



Click your browser's refresh button, while pressing "ctrl" on your keyboard – to ensure you are viewing the latest version of this doc.

# UPDATE

08/05/2011 10:30 AM

Security controls originally put in place on 7/25/11 are being reinstated.

Personal Blackberries®  
will be disconnected from the State network\*.  
**9:30 AM on Monday 8/8/11.**

\* - state.de.us and cj.state.de.us networks

*(Individuals that are not using AstraSync or NotifySync will be unable to send/receive State email\* from their personal Berry.)*

Be sure to check out the...

[\*\*AstraSync Configuration Instructions\*\*](#)

For the most timely customer service, always contact the  
[DTI Service Desk](#) 302-739-9560  
with questions or concerns; *not* individual DTI team members.

NOTE: DTI is NOT able to provide troubleshooting or support for personally-owned mobile devices. For assistance configuring, ActiveSync on personally-owned devices, please contact the third-party vendor's application customer/technical support.



# SECURING NON-STATE-ISSUED BLACKBERRIES® CONNECTING TO THE STATE NETWORK

SUPPLEMENTAL INFO FOR THOSE MOST IMPACTED originally posted: 07/05/2011 11:38am last updated: 08/05/2011 10:30am

Click your browser's refresh button, while pressing "ctrl" on your keyboard – to ensure you are viewing the latest version of this doc.

## WHO IS IMPACTED & WHAT ARE THEIR OPTIONS

Individuals that have been accessing their STATE.DE.US or CJ.STATE.DE.US work email, calendar and/or contacts via their **PERSONALLY-OWNED** BlackBerry® now have the following options:

### OPTION ONE – Use Outlook Web Access (OWA) using the Opera web browser

(NO SECURITY REQUEST REQUIRED) **YOU WILL BE UNABLE TO ACCESS OWA VIA THE 'BUILT IN' BLACKBERRY WEB BROWSER.**

Access OWA using the approximate link below using the web browser or computer device with Internet access to VIEW your work email, calendar, contacts, etc.

- individuals with a State.de.us email address use: <https://owa.state.de.us>
- individuals with a CJ.State.de.us email address use: <https://owa.cj.state.de.us>

### OPTION TWO – Continue to use your PERSONALLY-OWNED BlackBerry® to access your work email

Opt-in to the more secure method of accessing your work account via your **PERSONALLY-OWNED** BlackBerry®, by completing the following steps...

- Review and agree to the terms and security controls listed on the [Personal Mobile Device/Smart Phone Network Access Request Form](#), which include the following security controls being download/applied to your **PERSONALLY-OWNED** BlackBerry®:
  1. Strong Passwords
  2. Password History
  3. Password Expiration
  4. Inactivity Timeout (60 minutes)
  5. Lockout after 7 failed password attempts
  6. Encryption
  7. Remote wiping for lost/stolen devices  
*(see Potential Loss of Personal Data on Device below)*
- Submit the completed/signed form to your [organization's Information Security Officer \(ISO\)](#).<sup>\*</sup> They will submit the request on your behalf.

**STATE.DE.US email address** –Contact your ISO. If you are unsure who your [organization's ISO](#)<sup>\*</sup> is, contact your Network Admin or IT Support group. You may also contact the DTI Service Desk with questions at 302-739-9560.

**Only users with CJ.STATE.DE.US email address** - fax signed forms to 302-739-6285 – attention DELJIS ISO. (Call 302-739-4856 if you'd like to confirm receipt.)

<sup>\*</sup> - link only accessible when connected to the State or CJ network

- Download and install one of the approved third-party BlackBerry® ActiveSync application listed below, on your **PERSONALLY-OWNED** BlackBerry®.
  - The vendors charge a yearly fee for the use of their application.
  - While your organization *may* reimburse this cost, DTI will NOT.

third-party BlackBerry® ActiveSync Applications (aka Emulators)	DTI has tested both of these 3 <sup>rd</sup> party applications, but makes no warranties, either express or implied, concerning the content of such site or any information, products or services located therein, including the accuracy, completeness, reliability or suitability thereof for any particular purpose.
ActiveSync - <a href="http://astrasync.com">astrasync.com</a>	NotifySync - <a href="http://notifycorp.com">notifycorp.com</a>
\$49.00 per year, per user <small>(retrieved from vendor's website 06/29/2011 9:17am)</small>	First year cost is \$120.00 per user Second year cost is \$30.00 per user <small>(retrieved from vendor's website 06/29/2011 9:17am)</small>

- Complete the one-time configuration process on the mobile device, as outlined below under the heading, "Interim Solution - Ten (10) Business Day Evaluation Period."

