LEWIS-CLARK STATE COLLEGE

DATA BREACH CHECK LIST

1) Notify one's immediate supervisor. The immediate supervisor and the person issuing the notice will coordinate communication with the appropriate vice president (units reporting directly to the president should include the Vice President for Finance and Administration in the notice),
2) The vice president will notify the President, the Director of Information Technology, the Office of Risk Management, the Executive Cabinet, and Director of Communications and Marketing.

    a. The Director of Communications and Marketing begins formulating a public relations strategy (primarily a response/statement) in case the breach goes public and media members begin to inquire. This public relations work is to begin in step 2 and be further refined as more information becomes available from steps 3-5.

    b. The Registrar's office notifies students within the Policy timeline.

    c. Financial Aid reports a breach via email to cpssaig@ed.gov. The email should include info listed from i to vi. If email is unavailable call the Department's security operations center (EDSOC) at 202-245-6550 to report this data. EDSOC operates 24 hours a day, seven days per week.

        i. date of the breach (known or suspected),
        ii. impact of the breach (number of records, number of students, etc.),
        iii. method of the breach (hack, accidental disclosure, etc.),
        iv. information security program point of contact (email address and phone number are required),
        v. remediation status (complete, in-process, etc. with detail), and
        vi. next steps (as needed).

3) The Office of Risk Management will work with third-party partners, including other state agencies, cyber insurance and breach coaches to coordinate the college's response to the people whose data was compromised. In cases of cyber-based data breaches, the Director of Information Technology will coordinate the development and distribution of an incident report in cooperation with the Office of Risk Management.
4) Cyber insurance provided by the Idaho State Office of Risk Management will contract with a third party vendors to prepare and distribute notifications to the people whose data was compromised.
5) The Office of Risk Management will advise the executive cabinet and impacted departments on additional steps they are required to take in response to the data breach.