



EMORY COLLEGE STATEMENT ON ADMINISTRATIVE ACCESS

I. Program Overview

Any computer connected to the Internet is at risk for malicious attack. These attacks can cause damage to the computer, loss or theft of sensitive information, user downtime, and interruption of Emory shared services. While attacks used to come mainly from viruses, flaws in operating systems and applications are being exploited by malicious code embedded in websites or web applications. This is now the primary avenue of attack. Emory College Computing Support (ECCS) will be reducing the risk of these attacks by adjusting the administrative control users have over their computers. Users will not be given administrative or root privileges on their computers by default. It is an industry best practice to grant all users non-administrative privileges in order to aid in protecting the integrity and security of the College computing environment.

II. Benefits to the Institution

Reducing end user administrative rights will help to protect important and/or confidential data (teaching, administrative, scholarship, and research), reduce downtime, and protect the shared resources of the University. This change will substantially reduce the time that ECCS spends on repairing or rebuilding compromised machines.

III. Security and Support

Emory College Computing Support is implementing tools to assist users in installing software and to provide faster support. University authentication mechanisms further protect against unauthorized access. ECCS support standards will be adhered to in order to ensure that the end user remains productive and to reduce any potential impact or downtime.

IV. Academic Freedom and Exceptions

Computers purchased using University funds (including research and grant money) are the property of the University and are therefore governed by the policies of the institution. Emory College Computing Support personnel are responsible for the maintenance and security of computers within the College's support scope. Our goal is to support and further the academic mission of the College and University in a way that protects both personal and institutional assets. The goal of ECCS is to prevent downtime and the loss of sensitive data, while providing professional and expedient service.

Exceptions to the administrative access policy will be made on a case by case basis. These will include mobile users and those with specific and applicable business needs. Individuals needing administrative access to their computers will be counseled on the security risks and will be required to acknowledge those by filling out an administrative privilege exception form. Computers with end user administrators

will be monitored for compromise. Administrative access will be re-assessed if a computer is compromised.

V. Related Policies

ECCS personnel comply with the Emory College Desktop Management Policy and Emory College Administrative Privilege Policy. The Deans of Emory College and the Emory College Faculty Governance Committee have approved these policies.

The Emory University Desktop Management Policy, Emory University Policy on Information Technology Conditions of Use, the Emory University Network IDs and Passwords Policy, and the Emory University Information Access Policy govern every Emory faculty and staff member.

All policies are available upon request.