Employee Owned Devices

Information

The information outlined below should be carefully considered by all individuals who wish to utilize a personal mobile device for direct use with and connection to INTEGRIS Email or Applications. To request the installation of INTEGRIS Email, Calendar, Contacts on your personal smartphone or other device you may contact the Help Desk however an approval email from your department VP and Director may be necessary before installation can take place. Including time allowed for receipt of approval, installation of a personal mobile device once the Help Desk has been contacted could take 7-10 business days.

Please note that not all types of mobile devices or smartphones are supported and compatible with INTEGRIS Health systems. Currently we can only support BlackBerry, iPhone and Windows Mobile (Credant Security software required). We do not support connection to Android OS enabled devices at this time. Information Technology is not responsible for loss of personal data on your personal device.

Service Charges

Please be advised that the addition of any company email, calendar, and contacts may result in increased data traffic and usage on your personal smartphone or other device. As such you may need to adjust your current service provider data plan accordingly. Some smartphone devices may require the upgrade of the wireless data plan to an enterprise version for your specific device so as to be able to communicate with INTEGRIS servers and receive INTEGRIS email. For information on data plans, please contact your wireless service provider.

Technical Support

You would be responsible for any device related issues that arise and would need to contact your service provider or device manufacture for all warranty requests. You would also be responsible for the backup and keep of your own personal data (non-INTEGRIS email, pictures etc). INTEGRIS Information Technology personnel would only provide assistance relating to the device’s connection to and availability of INTEGRIS Email and other business related applications for which a support model has been established.

Security Requirements

Your device must also meet certain security requirements which may include the requirement of a complex password and installation of security policies and/or encryption software to be applied in such fashion that is available depending on the device manufacture and to be managed by INTEGRIS Information Technology. For more details on what the security requirements for mobile devices currently include, see the Example Security Policy below.

Example below may represent only a partial list of security requirements

- Password Requirements as stated in SYS-IM-100:
  - Must be at least 8 characters in length
  - Must contain each of the following characteristics:
    1. Alphabetic character (example: a,b,c,d)
    2. Number (example: 1,2,3,4)
    3. Special character (example: !@#$%^&*)
  - Common words and phrases won’t be allowed (example: INTEGRIS, Password, Sooners, Cowboys)
  - Passwords will expire every 120 days and will be required to be changed
  - After 7 invalid password attempts the device will erase all data, requiring setup again
  - Additionally, local content encryption may be enabled
  - The device will automatically lock after 60 minutes of inactivity
  - To access the device after it has been locked will require you to enter your password