Rios CCD Data Breach Notification Procedures

The procedures provided below detail what needs to be done in the case of a suspected data breach at any college or district site. Please make sure individuals at your site know who your local Information Security Officer (ISO) is and how to report suspected breaches.

Please contact me if you have any questions or concerns. Thank you.

Cc: College Vice Presidents, District IT Directors, Emmie Oesterman, Chief Sears

Los Rios Community College District
Data Breach Notification Procedures

The Data Breach Notification Triggering Information includes:

1. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are **not encrypted**: *Cal. Civ. Code Section 1798.82(h)*
    i. Social security number.
    ii. Driver's license number or California Identification Card number
    iii. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
    iv. Medical information.
    v. Health insurance information.
2. A user name or email address, in combination with a password or security question and answer that would permit access to an online account. *Cal. Civ. Code Section 1798.82(h)*
3. Any other data that would cause severe damage to the District if disclosed. *Information Security R-88713.1.1.1.*

A. Internal Notifications

If after investigation the site (college or District) Information Security Officer (ISO) determines that a security breach involving notice triggering information has or is reasonably believed to have occurred, he/she will immediately notify the District-Wide (DW) ISO and the college President. The DW ISO will notify the General Counsel, and appropriate District administrator (Deputy Chancellor/Chancellor).

B. Press Notification

If it is determined that a breach is of a magnitude that may require a press release, the DW ISO shall notify the Associate Vice Chancellor of Communications and Media Relations. With the exception of the Associate Vice Chancellor of Communications and Media Relations, neither college nor District personnel are authorized to speak on behalf of the District to media personnel or representatives of other outside agencies. All media inquiries or other public affairs inquiries should be directed to Associate Vice Chancellor of Communications and Media Relations.

C. External Agencies Notification

1. Credit card/debit card information: If it is determined after investigation that a security breach involving credit/debit card information has or is reasonably believed to have occurred, the DW ISO will notify the Associate Vice Chancellor of Finance. The Associate Vice Chancellor of Finance will directly notify the appropriate merchant bank(s):

    a. Within three (3) business days of the breach to provide an Incident Report document, and
    b. Within ten (10) business days to provide a list of all potential compromised accounts. *PCI data breach requirements.*

2. If more than 500 California residents are notified as a result of a single breach incident, the DW ISO will submit a sample copy (without any identifiable information) of the notice to the Attorney General. *Cal. Civ. Code Section 1798.29(f)*

D. Affected Individuals Notifications

The site ISO (college or district) in conjunction with the department responsible for controlling access to, and security of, the breached electronic devices (i.e., USB, server, laptop, etc.) will compile the list of the names of the individuals whose personal information was or is reasonably believed to have been compromised. The site ISO will coordinate with the DW ISO to send the notification to the affected individuals.

E. Notification Timing

Individuals whose notice-triggering information has been compromised shall be notified in the most expedient time possible and without unreasonable delay. Notice to individuals may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation or in order to take measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. *Cal. Civ. Code Section 1798.29 (a) & (c)*

F. Content of Notification

The breach notification will provide at the minimum all the following information:

1. The name and contact information for inquiries.
2. A list of the types of personal information that were or are reasonably believed to have been compromised.
3. If possible to determine, the date of the breach, the estimated date of the breach, or the date range within which the breach occurred, and the date of the notice.
4. If the notification was delayed due to law enforcement investigation.
5. A general description of the breach incident.
6. The toll free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number, driver's license, or California identification card number.

If the DW ISO in consultation with the General Counsel, Associate Vice Chancellor of Communications and Media Relations, and Associate Vice Chancellor of Finance, determines the college or District needs to purchase credit monitoring services for those affected or potentially affected by the breach, the DW ISO will work with District General Services to obtain the monitoring and will provide the information on how to access the monitoring to the individuals responsible for writing the notification message.

Cal. Civ. Code Section 1798.29 (d)

G. Method of Notification

The breach notification letter will be printed on official college/District letterhead and mailed to the individual at the last recorded home address. If only an email address is known, a breach notification email will be sent to the last recorded email address available to the District. Any notices returned with address forwarding information will be re-sent by the responsible college/District.

If more than 500,000 individuals are affected, or if the cost of providing notice will exceed $250,000, or if there is insufficient contact information, the following substitute notification procedures will be followed:

- Notices will be emailed to all affected individuals whose emails are known.
- The breach notice will be conspicuously posted on the District website*.
- Major statewide media and the Office of Information Security within the California Technology Agency will be notified.

*After six month period of time the General Council and the DW ISO will determine if additional website posting time is necessary.

Cal. Civ. Code Section 1798.29 (i)

H. Breach Notification Inquiry Response

The DW ISO and the Associate Vice Chancellor of Communications and Media Relations will provide a written *inquiry response guide* to be used by the college and/or District to respond to any phone calls, emails, letters, or walk-in-traffic inquiries regarding the breach.