### OPTION THREE – Switch to another type of mobile device (iPhone, iPad, Droid, etc.)

Opt-in to the more secure method of accessing your work account via iPhone, iPad, iTouch, Droid or other [Microsoft Exchange ActiveSync \(aka Microsoft Direct Push Technology\) compatible device](#), completing EACH of the following steps...

- Review and agree to the terms and security controls listed on the [Personal Mobile Device/Smart Phone Network Access Request Form](#), which include the following security controls being download/applied to your **PERSONALLY-OWNED** BlackBerry®:
  1. Strong Passwords
  2. Password History
  3. Password Expiration
  4. Inactivity Timeout (60 minutes)
  5. Lockout after 7 failed password attempts
  6. Encryption
  7. Remote wiping for lost/stolen devices  
*(see Potential Loss of Personal Data on Device below)*

NOTE: DTI is NOT able to provide troubleshooting or support for personally-owned mobile devices. For assistance configuring, ActiveSync on personally-owned devices, please contact the third-party vendor's application customer/technical support.



## SECURING NON-STATE-ISSUED BLACKBERRIES® CONNECTING TO THE STATE NETWORK

SUPPLEMENTAL INFO FOR THOSE MOST IMPACTED originally posted: 07/05/2011 11:38am last updated: 08/05/2011 10:30am

Click your browser's refresh button, while pressing "ctrl" on your keyboard – to ensure you are viewing the latest version of this doc.

- Submit the completed/signed form to your [organization's Information Security Officer \(ISO\)](#). \* They will submit the request on your behalf.

**STATE.DE.US email address** –Contact your ISO. If you are unsure who your [organization's ISO](#)\* is, contact your Network Admin or IT Support group. You may also contact the DTI Service Desk with questions at 302-739-9560.

**Only users with CJ.STATE.DE.US email address** - fax signed forms to 302-739-6285 – attention DELJIS ISO. (Call 302-739-4856 if you'd like to confirm receipt.)

\* - link only accessible when connected to the State or CJ network

- Ensure the device has the latest software version installed and complete the one-time configuration process on the mobile device, as outlined in the automated email that you will receive from DTI, when we ActiveSync-enable your account.

### **OPTION FOUR – Utilize a State-owned BlackBerry®**

- Obtain authorization within your organization to establish an account for a State-issued BlackBerry®.
  - To request this functionality, you must contact your [State Organization's Information Security Officer \(ISO\)](#), as outlined via [this process](#).\*

**STATE.DE.US users** – If you are unsure who your [organization's ISO](#)\* is, contact your organization's Network Admin or IT Support group.

\* - link only accessible when connected to the State or CJ network

### **INTERIM SOLUTION - Ten (10) Business Day Evaluation Period:**

As an interim solution, you may request a ten (10) business day evaluation period, to evaluate the vendors and select either option one or two and then complete each step, in the order listed below: *NOTE: evaluation periods must be requested - they are NOT automatically issued.*

1. Contact the DTI Service Desk (Mon – Fri 7am – 7pm) [dti\\_servicedesk@state.de.us](mailto:dti_servicedesk@state.de.us) or 302-739-9560 to request your ten (10) business day evaluation period.
2. As a part of this trial period, the following security controls will be applied to your **PERSONALLY-OWNED** BlackBerry®:
 

1. Strong Passwords	3. Password Expiration	5. Lockout after 7 failed password attempts
2. Password History	4. Inactivity Timeout (60 minutes)	6. Encryption
		7. Remote wiping for lost/stolen devices

