Purchase College Computer Services
Security Investigation Clearance Form

A Security Investigation is to be conducted only with the prior approval of the Director of Campus Technology Services and senior campus executives. Each Security Investigation must be fully and completely documented. Non-emergency investigations must have approval of two senior College administrators (President or VPs).

Documentation of Security Investigations must include:

- Report of DMCA violation (non-emergency investigation)
- Other “Due Cause” documentation (emergency or non-emergency)
- Identification of security threat type
- Risk analysis – severity of threat and potential exposure
- Log files from threatened/compromised system
- Steps taken to contain threat
- Steps taken to contain possibility of exposure of sensitive materials or private information
- Steps necessary to prevent recurrence

The following policy pertains to all Security Investigations:

- **In an emergency** a the Privileged User conducting the investigation may view, copy, modify, or delete data placed on a computer or network by another user – and not normally shared - **if and only if** the Privileged User has documented probable cause that the contents of the data **poses an immediate threat** to the system or network. Examples of an immediate threat would include a “Root Kit” or other “Trojan Horse” back door, a worm or virus, or other materials or activities that pose a threat to the normal operation of College computer networks or systems.
- The Privileged User conducting the investigation may view, copy, modify, or delete data placed on a computer or network by another user **if** the Privileged User has documented that there is probable cause that the account is being used for illegal purposes (copyright violation, commerce, harassment, piracy or other crime) **and** has a completed Security Investigation Clearance Form.
- The Privileged User conducting the investigation may not erase or tamper with any system log file for any reason other than to archive the log file. If it is necessary to remove a log file from the system due to storage limitations, then the log file must be archived to tape for permanent storage. The archived records must provide an uninterrupted history of events on the system for auditing purposes. Exceptions must be approved in writing by the Director of Computing and Information Systems and IT security personnel.

Investigation of: ____

To be Conducted by: ____

Approved By: Director of Computer Services: ___________________________ Date: ______________

Senior Administrator #1 Date:________ Name: (Please Print) _______________ ________________________________ Signature	Senior Administrator #2 Date:________ Name: (Please Print) ____________________ ___________________________________ Signature