

GCSU

Information Security Operational Procedures

Windows Local Administration

INTRODUCTION

Georgia College & State University (GCSU) and The Division of Information Technology (IT) recognize that some faculty and staff have a demonstrated need to perform what would otherwise be considered administrative functions on computer equipment assigned to them by GCSU. It is also recognized that additional administrative functions may pose a risk to both the individual and the University. Risks that could face the University may be in the form of mis-configuration, errors, omissions, lack of diligence, poor understanding, or malicious intent. Whatever the cause of the risks, they are real and may severely impact the University or the student body.

DEFINITIONS

The following definitions are germane to the understanding of this procedure:

Local computer – As far as this procedure is concerned, a local computer refers to the computer, laptop, or workstation that is assigned to an individual or department.

Local Administrator – A local administrator is an individual who has been assigned certain computer privileges that allow for the execution of special administrative processes on a local computer.

Domain – A domain is a group of computers that receives information from a primary computer known as a domain controller. This information allows for the efficient and centralized management and coordination of a large number of local computers. The primary GCSU domain provides the basic file and network access and privileges to every local computer in the domain.

Background

The University implemented an infrastructure known as an Active Directory or Domain as a means to more effectively manage computer labs at a time when the number of lab computers was growing rapidly. In this area, the domain continues to function well allowing a relatively small number of staff to manage a large number of lab computers. During that period a change was made to our mission and faculty were being hired at a rapid pace. The support staff was unable to keep pace with the increasing demand for services and looked for ways to work more efficiently. The domain model in the computer labs had been very effective and was used initially as a stop gap measure to be able to manage local computers for new faculty. Time passed and the demands increased, so a computer management system known as Altiris was moved into production in addition to the existing domain. Altiris allowed remote administration to any domain affiliated computer anywhere on campus. Advances in Altiris continue to improve efficiencies for what is now Technology Support Services and benefit the campus as a whole.

Risks

Local administration is a responsibility to be considered seriously by both the individual and the University. Information technology and the Internet have placed each individual by way of the computers on the global forefront of communications. Though physically located in rural Georgia, in the world of technology each of us are now in Tokyo, New York, or Brussels via the Internet. Individuals must consider information security from this perspective rather than from the view of rural Georgia. The reality is that computing network power and ability expose us directly to individuals that would destroy, damage, or sell the University's information. Any risk normally associated with being connected to the internet becomes multiplied greatly when local computer administration does not assure proper configurations. Risks directly associated with local administration include:

- Loss of data by error or omission;
- Accidental or intentional publication of private individual data;
- Viral infection;
- Hardware damage due to mis-configuration;
- Hardware damage due to virus or worm;
- Unwitting participation in viral propagation;
- Unwitting participation in a Denial of Service attack (DoS), or intrusion;
- Disruption of University services;
- Publication of proprietary University data.
- Corruption of proprietary University data.
- Capturing proprietary information by recording activity through key computers.

RESPONSIBILITIES

The following responsibilities shall lie with the individual who undertakes the role of local administrator and the unit or college administrator approving the waiver. The local administrator shall:

- Only perform installation or maintenance on the local computer(s) assigned to them;
- Update all software patches including but not limited to MS Windows, and MS Office;
- Update antivirus definitions weekly or set to automatically update weekly or more often if needed;
- Install software that is not listed on the "Approved Software" list in emergency or time sensitive situations only. All other software installations shall be coordinated through Serve unless the software to be installed is "Approved Software". In the event of an emergency installation, the faculty or staff member shall notify Serve no later than the next business day via email or telephone.
- Provide IT with original media and software licenses regardless of funding source. Software purchased by grant or non-state funds shall be kept by the party awarded the funding along with accurate records of licensing. IT shall be provided with a working copy of the installation media in addition to a photocopy of the software license.
- Only install software essential to the local administrator's business function.
- Local administrators may install software listed on a published "Approved Software" list providing that appropriate licensing has been purchased by or on behalf of the installing party. Local administrators may request that IT review software for addition to the "Approved Software" list.
- Faculty may install test packs from known and reputable publishers.
- Local administrators may not install software from a published "Refused Software" list. Software on this list has been proven to be of detriment to the local computer or the overall infrastructure of the University.
- Screensavers may be native Windows screensavers or the local administrator may request approval of an alternative commercial screensaver.
- All non-commercial software including items developed by other faculty or other Universities shall be approved by IT prior to installation.

