



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 3rd party vendor's application customer/technical support.



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

GENERAL FACTS originally posted: 07/05/2011 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.

GENERAL FACTS	Securing Personal Blackberries® General Facts									
WHEN	Starting Monday, 7/25/2011 – 9:30am Re-blocked: Monday, 8/8/2011 9:30am									
WHAT	PERSONALLY-OWNED Blackberries will be unable to access their STATE.DE.US or CJ.STATE.DE.US email, calendar and/or contacts as they previously have. For this access to continue, actions will need to be taken by BOTH the individual and their organization's Information Security Officer (ISO).									
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: <ul style="list-style-type: none"> OPTION ONE: Access these resources via another device such as a STATE-issued Blackberry, an ActiveSync-compatible device, or access via Outlook Web Access (OWA). (Information regarding the above options.) OPTION TWO: Continue to use your PERSONALLY-OWNED BlackBerry®, but review and agree to the terms and security controls, listed on Personal Mobile Device/Smart Phone Network Access Request Form. <i>(Note: there is a yearly cost.)</i> 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. <ul style="list-style-type: none"> Contact the DTI Service Desk (Mon – Fri 7am – 7pm) dti_servicedesk@state.de.us or 302-739-9560 to request your ten (10) business day evaluation period. 									
WHO IS <u>NOT</u> IMPACTED	There is NO impact to... <ul style="list-style-type: none"> State-owned/issued Blackberries Individuals currently using an iPhone, iPad, iTouch, Droid, Windows Mobile Device, etc. to access your STATE.DE.US or CJ.STATE.DE.US email, calendar and/or contacts, over-the-air NO ACTION NEEDED									
WHY	The security of our information infrastructure and information assets is a priority for the State of Delaware. Each State employee has a responsibility to do everything they can to reduce vulnerabilities and improve our resilience to cyber-attacks. This change is required to close potential security vulnerabilities and to reduce the risk of leaking sensitive State data. With the growth in the use of mobile devices and the applications deployed on them, these devices are increasing as targets for cyber criminals. With that in mind, a potential vulnerability involving State data on personally-owned smart phones and mobile devices was identified and closed by ensuring these devices that connect to our networks, meet the following minimum security controls: <table border="0" style="width: 100%;"> <tr> <td>1. Strong Passwords</td> <td>3. Password Expiration</td> <td>5. Lockout after 7 failed attempts</td> </tr> <tr> <td>2. Password History</td> <td>4. Inactivity Timeout (60 minutes)</td> <td>6. Encryption</td> </tr> <tr> <td></td> <td></td> <td>7. Remote wiping for lost/stolen devices</td> </tr> </table>	1. Strong Passwords	3. Password Expiration	5. Lockout after 7 failed attempts	2. Password History	4. Inactivity Timeout (60 minutes)	6. Encryption			7. Remote wiping for lost/stolen devices
1. Strong Passwords	3. Password Expiration	5. Lockout after 7 failed attempts								
2. Password History	4. Inactivity Timeout (60 minutes)	6. Encryption								
		7. Remote wiping for lost/stolen devices								
FOR ADDITIONAL INFORMATION	Each of these resources is available on the public-facing Internet: <ul style="list-style-type: none"> SUPPLEMENTAL INFO for THOSE MOST IMPACTED 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.) <p style="font-size: small; margin-left: 40px;">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 CI network</p> <p style="text-align: center;">For the most timely customer service, always contact the DTI Service Desk with questions or concerns; <u>not</u> individual DTI team members.</p>									

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 3rd party vendor's application customer/technical support.