*(see Potential Loss of Personal Data on Device below)*
3. Select one of the approved BlackBerry ActiveSync applications (aka emulators) from the third-party vendors listed under Option Two (above). *NOTE: Both vendors offer a FREE trial period.*
4. Register for a 7 day free trial, with one of the third-party vendor applications, listed under Option Two (above).
  - NOTE: To ensure that you are NOT personally charged for the application, be sure to cancel with the 3<sup>rd</sup> party vendor, before the 7 day trial expiration period ends. DTI will not reimburse individuals for the application, should they fail to cancel the trial before the 7 day expiration period.
5. Perform each of the following tasks, before you start the third-party application download:
  - Backup your existing data using the BlackBerry® Desktop Manager.
  - Turn off desktop synchronization of your calendar, contacts or emails with BlackBerry® Desktop Manager if you have enabled it.
  - Disable Content Protection if you have enabled it. *(Check this setting in Options | Security Options | General Settings.)*  
*<continued on following page>*
  - During setup you will need to have the following information:
    - Mail server type: MS Exchange 2007
    - Your Email Address: example: first.lastname@state.de.us or first.lastname@cj.state.de.us
    - Your Email User Name example: first.lastname
    - Email Domain: state.de.us or cj.state.de.us *(depending upon your email address)*
    - Your Account Password *(the same password you use to access your work email)*
    - ActiveSync Server Address: owa.state.de.us
    - Enable "SSL" *(if prompted)*

**NOTE: DTI is NOT able to provide troubleshooting or support for personally-owned mobile devices. For assistance configuring, ActiveSync on personally-owned devices, please contact the third-party vendor's application customer/technical support.**



SECURING NON-STATE-ISSUED BLACKBERRIES® CONNECTING TO THE STATE NETWORK  
SUPPLEMENTAL INFO FOR THOSE MOST IMPACTED originally posted: 07/05/2011 11:38am last updated: 08/05/2011 10:30am

Click your browser's refresh button, while pressing "ctrl" on your keyboard – to ensure you are viewing the latest version of this doc.

- 6. Follow the third-party vendor application's instructions to download and install the software on your personal Blackberry – entering the unique code/license key, provided by the third-party vendor when you registered for your free trial. (see step 3 above)
- 7. **IMPORTANT NOTE:** Your state.de.us or cj.state.de.us account will be ActiveSync enabled for a ten (10) business day evaluation period – to allow you time to submit [your request](#) to your organization's Information Security Officer (ISO) and for them to submit the request on your behalf.

**STATE.DE.US email address** –Contact your ISO. If you are unsure who your [organization's ISO\\*](#) is, contact your Network Admin or IT Support group.  
**Only users with CJ.STATE.DE.US email address** - fax signed forms to 302-739-6285 – attention DELJIS ISO. (Call 302-739-4856 if you'd like to confirm receipt.)

\* - link only accessible when connected to the State or CJ network

- If DTI does not receive an approved security request from your organization's Information Security Officer (ISO), on your behalf, before the 10 day evaluation period ends, your ActiveSync access will be disabled and you will be UNABLE to connect your personal BlackBerry® to the state.de.us or cj.state.de.us network.
- NOTE: DTI is unable to accept the "paper" [Personal Smart Phone Device Network Access Request Form](#).

- 8. Upon successful completion, your State.de.us email will only appear upon opening the ActiveSync or NotifySync application on your BlackBerry® -- these messages WILL NOT appear in your default BlackBerry® inbox, as they may have previously.

**\*\*\*\* AGAIN, THIS IS ONLY AN INTERIM, NOT A LONG-TERM SOLUTION. \*\*\*\***

**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-issued 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-issued 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 mobile devices. For assistance configuring, ActiveSync on personally-owned devices, please contact the third-party vendor's customer/technical support.

**FOR  
ADDITIONAL  
INFORMATION**

Each of these resources is available on the public-facing Internet:

- [General Facts](#)
- [Updated AstraSync Configuration Instructions](#)
- [SUPPLEMENTAL INFO for ISOs, IRMs, Network Admins, and other support personnel](#)
- [Frequently Asked Questions \(FAQ\)](#)
- [Personal Mobile Device/Smart Phone Network Access Request Form](#) (Completed by the requestor and submitted to their ISO.)

**STATE.DE.US email address** –Contact your ISO. If you are unsure who your [organization's ISO\\*](#) is, contact your Network Admin or IT Support group.  
**Only users with CJ.STATE.DE.US email address** - fax signed forms to 302-739-6285 – attention DELJIS ISO. (Call 302-739-4856 if you'd like to confirm receipt.)

\* - link only accessible when connected to the State or CJ network

**For the most timely customer service, always contact the DTI Service Desk  
with questions or concerns; not individual DTI team members.**

NOTE: DTI is NOT able to provide troubleshooting or support for personally-owned mobile devices. For assistance configuring, ActiveSync on personally-owned devices, please contact the third-party vendor's application customer/technical support.