PERSONALLY-OWNED SMART PHONES/MOBILE DEVICES – EXCHANGE ACTIVESYNC
FREQUENTLY ASKED QUESTIONS (FAQ)

Updated December 3, 2010 5:50pm

The security of our information infrastructure and information assets is a priority for the State of Delaware. Each State employee and contractor has a responsibility to do everything we can to reduce vulnerabilities and improve our resilience to cyber-attacks.

With that in mind, a potential vulnerability involving State data on personally-owned smart phones or mobile devices was identified and closed by ensuring that smart phones (iPhones, Droids, etc.) and mobile devices (iPad, iPod Touch, etc.) that connect to our networks, via ActiveSync OVER THE AIR, must meet the following minimum security controls:

- Strong Passwords
- Password History
- Password Expiration
- Inactivity Timeout (60 minutes)
- Lockout after 7 failed attempts
- Remote wiping for lost/stolen devices (see Potential Loss of Personal Data on Device below)
- Encryption (if device is capable)
  - NOTE: If your device is not able to support encryption (many Droids fall into this category), it will be placed on a policy that does not require encryption, until an OS update that supports encryption is released. Once updates are released all individuals affected will be informed that they need to upgrade the software on their device by a certain date.

******* While others within your organization may also be connecting to the State network with other mobile devices (i.e. personally-owned Blackberries), we are focusing on ActiveSync connections at this time. ******

Individuals with a state.de.us and/or cj.state.de.us email address can request access to the State or CJ network to access their email and/or calendar, via their mobile device(s).

- These mobile device(s) must be compatible with Microsoft Exchange ActiveSync (also known as Microsoft Direct Push Technology).
- To request this functionality, individuals must contact their State Organization's Information Security Officer (ISO).
- Once this functionality is approved and enabled, the process below needs to be completed on the device.

IMPORTANT NOTE:

While others within your organization may also be connecting to the State network with other mobile devices (i.e. personally-owned Blackberries), we are focusing on ActiveSync connections via these popular devices AT THIS TIME:

Android	Inc	Lg vx11000	Palm
Htcdesirec	iPad	Lg vx9200	Pocketpc
Htcheroc	iPhone	Motoblur	Samsung schu960
Htcsupersonic	iTouch	Opal	Sonyericssonw760i

Device Compatibility

- What devices are compatible?
  - Any mobile device (Smartphone, PDA, iPad, etc) that supports Microsoft (Exchange) ActiveSync can be configured to work with the State and CJ email system. ActiveSync is also known as Microsoft Direct Push Technology.
  - **Windows Mobile Devices** – Any windows mobile device running Windows Mobile 6.x or higher is fully compatible with the State email system and ActiveSync.
  - **iPhone / iPad / iPod** – Any iPhone with the **OS 4.x or higher** can be configured for push email using ActiveSync.
    There have been isolated cases where the device needs to be updated via iTunes to the latest version 4.1 (as of 11/17/2010) to work.

- **Palm** – Palm WebOS devices, such as the Palm Pre & Palm Pixi, are compatible with ActiveSync. If the Palm is running the PalmOS, then it will not work with our system because the VersaMail program does not accept the SSL certificate that we had to use in order to load-balance the servers.
  *** SPECIAL ALERT *** for Owners of older Palm devices that DO NOT have wireless capability

- **Google Android** – Google Android phones with the **2.2 software** support ActiveSync.
  - *** SPECIAL ALERT ***

- What version of Exchange is the State running?
  - 2007

Requesting Access

- Individuals submit a completed Personal Smart Phone Device Network Access Request to their organization's Information Security Officer (ISO) who will, in turn, enter a "Personal Smart Phone Device Network Access" security request within the DTI ServiceManager application.

- Will DTI accept the "paper" Personal Smart Phone Device Network Access Request Form?
  - No; completed "paper" forms must be submitted to the organization's ISO who will, in turn, enter a "Personal Smart Phone Device Network Access" security request within DTI ServiceManager.
    - ISOs should NOT submit a "DTI Portable Wireless Access Request (Blackberry)" to request this access.

- Do I really need to give the last four-digits on my SSN or a four-digit pin (on the Access Request Form)?
  - Yes; In the event your personal mobile device is lost or stolen, this will be used to authenticate your identity before the signal is remotely sent to wipe the device.
    - You wouldn't want someone to report your device lost/stolen (to have your device wiped), as a mean joke.

