Columbia Business School

Mobile Password Policy

1.0 Purpose

This document describes the ITG Information Security requirements for providing a password on every mobile device that is contained on Columbia Business School's Email Server. It is based on Columbia University's best practices as of March 25, 2010.

2.0 Scope

This policy applies to any mobile device issued by Columbia Business School or personal device used for Columbia Business School business which contains stored data owned by Columbia Business School.

3.0 Policy

All mobile devices containing stored data, calendar and contact information owned by Columbia Business School must use a password to protect data at rest. This includes all devices accessing Columbia Business School's mail server(s). Mobile devices are defined as, but not limited to include tablets, PDAs, and cell phones.

3.1 Mobile Devices

Any Columbia Business School data stored on a mobile device must be saved on a device that is password protected by the Columbia Business School. Columbia Business School shall employ remote wipe technology to remotely disable and delete any data stored on a Columbia Business School PDA, tablet, cell phone or mobile device which is reported lost or stolen.

3.2 How it Works

The policy will force your device to time out in 30 minutes unless you have a more restrictive policy set and you will be required to type in your password to make a call or send a message or email. After 10 failed attempts, your device will be reset and your contacts, email, texts and applications will be wiped out. Please be sure you sync your mobile device applications periodically to your desktop in order to save a backup so you can restore should your device need to be wiped. A unique character combination that cannot be easily derived (such as 1111 or any single number pattern, your birthday, home address or zip code) and is at least 5 characters long is suggested. We recognize many devices can only store 4 character passwords. In this case, it is important to use all 4 characters.

3.3 Loss and Theft

The loss or theft of any mobile device containing Columbia Business School data must be reported immediately to the Information Technology Group.