Personal Mobile Device Network Access Request

Completed forms must be submitted to your organization's Information Security Officer (ISO) to process the request.
Only requests or changes submitted by ISOs, through the DTI Service Now application, will be processed by DTI.

Section I Employee Information (Completed by employee)

		Add ◉ Update ○ Delete ○	
Date:	**Employee Name (Last, First, MI):**		**Last 4-digit SSN:**
State Exchange e-Mail Address:		**Employee's State Organization:**	
Work Phone:	**Device Make/Model:**	**Device Software Version:**	

Section II Statement of Understanding

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 mobile device 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.
8. 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. The Delaware Acceptable Use Policy governs the State data and activity on the personal device; it DOES NOT govern personal use of the device.

Employee Signature: _____ **Date:** _____

Section III Organizational Information (Completed by Requestor's State Organization)

Information Security Officer (ISO) Name (Print)	**Organization's Approving Authority Name and Title (Print)**
Information Security Officer (ISO) Signature and Date:	**Organization's Approving Authority Signature and Date:**

INSTRUCTIONS	**Reminder to Customers**
Section I and Section II - Employee completes. Section III - Customer's ISO and Approving Authority (Agency Head, District Superintendent, or similar approving authority) sign the request form.	Device synchronization will be completed no later than 10 business days after approval. Customer will have to complete a one-time process to set this up on their device. Each time you change your password, you will have to enter your new password on your mobile device.

PRINT