Security Incident Response Policy

Purpose and Scope

- The purpose of this policy is too ensure that
  - Information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be made
  - A consistent and effective approach is applied to management of information security incidents.
- This policy applies to all Wofford College students, faculty, and staff.

Policy

- A security incident may meet one or more of the following conditions:
  - Any potential violation of Federal law, South Carolina law, or Wofford College policy involving a College Information Technology (IT) asset.
  - A breach, attempted breach, or other unauthorized access to a Wofford IT asset.
  - Any Internet worm, virus, Denial of Service (DoS) attack, or related incident
  - Any change in a computer system that disables or defeats security precautions that have been installed on the machine
  - Any conduct using in whole or in part a Wofford IT asset that could be construed as harassing or in violation of Wofford College policies.
  - Any failure in our network or computer systems that disrupts IT services, particularly the critical services as defined in the IT Service Level Agreement.
- The appropriate authorities should be notified immediately of any suspected or real security incident. If it is unclear as to whether a situation should be considered a security incident, IT should be contacted to evaluate the situation.
  - Incidents that potentially involve violation of Federal or state law should be immediately reported to the Wofford Department of Campus Safety (597-4350)
  - Incidents that potentially involve malicious or accidental damage to the Banner database should be reported to the Banner DBA (597-4270) or Vice President of Technology (597-4294).
  - Incidents that potentially involve harassment should be reported to the Student Affairs Office (597-4040)
  - Any other potential security incident should be reported to the IT Help Center (597-4357).
- In the event of an incident that potentially involves malicious or accidental damage to the Banner database, IT will do the following:
  - If the incident still has the potential of causing damage, we will shut the database down immediately.
    - Shutdown generally will be authorized by the College Risk Officer or the Vice President of Technology.
    - In the event of an emergency, the Banner Database Administrator (DBA) is authorized to shut down the database. In this case, the Banner DBA will obtain written authorization from the College Risk Officer or Vice President of Technology as soon as possible and, in any case, within 24 hours of the event.

    - If the incident already has occurred and does not have the potential of recurring, we will ascertain the extent of the damage and take the appropriate measures.
    - In any event, the Banner DBA will do one or more of the following:
        - Perform a complete database backup and schema export.
        - Start up the database in restricted mode so that no user except the DBA can log on.
        - Disable the user account in question.
        - Extract data changed via a report.
        - Extract the audit trail of the change via report.
        - Obtain written authorization from the college risk officer to correct the changed data.
    - The DBA will submit the following to the College Risk Officer:
        - Documentation of post-incident actions.
        - A report of on any data that was changed.
- In the event of an incident, such as a virus, worm, or DoS attack, that threatens the health and security of the campus network, IT will do the following
    - The IT Network Group will analyze the problem and attempt to confirm that it actually is the result of a security incident
    - In the case a compromised computer is actively causing widespread network problems, that computer's network access will be revoked without prior notification.
    - In extreme and widespread cases of infection, network access may be revoked for a significant portion of the college network, such as the Residence Hall network.
    - If a College-owned computer has been disconnected from the network, the Help Center will assist in cleaning and protecting the machine.
    - If a personal computer has been disconnected from the network, it is the owner's responsibility to clean the machine and take any other steps necessary to secure it from future attacks.
        - The Help Center will offer guidance to computer owners on cleaning machines.
    - Network access will remain revoked until IT has verified that infected or compromised computers have been restored to health.
- In the event a user has disabled or defeated security precautions that have been installed on his or her machine, IT will do the following:
    - The Help Center staff will examine the machine to confirm that there actually is a security problem
    - In the case there is a problem, the Help Center staff will inform the user of the importance of security on the machine and advise them of ways he or she can avoid disabling the security feature again.
- In the event that a failure in our network or computer systems threatens IT services, particularly critical ones, IT will follow the procedure outlined in the IT Service Level Agreement.

Enforcement

- In accordance with the Banner Data Security Policy, unauthorized or inappropriate use of data or lack of adherence to Banner security policies and procedures will not be tolerated and may result in disciplinary action, which may include termination of employment.
- In accordance with the Policy on the Responsible and Ethical Use of Wofford College Technology Resources, the College reserves the right to temporarily suspend a user's access privileges or to disconnect a user's network port if it appears that this policy, or any other applicable College policy, has been violated or that a user's activity is a threat to the operation of our network system.
  - If the infractions also violate local, state, or federal laws, or other Wofford College policies, civil, criminal, and/or college sanctions may be independently applicable.
- In the cases of repeated situations in which a user has disabled or defeated security precautions on a Wofford-owned computer, IT will notify the user's supervisor. Continued infractions will result in removal of the computer from the user's work area**.**
- The College reserves the right to monitor previous offenders for further abuse.

Responsibilities

- Responsibilities are defined in the policy above.