209-02 DATA BREACH NOTIFICATION—PROCEDURE

1. PURPOSE

Confidential personal information compromised by a security breach may lead to identity theft and invasion of privacy for affected individuals. Coconino Community College (CCC) may be required by law to take specific action in the event of a breach to the confidentiality of such information.

2. PROCEDURE

CCC will abide by the State of Arizona statute 44-7501: Notification of breach of security system; enforcement; civil penalty; preemption; exceptions; definitions.

1. "Covered Information" or "Personal Information" are used interchangeably—sensitive, non-public, personally identifiable information of an individual. These include, but are not limited to:
    a. An individual's name (first name or first initial and last name), or phone number, or address, in conjunction with any of the following data elements:
        1. social security number
        2. credit and debit card information
        3. income and credit history
        4. bank account information
        5. driver's license number
        6. tax return
        7. asset statement
    b. Any number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account.
    c. Covered Information includes both paper and electronic records.

2. The following safeguards must be implemented by offices which maintain or handle Covered Information:
    a. Require all employees to immediately notify their supervisor of any actual or suspected security breach involving files containing Personal Information. For example, a breach may involve a lost or stolen computer or other device containing unencrypted Covered Information or the access of Personal Information by unauthorized individuals. If employees are uncertain whether there has been a breach, they must be advised to report the event to their supervisor.
    b. Regularly train employees, including all temporary, contract, or work-study employees, to take basic steps to maintain the security, confidentiality and integrity of personal information, such as:
        1. locking rooms and file cabinets where paper records are kept
        2. using password-activated screensavers

3. using unique passwords (non-dictionary words and/or number combinations)
4. changing passwords periodically and not posting passwords on employees' computers
5. never sharing passwords with others
6. encrypting personal information when it is transmitted electronically over networks or stored on-line
7. referring calls or other requests for personal information to designated individuals within the department, college Registrar, or human resources
8. requiring all third-party vendors/contractors having access to Covered Information to exercise reasonable care in the handling of Personal Information and to implement commercially reasonable policies, procedures and systems to protect the confidentiality, security, and integrity of personal information and to detect the occurrence of a data breach. This requirement must be imposed on the third-party by a written provision in a contract.

3. If a data breach has occurred or is suspected, supervisors must immediately report the event to the Chief Technology Officer (x4285 or cto@coconino.edu).

4. Evaluation regarding whether there has been a data breach of Personal Information requiring notification to affected individuals will be determined by the Office of Information Technology and other relevant offices.

5. Failure to follow these guidelines may result in disciplinary action up to and including termination (refer to Procedure 450-01(Disciplinary Action)).

3. BACKGROUND

1. References: State of AZ, Bunker Hill CC, and George Washington University
2. Revision history: 03/27/2013 (new)
3. Legal review: none
4. Sponsor: Information Technology Services

Adopted by College Council: 03/27/13

COCONINO COMMUNITY COLLEGE