



## ECCS DESKTOP MANAGEMENT USAGE POLICY

### I. Introduction

As the number of faculty and staff have grown within Emory College, it has become necessary to perform some support tasks remotely in order to continue to provide timely service to customers. The purpose of this policy is to establish guidelines for the acceptable use of desktop management and remote control utilities by ECCS personnel.

### II. Scope

The scope of this policy applies to all ECCS Personnel and any computer or customer under the College's support jurisdiction. This policy applies to all Desktop Management and Remote Control products that may be in use within the College environment.

### III. Definitions

- Desktop Management – Activities such as installing software, deploying a patch, gathering inventory data, group policy changes, etc. that are non-intrusive to the user.
- Remote Control – Actively viewing and or interacting with a user's desktop or activities (i.e. Remote Desktop)

### IV. Policy

- All computers within the College's support scope will utilize desktop management and remote control software. Disabling or uninstalling any desktop management or remote control software by users is prohibited.
- The use of desktop management and remote control utilities are strictly limited to the purposes of customer support, education, and problem resolution.
- The use of desktop management and remote control utilities for personal gain, profit, knowledge, or interest is strictly prohibited.
- The use of desktop management and remote control utilities is limited to College owned and supported workstations.
- All remote control utilities will be configured such that user permission is necessary when accessing user files or controlling the computer remotely.
  - No member of ECCS will remotely control a workstation without the consent of the user. This does not apply to public workstations (kiosks, classrooms, labs, etc).
  - ECCS will not access or copy user created data without the consent of the user.
- User permission is not required to use desktop management utilities (i.e. install or push a new software package, update to the customer's workstation, pull inventory, etc). However, if there will be an interruption (such as a reboot) the customer should be notified beforehand.

- Mass deployment of configuration changes, software, or patches to all College workstations will be approved through the College's change management process. These activities will be performed by approved personnel.
- Failure to abide by this policy will result in disciplinary action up to, and including, termination.

#### **V. Roles & Responsibilities**

- It is the responsibility of all ECCS personnel to implement this policy within the defined scope.
- It is the responsibility of the security lead to maintain and update the policy as necessary.