- Why do you need to know my device's software version?
  - This is needed to confirm the compatibility of your mobile device with our servers.
    - For example: iPhones with software 2.x ARE NOT compatible, but if the same device is updated via iTunes to 4.x, it would be compatible.
    - There have been isolated cases where the device needs to be updated via iTunes to the latest version 4.1 (as of 11/17/2010) to work.

- How do I find out the software version of my device?
  - See the manufacturer's website and/or instruction manual.

Once Access is Granted

- During the initial synchronization, what settings or policies are being pushed down (over the air) to my device?
  - The ActiveSync Security policy
    - NOTE: Remote wiping for lost/stolen devices (see Potential Loss of Personal Data on Device below)

- Will the installation of 3rd party applications be restricted on personally-owned devices?
  - No; there are no plans to do this, at this time.

- Will the State network invoke these policies on the Smart Phone, or does the user have to perform any configurations?
  - The first time the device is synced with the State network, the policies will be "pushed down" to the device.

PERSONALLY-OWNED SMART PHONES/MOBILE DEVICES – EXCHANGE ACTIVESYNC
FREQUENTLY ASKED QUESTIONS (FAQ)
Updated December 3, 2010 5:50pm

ONE-TIME ActiveSync Setup Process: NOTE: The process is different on each device, but the following steps apply to the majority of devices:

1) **It is advisable to back up your data BEFORE creating a partnership (syncing) with ActiveSync.**
2) On the device, click on your ActiveSync setup
3) You will be prompted for a server. Enter in: **owa.state.de.us**
4) Make sure that "**This server uses SSL**" is checked
5) On the next screen you will be prompted for your username, password, and domain
   a. Username: **this is your state username**
   b. Password: **this is your state password**
   c. **Domain: State** *(if you have a state.de.us email address)*
   - or -
   CJ *(if you have a CJ.state.de.us email address)*
6) After you have entered in this information, you can sync your device with your mailbox. The first time you do this, it MAY take a several minutes to download your calendar, contacts, and emails.

See the Customer/Technical Support section below for additional information.

Potential Loss of Personal Data on Device

- DTI may wipe mobile device without any notification, resulting in loss of ANY AND ALL data on the mobile device and setting the mobile device back to factory default settings. DTI will make a reasonable effort to contact the appropriate agency personnel to inform them of the mobile device wipe and reasons for the wipe, in a timely manner.
- Remote wiping will be used only in extreme situations, where the device and/or network is at risk. One example is if your device gets in the wrong hands and more than 7 password attempts fail, it will automatically wipe. This is consistent with the State Blackberry policy. Other examples are if the user violates State policies, or a technical issue arises, or the device owner has resigned, been terminated, or suspended without pay. When the circumstances allow, we will give advance notice to you or the appropriate personnel of the wipe and the reasons for the wipe.
  - Some of the common reasons a mobile device would need to be wiped are:
    - if the mobile device is suspected of being compromised and poses a threat to the State
    - if the user of the mobile device violates State policies and statutes concerning the use of the mobile device
    - if a technical issue arises that requires the mobile device to be wiped to resolve
    - if the State.de.us account associated with the mobile device is disabled
    - if the owner of the mobile device has resigned, been terminated, or suspended without pay
  - Remote wiping will be used only in extreme situations, where the device and/or network is at risk.
    - One example is if your device gets in the wrong hands and more than 7 password attempts fail, it will automatically wipe. This is consistent with the State Blackberry policy.
    - Other examples are if the user violates State policies, or a technical issue arises, or the device owner has resigned, been terminated, or suspended without pay. When the circumstances allow, we will give advance notice to you or the appropriate personnel of the wipe and the reasons for the wipe.

Customer/Technical Support

- As agreed to on the Personal Smart Phone Device Network Access Request, DTI **IS NOT** able to provide troubleshooting or support for personally-owned devices.
- Individuals who have been granted this access, and who need assistance to configure ActiveSync on their device should:
  - Visit the device manufacturer's website
  - Visit their cell carrier/provider's website
  - Contact their cell carrier/provider's customer support

Miscellaneous

- Does this allow personal mobile devices permission to connect wirelessly to the State's network, i.e. State Net?
  - No; this would need to be requested separately.

- What if I decide that I do not like what has changed? How do I go back to my previous settings?
  - Delete the partnership (sync relationship) which will remove email, contacts, tasks, and calendar.
    - We DO recommend that you back up your data BEFORE deleting the partnership.

- Are you limiting access to my personal device, such as settings, webpages, or applications?
  - Aside from policy changes, which include encrypting any memory card; no.

