Information Security Incident Response Policy

Approved by Cabinet on September 4, 2013

Purpose:

The purpose of this policy is to provide a consistent method of handling any information security incidents that may occur on the Catawba network.

Scope:

This policy applies to all Catawba College students, faculty, and staff.

Policy:

An information security incident is defined as any event that affects the confidentiality, integrity, or availability of network resources. Any of the following would constitute an information security incident:

- Any potential violation of federal law, North Carolina law, or Catawba College policy involving a Catawba Information Technology (IT) asset
- A breach, attempted breach, or other unauthorized access to a Catawba 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 Catawba IT asset that could be construed as harassing or in violation of Catawba College policies.

The appropriate authorities should be notified immediately of any suspected or real information security incident. If it is unclear as to

whether a situation should be considered an information 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 Campus Safety (704-637-4000).
- Incidents that potentially involve malicious or accidental damage to the Banner enterprise database should be reported to the Director of Enterprise Systems.
- Incidents that potentially involve harassment should be reported to the Student Affairs Office.
- Any other potential information security incident should be reported to the IT Help Desk.

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 Director of Enterprise Systems or the CIO.
    - In the event of an emergency where the Director of Enterprise Systems or the CIO is unavailable, a member of the Systems & Networking team is authorized to shutdown the database.
- If the incident already has occurred and does not have the potential of recurring, we will ascertain the extent of the damage and take appropriate measures.
- In any event, the Director of Enterprise Systems or CIO will authorize the DBA to 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
    - Correct the changed data

- The DBA will document the following:
  - Post-incident actions
  - A report of 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 Systems & Network Team will analyze the problem and attempt to confirm that it is the result of an information security incident
- If a compromised computer is actively causing widespread network problems, the 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.
- If a College-owned computer has been disconnected from the network, the IT Help Desk 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 safeguard it from future attacks.
  - The IT Help Desk offers virus removal for a fee
  - Network access will remain revoked until IT has verified that infected or compromised computers have been restored to health

If IT detects that a user has disabled or defeated security precautions that have been installed on his or her machine, IT will do the following:

- The IT Help Desk staff will examine the machine to confirm that there is an information security problem
- If there is a problem, the IT Help Desk staff will inform the user of the importance of information security on the machine and advise them of ways to avoid disabling information security features

Enforcement:

Any network user found to have violated this policy may be subject to disciplinary action, including suspension or termination of network privileges.

Any employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.

If infractions also violate local, state, or federal laws, other civil or criminal penalties may apply.

The College reserves the right to monitor previous offenders for further abuse.