Office/Contact: Division of Technology and Security
Source: SDBOR Policy 7.1 and 7.4
Link: https://public.powerdms.com/SDRegents/documents/1727287

b. Security of Login Credentials and Passwords

    i. Releasing login credentials and passwords compromises an individual's account and SDBOR and University Information Technology Systems.

    ii. Under no circumstances shall an account holder share or disclose their login credentials and password to anyone else, including but not limited to third parties, other departmental staff, faculty, or students.

    iii. No individual, including Division of Technology and Security staff, will ask another individual to share or disclose their login credentials and password.

c. Account Information Security

    i. Account holders with access to student information or protected health information will make themselves aware of, and comply with, all state and federal laws regarding student information (e.g., FERPA and HIPAA).

    ii. No user has any expectation of privacy in any message, file, image, or data created, sent, retrieved, or received by use of the SDBOR or University's equipment and/or access. The SDBOR and University have the right to monitor any and all aspects of SDBOR and University owned computer systems and to do so at any time, without notice, and without the user's permission. This policy applies to all employees, faculty, students, affiliates and visitors at the University.

d. Investigations of Electronic Communications

    i. Use of SDBOR and University Information Technology and Computer Resources are subject to SDBOR and University policies, including but not limited to Acceptable Use policies. "Electronic communications" includes telephone communications, Internet usage, phone messages, e-mail, and computer files traversing the SDBOR and University's network

4. Routine administrative functions, such as security tests of computing systems, including password testing by system administrators to identify guessable passwords and investigations of attempted access into systems by unauthorized persons (system administrators and other technical staff will not access employees' electronic communications or files while performing these functions).

5. Situations, such as the following two examples, will be specifically reviewed by and approved by the Vice President for Technology & Security and the A.V.P., their successors, or designees:

    a. An investigation into allegations of violations of law or policy affecting employment.

    b. An urgent need for access to college business documents when an employee is unavailable.

6. More specialized services offered by the Division of Technology and Security, such as the administrative database and the Library catalog, may have their own more specific policies regarding issuance, use, privacy and expiration of accounts which should take precedence over these more general policies.

3. Procedures

    a. If an individual receives a request for release of their login credentials and password they should not release this information and should contact the University Support Desk to report the incident.

    b. If an individual receives an email message claiming to be from the Division of Technology and Security asking for their login credentials and password or any other confidential information, the individual should not respond to the message. The individual should notify the University Support Desk.

    c. Any account that has been compromised by release of login credentials and password to a third party must be immediately locked without warning. The Division of Technology and Security designated staff will lock the account. To re-enable the account, the user must contact the University Support Desk for assistance.

4. Responsible Administrator

    The Vice President for Technology & Security, or designee, is responsible for the annual and ad hoc review of this policy. The University President is responsible for formal policy approval.

SOURCE: Approved by President 09/28/2017. Revised 01/31/2024 (clerical).