**Personal Mobile Device Access to Non-Public Data Policy**

## I. Overview/Purpose

The purpose of this policy is to set a minimum standard for protecting access to Augsburg College's information systems. The portability and size of mobile devices creates an opportunity for increased access to college resources but also creates a greater risk as login information is often saved on the device. To protect information stored on the mobile device and the access to non-public data the device affords a screen lock needs to be active. It is common modern security practice to have a mechanism for locking a device screen. While this may be inconvenient, the protection this provides individuals and the institution is large.

## II. Scope

The policy applies to any mobile device, college or personal, used by a faculty or staff member to connect to Augsburg College's information systems.

## III. Definitions

Mobile device – any device – phone, tablet, personal music player – that has the capability to connect to college systems such as email, calendar or file servers.

Non-Public Data – any information that is not available to the general public through public channels including, but not limited to HIPAA, FERPA, and social security data. This includes items such as College email communication, files stored on College file servers, and data housed in a College information system that requires a password to access.

## IV. Policy

Any mobile device that is configured to connect to college systems must have screen lock active and to be enabled after no greater than 5 minutes of no activity.

## V. Enforcement

Anyone found to have violated this policy may be subject to appropriate disciplinary action.

### Revision History

| Revision | Change | Date |
|---|---|---|
| 1.0 | Original Version | 4/5/2012 |
| | | |
| | | |
| | | |