- Will I be able to change settings on my device?
  - Certain settings will be locked (like password required), but you will be able to change timeouts. For example, a 60- minute lock policy allows a user to change to 15 minutes, if you so choose.

- What features could be enabled or disabled by the synchronization?
  - See the ActiveSync Security policy section above

- Does the initial synchronization cause any loss on the device, i.e. applications or data?
  - It should not; but it is advisable to back up your data BEFORE creating a partnership with ActiveSync. The policy is applied, certain aspects of the policy are locked, and whatever the user has configured will sync (mail, calendar, etc). Note that deleting a partnership would remove email, contacts, tasks, etc on the device however.

- Does the initial synchronization require resetting the device?
  - **Restarting** the device, not resetting, is required.

- What about the contacts already on the device? Does it overwrite the contacts; sync contacts both ways, etc?
  - It depends on the device. Some devices have SIM cards.
  - ActiveSync only syncs contacts in Outlook. If you delete the partnership with Exchange, the contacts will be deleted. Many phones have programs that will copy the contacts out so you can more easily restore them should you need to.

- It is stated that I will have to change my password when my domain password expires. Is that automated, or is it up to me to do?
  - The user will have to manually change the password on their device since it uses the domain password to sync (which is changed every 90 days).

- Who is held responsible for the device for the configuration of the device?
  - The user is responsible for the device. See the Customer/Technical Support section for more info.

- How do I get the request form?
  - Personal Smart Phone/Device Network Access Request Form

- Why are you asking if this is a personal or State-issued Smart Phone or Mobile Device (on the ServiceManager request form)?
  - This permits us to keep better track of the VERY limited of non-Blackberry State-issued Smart Phone or Mobile Devices

- I am hearing that there are a lot more employees who are accessing the state network with their personal blackberries other than those listed on the smart phone list.
  - While others within your organization may also be connecting to the State network with other mobile devices, we are focusing on ActiveSync connections at this time. Personal blackberries are capable of connecting to the State network in a different way than other smart phones. They do present a similar risk, however. Phase 1 of our effort is intended to close the vulnerability with Active Sync connections. We plan to tackle the personal berries in 2011, as it will impact a different user base and requires a different communication plan. Personal Blackberries will not lose connection on 11/15/10.

- If a user's device currently has all the default security settings in place, how will the new policy change the use of the device? Will the policy change any access via the Internet?
  - Once the request form has been approved and access is granted, the 7 security polices will be pushed to the device **the first time** the device is synced with the State network. Internet access on the device will not change.

- If I get locked out of my device, after 7 failed attempts, how do I unlock the device? Can the password be reset by calling the DTI Service Desk, or would the phone be wiped?

  - If the failed password attempts exceed the limit, the unit would be wiped. If a user forgets their password, they can use the password recovery option (**BEFORE** they exceed the limit of course) to unlock their phone. This is done via the Outlook Web application (OWA).

- Will a 10+ character strong password be required? If not, what is the minimum password length?
  - ActiveSync is currently set to 7 characters (but MAY be changed to 10 to match the Domain). As many as 18 characters can be set. Domain password is set at 10 characters. State-issued BlackBerrys are currently set to 7 characters.

- Are there any plans to make the state web access page (https://owa.state.de.us) smart phone format-compatible so we can still access calendar and e-mail?
  - There NO plans at this time. The whole purpose of a mobile device is to allow it to use the operating system and applications to format the email so that it can be easily read on the mobile device. Tasks like reading email via a browser is best saved for larger devices like laptops and the emerging iPad type devices.

- What responsibility does DTI take in the new procedure and what might fall back to the agency to support?
  - See the Customer/Technical Support section for more info.

- For the hard connected devices, such as the older Palm devices that do not have wireless capability, do I still need to submit the Personal Device request via the Service Manager system?
  - Devices that are being synced via a cable (NOT wirelessly) – such as older Palm Treos - **DO NOT** need a Personal Device request entered within DTI ServiceManager.

- What if my device DOES NOT support encryption, which is one of the requirements?
  - Encryption is a show stopper for a handful of devices – such as the HTC Droid Eris.
  - The handful of individuals with an HTC Droid Eris will be issued a waiver; so that encryption will not be required at THIS TIME – as the latest version of the HTC Droid Eris software currently DOES NOT support encryption.
    - As soon as encryption is avail on the HTC Droid Eris, we will request that you update the software on your device AND we will push the encryption requirement (over the air) to the device.
  - **ISOs:** When submitting a Personal Smart Phone/Device Network Access Request within DTI ServiceManager - make a note in the comment field that "the device currently DOES NOT support encryption".