- If comparable software products are available, the approved software shall take precedence over unapproved software. Local administrators may install unapproved software if that software directly supports an academic course or scholarly research. No support shall be provided by IT for unapproved software.
- Local administrators shall not disable or alter any operational settings on a local computer put in place by IT.
- Updates published by IT are considered critical and shall receive precedence over updates or patches from other sources.
- Local administrators shall not alter or disable hardware without prior approval of IT. Removable media and external peripherals are exempt from this point.
- Local administrators shall not attempt to circumvent any security established on the local computer.
- Local administrators will not attempt to capture login information, network traffic, or any other data that may be considered sensitive.

Local administrators must be renewed and re-registered annually with IT by October 1 or the next business day if October 1 falls upon a weekend or holiday.

NOTE: This procedure does not supersede other GCSU policies or procedures. The local administrator must agree to abide by all GCSU policies and procedures as well as local, state, and federal legislation.

RESPONSIBILITIES FOLLOWING AN INFORMATION SECURITY INCIDENT

It is the responsibility of the local administrator to follow best practice guidelines in securing workstations and servers and the administrator's supervisor to ensure that expectations in this area are clearly understood and in writing, and that the local administrator is adequately trained and qualified.

In the event that problems arise as a result of local administration of a faculty member's computing equipment, the local administrator and their supervisor, will work with the IT to correct any problems that result from the event. The local administrator and the administrator's supervisor, in cooperation with the Division of Information Technology, will review administrative practices or procedures in place that may have contributed to the security event and take immediate corrective actions to avoid future re-occurrences.

PROCEDURE FOR REQUESTING LOCAL ADMINISTRATION

PRIVILEGES

1. Interested parties shall complete, sign, and submit the form, "Application for Local Administration" (Appendix A) to the designated administrators by the Dean of the College or the University Librarian.
2. The designated administrators will forward the Application for Local Administration to the CIO.
3. The CIO will review the application and associated justification.
4. The CIO will approve or deny the request and notify the designated administrators.
5. Upon approval the local administrators will read and agree to comply with the Information Security Procedures.

6. The local administrators will complete the appropriate WebCT security course and pass the included exam.
7. IT will register the computer assigned to the local administrators for routine scans for inadvertent vulnerabilities.
8. The application process will be renewed annually in October of each year.

Appendix

Application for Local Administration

Information Technology
Campus Box 050
Milledgeville, GA 31061-0490
(478) 445-1196

Revised: 03/16/09

GCSU

Application for Windows Local Client Administration

Name of Applicant:		
Department:		
College/Library:		
Date:		
Justification for Administrative Access:		
I have read and understand the associated Windows Local Administration Procedure I agree to abide by the statements within that procedure to the best of my ability. If approved for local administration authority, I will not knowingly violate federal, state, local, or University policies or law. I fully understand the implications and potential dangers of local administration and hold harmless Georgia College & State University (GCSU) its agents for any damages or loss that may occur as a direct or indirect result of local administrative actions. I attest that I am qualified to administer the computer equipment assigned to me by the University System of Georgia, the state of Georgia, or GCSU, and will use due diligence in protecting those assets or information stored on them from harm.		
Applicant Signature:		Date:
Name of College/Library Approving Authority:		
Signature of Approving Authority:		Date
CIO Signature		Date
Date Training Course Passed		
Administration Authority Approved/Denied		
If denied, state reasons for denial.		

Submit form to: Division of Information Technology
 Attention: Chief Information Officer
 Campus Box 50