Cell Phone Policy

OVERVIEW:

Increasingly employees are using cellular technology as a means of sending and receiving Becker email, synchronizing calendars and contacts, transmitting text messages and connecting to the Internet. The purpose of this policy is to:

1. describe the conditions under which Becker purchases a cell phone and plan for its employees;
2. assist employees who purchase cell phones and plans independent of Becker with connecting to our servers for email and other online services;
3. describe how Becker manages cell phone technology to minimize risk, especially in the event of loss or theft;
4. remind employees about the use of email by offering helpful hints

APPLICABILITY:

Some employees are required to be "on call" during non-business hours. Communicating with these people is greatly enhanced through the use of cellular technology. Divisional heads, working in conjunction with the Chief Financial Officer, identify employees who require a cell phone as part of their position responsibilities. These phones and plans are purchased and managed centrally to take advantage of the most attractive rates and plan options. Please note the annual cost of providing an employee with a cell phone for voice communications only is about $500, and the annual cost of providing an employee with a cell phone for voice, data (email, Internet) and texting capabilities is about $1,000.

Although these are considered Becker phones, the College recognizes that allowing incidental personal use enables a person to carry one rather than two cell phones. Employees are reminded that these cell phones, the digital content on the cell phone and cell phone records remain the property of Becker.

Becker recognizes that some employees, although not required to carry a cell phone as part of their position responsibilities, would still like to connect their own device to Becker's email server so they can access and synchronize their email, contacts and calendar. Employees interested in connecting to Becker's email server should contact the Help Desk at x1999.

ADMINISTRATION AND IMPLEMENTATION:

When an employee leaves Becker, we adhere to the following practices regarding the removal of data if they connect phones to Becker's email servers:

Becker Owned Phone, Becker Sponsored Account	Upon exit, employee is given the opportunity to copy personal data (i.e. contacts, calendar) to an alternative location. After that, employee relinquishes the device, the device is wiped, and the account is cancelled.
Privately Owned Phone, Privately Owned Account	Upon exit, the employee is instructed to delete all Becker e-mail from the device. Employees may keep contacts, calendars and other personal items.

The nature of highly portable devices like cell phones lends them to a greater risk of loss. The fact that cell phones can also be used to store information like email, contacts and documents serves to increase the risks associated with such loss, but there are software policies that can be placed on the device to help minimize this risk.

If an employee, either because of work-related requirements or through their own choosing, elects to access Becker email and documents via their cell phone, they comply with the following:

- connect to Becker's email server,
- accept the security policies downloaded onto the device as a result of that connection, *and*
- agree **not** to store any Level 1 Data (SSN, Driver's License, Financial Account Numbers, Credit Card Numbers, etc.) on the phone consistent with Becker's Data Classification and Usage Policy

Please note these security policies are designed to accomplish 4 primary objectives:

1. Require a password to access the information on the device;
2. Automatically wipe the data on the device in the event of 5 failed login attempts;
3. For all Becker sponsored phones or plans, enable the Help Desk to remotely wipe the device in the event that the device is lost or stolen;
4. Limit the amount of email that can be stored on the device to 3 weeks of historical data

Employees are responsible for ensuring these security policies are activated on their cell phones (please call the Help Desk at x1999 if you need assistance). Privately owned and Becker issued phones will be wiped if the device is lost or stolen.

ADDITIONAL INFORMATION:

Employees are reminded that any e-mail messages created or received using Becker's mail system are considered College property, regardless of content. Please be aware that email sent and received using the College's computer resources is neither confidential nor private because the recipient of email could potentially forward the message to others without your consent or knowledge. While email is a valuable tool for communication, it does come with unintended consequences.

Employees are reminded that Becker's ability to reasonably secure (encrypt) email messages sent between parties is limited to messages sent to or from Becker email accounts. Becker has no ability to secure email that is sent or forwarded from a Becker email account to another email account (i.e., sent to email accounts on Yahoo, Gmail, etc.); consequently employees are reminded not to send or forward email that contains confidential or personally identifiable information from their Becker account to a non-Becker email account.

ENFORCEMENT:

Any person that violates any of the policies found in this policy will be subject to the same disciplinary actions as outlined in Becker's Confidentiality Agreement.

APPROVAL:

Approved by Becker's Information Security Advisory Committee on February 23, 2012.

REVIEW CYCLE:

This program will be reviewed and updated as needed, at least annually.

Last Updated: 2/20/17