- How do I get a list of the individuals within my organization (agency) using ActiveSync to connect their personally-owned devices to the State network?
  - Information Security Officers (ISOs), Information Resource Managers (IRMs), and Senior Management can request this list, by emailing the DTI Service Desk.

- I see "iPad" listed as acceptable – does that mean we can start using iPads here at work?
  - One can request access to their email, calendar, etc. via their personally-owned iPad.

- Will the State be monitoring or restricting personal use of my personally-owned device?
  - No; the State Acceptable Use Policy (AUP) has governance over the State communication and documents only. The AUP does NOT apply to personal, non-State usage on the device.

- If an ActiveSync-enabled individual moves from one State agency to another, are any changes needed?
  - If the individual is keeping their state.de.us email address; NO CHANGES are needed.
    - As the individual's state.de.us Active Directory (AD) account is already ActiveSync enabled, no changes should be needed by the individual, or the ISO of the departing agency or the ISO of the new agency.
    - But if the individual discontinues use of the device (i.e. opting for a State-issued Blackberry) at some point in the future, a security request would need to be submitted by their current agency's ISO to terminate the individuals' ActiveSync access.
  - If the individual is moving from a state.de.us email address to a cj.state.de.us email address (or vice versa), a new security will need to be submitted by the new agency's ISO.

- If the individual is moving from a state.de.us email address to a k12.de.us email address, ActiveSync access would be terminated – and we presently do NOT offer ActiveSync on the K12 network.

Disclaimers: Statement of Understanding {from the **Personal Smart Phone/Device Network Access Request Form** which the requesting individual must sign and submit to their Agency ISO.}

In addition to having read and understanding the Delaware Acceptable Use Policy, the Delaware Information Security Policy, the State of Delaware Mobile Device Encryption Standard, and the Delaware Data Classification Policy, as indicated by my signature below, I also agree and understand the following:

1. I have reviewed the list of device requirements to ensure my phone is provision able and will accept the Department of Technology and Information (DTI) Security Policy.
2. Only single-user mobile devices that can accept DTI's security configuration will be supported.
3. During the initial synchronization with the State Network, a default Security Configuration will be pushed to my mobile device. This configuration is meant to protect and secure the State's information on my mobile device. This configuration may change the way my mobile device works when I connect it to the State Network and could disable or enable features on my mobile device. If I do not accept the configuration, the mobile device will not be enabled to receive email from the State of Delaware's Network.
4. The configuration may change because it is periodically reviewed. DTI will attempt to inform customers prior to any changes, but, in the case of an emergency change, this contact may not be possible.
5. DTI may wipe my mobile device without any notification, resulting in loss of all data on the mobile device and setting the mobile device back to factory default settings. DTI will make a reasonable effort to contact the appropriate agency personnel to inform them of the mobile device wipe and reasons for the wipe, in a timely manner. Some of the common reasons a mobile device would need to be wiped are:
    a. if the mobile device is suspected of being compromised and poses a threat to the State
    b. if the user of the mobile device violates State policies and statutes concerning the use of the mobile device
    c. if a technical issue arises that requires the mobile device to be wiped to resolve
    d. if the State.de.us account associated with the mobile device is disabled
    e. if the owner of the mobile device has resigned, been terminated, or suspended without pay
6. If I lose my mobile device that is configured to connect to the State Network, I am required to take the actions listed below, as soon as possible, but no later than 24 hours from losing my mobile device.
    a. Notify DTI of the loss and what actions have been taken. Notification can be done by contacting DTI's Service Desk, either via email to DTI_ServiceDesk@state.de.us or by calling (302)739-9560. After being notified of a lost mobile device, DTI will confirm the data wipe of the mobile device. I will contact my Information Security Officer and report the loss.
    b. I will contact the cellular company that provides my service and have the mobile device deactivated.
    c. I will change my password immediately.
7. DTI is not able to provide troubleshooting or support for personally-owned mobile devices.

My use of mobile devices is also governed by various applicable polices and laws, including, but not limited to: Delaware Acceptable Use Policy, the Delaware Information Security Policy, the State of Delaware Mobile Device Encryption Standard and the Delaware Data Classification Policy.

What if my question or concern is **not** addressed on this FAQ?

- Email the DTI Service Desk.