ISC10D054

# Mobile Device Security

ISSC approved a security proposal for mobile devices synchronising data with UEA' Exchange 2007 service at its meeting on 4th February 2011.

The ICTF Forum has re-considered the requirement in the policy for five failed pass-code attempts to result in the device being reset to its factory default (formatted). This number was considered too restrictive, and the Forum now recommends that the figure should be set at 12.

The policy with this proposed revision is included below:

**ISSC approval is sought for this revision to the policy.**

# UEA Exchange 2007 Mobile Devices - Security Policy Proposal

## Background

Currently all mobile devices that synchronise with the UEA Exchange service, in order to access e-mail, calendaring and contacts, are configured to remember user credentials and do not prompt for them to be re-entered. The service is designed in this way in order to support the automatic delivery of new items to devices, when they arrive, without having to re-enter credentials every time the device polls the server. As such if mobile devices are not configured with any type of security code, typically a 4 digit pin code, or have a weak strength code such as 0000 or 1234, the device and its contents present a security and confidentiality issue. This is particularly evident if a device is lost, left unattended or stolen. It would allow anyone who obtains such a device unauthorised access to the UEA Exchange email service and potentially secure and confidential information, in addition to being able to send and delete emails on that device. This is not in keeping with generally accepted corporate IT best practice in this area or with the University's Security Policies.

Following the UEA General Information Security Policy (GISP) ITCS are responsible for all centrally managed systems and services. As such we must determine risks, their impact and the managed response required to remove the risk or reduce its impact (GISP1). As such we must ensure that only authorised users can access University computer systems and IT services by providing and implementing authentication mechanisms to control access (GISP4). In turn the University email service must provide the facility for secure and confidential email correspondence (GISP6).

To eliminate this as a security risk, ITCS is recommending implementing an Exchange Security Policy that would be enforced on all mobile devices that synchronise with the UEA Exchange service. The policy applied to the device would enforce the following settings:

- Mobile device requires pass-code
- Minimum pass-code length = 6
- Number of failed pass-code attempts until device is reset to factory default (formatted) = **12**
- Time without user input after which pass-code must be re-entered (in minutes) = 5
- Enforce pass-code history (remembers last 3 pass-codes)
- Require encryption on the storage card
- Enable pass-code recovery (user can obtain recovery pass-code via OWA) ** Apple devices do not currently support this feature**

## Implementation

As Exchange Security Policies can be assigned on a per user or per server basis, a test policy was created and pushed out to a selected group of test user's mobile devices to assess the impact it would have from a compatibility and usability point of view. This was then be tweaked until the settings were deemed compatible from both a user and security perspective. This limited pilot, run throughout October, provided a cross-section of devices and users who provided very valuable feedback. This feedback led to the policy settings currently proposed and provided knowledge of some of the compatibility issues associated with implementation.

Following on from the success of the limited pilot, a wider pilot of ITCS staff and IT Support was implemented on Wednesday 24th November. This wider pilot has highlighted that a significant number of users use their personal mobile devices to access UEA Exchange email services. This has led to some resistance amongst this group of users who feel that such measures should not be applied to these devices. Whilst we acknowledge these concerns, we are obliged to ensure that the security and confidentiality of email and other UEA data stored on mobile devices remains so and is guaranteed. Officially supported mobile devices remain those provided by the University and as such we must ensure that these are secure. Users of personal devices are not being discouraged from continuing to use the service but should stop synchronising with the Exchange email service if they do not wish these settings to be applied.

We now plan to roll this out to all UEA users in a phased manner, ensuring that sufficient time is allocated to ensure the changes are effectively communicated, and users of personal devices have been given the opportunity to remove UEA email settings.