System Administrator Responsibilities

In the interest of data stewardship and compliance with Georgia Tech’s Computer and Network Usage and Security Policy (CNUSP) and the Data Access Policy (DAP), all systems containing sensitive information must be maintained by professional IT support personnel. However, there may be cases in which the end users have a need to retain Administrator rights on machines containing sensitive information or on machines that are used to access sensitive information stored remotely.

A user who has chosen to self-administer a computer which contains sensitive information, or which has access to sensitive information stored remotely, must implement and document the following practices:

- Use a regular user account, one without administrative rights. The user must only use an account with administrator rights when maintenance tasks are required. Users should consult with their local IT support person.
- Change all account passwords on the machine every 120 days.
- Install and keep anti-malware software up-to-date.
- Install and use a host-based firewall.
  Install the latest security updates for the operating system, as well as any software packages installed on the machine.
- Install only software that is in compliance with Georgia Tech policies, including proper licensing and appropriate content.
- Allow only appropriate GT employees and students access to the system and its applications.

---

1 The working definition of sensitive information is contained in section 3.2 of the Campus Data Access Policy (DAP found at [http://www.oit.gatech.edu/sites/default/files/DAP.pdf](http://www.oit.gatech.edu/sites/default/files/DAP.pdf)). In particular, examples of sensitive information are provided in the Data Security Classification Handbook [http://www.oit.gatech.edu/sites/default/files/DSC_handbook.pdf](http://www.oit.gatech.edu/sites/default/files/DSC_handbook.pdf)

2 Much of the above security requirements are met if the computer in question has been configured to be a part of the campus McAfee ePO and LanDesk programs. Please see your Unit IT contact for additional info. This will ensure that your computer is monitored for virus issues and OS and application patches.
System Administration Selection – Select one of the following options:

☐ I have read and understand the requirements for implementing and demonstrating that all the mandated settings have been configured on this system and that the system is in compliance with all Georgia Tech policies. Furthermore, I acknowledge that my self-administered computer may be audited by campus or state auditors and that if any issues are found with my computer, I will be responsible for those issues. If my system contains sensitive data, I understand that I must generate regular reports showing that the system is regularly patched and has appropriate antivirus tools installed and running.

EPO and LanDesk can automatically generate these reports as long as the system is registered in the services.

Justification for computer administration rights:

☐ ___________________________________________ will maintain the operating system(s), applications, and access to my system in a secure manner to protect the computing assets of Georgia Tech. The system will be kept in compliance with all Georgia Tech policies. Furthermore, I acknowledge that campus or state auditors may audit this system and that if any issues are found with this system, my designee or I will be responsible for those issues. I understand that I may not receive administrator/root access to this system, but will be provided the appropriate access I need to perform my duties. If my system contains sensitive data, I understand that I must generate regular reports showing that the system is regularly patched and has appropriate antivirus tools installed and running.

System Administrator's Signature: ___________________________ Date: ________________
Print Name: ___________________________ Unit: ___________________________
Phone Number: ___________________________ E-mail Address: ___________________________

Computer Policy Compliance
I understand that I am responsible for complying with the Georgia Tech CNUSP, DAP, Computer & Network Security Procedures, my home unit’s information technology procedure (if any), and appropriate federal and state laws when operating this computer.

System Owner’s Signature: ___________________________ Date: ________________
Print Name: ___________________________ Phone Number: ___________________________

Manufacturer: ___________________________ OS: ___________________________
Model: ___________________________ IP: ___________________________
Host Firewall: ___________________________ MAC: ___________________________
Other Security: ___________________________ DNS: ___________________________
E-mail Address: ___________________________