State of North Carolina Department of Public Safety POLICIES & PROCEDURES	Division: ADMINISTRATION Chapter: INFORMATION TECHNOLOGY Policy: LAPTOP AND MOBILE DEVICE USE
INFORMATION TECHNOLOGY	Issue Date: JANUARY 26,2013 Revised:

I. PURPOSE

To establish information security guidelines for the use of laptops and other mobile devices including, but not limited to, tape media, memory sticks, thumb/flash drives, external hard drives, CDs, DVDs, Personal Digital Assistants (PDAs), and smartphones.

II. SCOPE

This policy applies to all employees, including permanent, contractual, and consultant employees who work for the Department of Public Safety and use the Department of Public Safety computing and networking resources. All users are expected to become familiar and comply with the guidance provided herein. Questions regarding this policy should be directed to the Department of Public Safety's Information Security Office (Statutory and/or Regulatory Authority: Statewide Information Security Manual; § 147-33.110).

III. POLICY

1. Due to the greater likelihood for theft or loss, users should avoid storing confidential information on laptops or other portable media and devices whenever possible. All Department of Public Safety (DPS) laptops shall have full disk encryption enabled and the encryption feature will be managed by the appropriate MIS personnel.

2. Backup media which is to be stored offsite shall be encrypted prior to delivery to the offsite storage facility and/or the offsite vendor.

3. Any mobile device (including a personally owned device such as a smartphone) that contains confidential information, DPS email, or other sensitive data, shall have the device and/or information encrypted using a department approved encryption method. If encryption is not feasible, other access controls (such as PINs, passwords, etc.) must be used. Additionally, mobile devices used to conduct DPS business must adhere to the following measures:

- When using password protection and if feasible, the password should contain a combination of letters, numbers, and special characters and have a minimum length of eight characters.

- Attachments should not be opened from untrusted sources.

- Links from untrusted sources should not be followed, especially from unsolicited email or text messages.

- Bluetooth functionality should be disabled if it is not in use.

- Data shall be removed before disposing of the device. The data removal method shall meet state standards when feasible.

4. Laptop and mobile device users will adhere to all relevant and applicable desktop security policies which include, but are not limited to, the following:

    - Utilizing a timeout period for inactivity
    - Logging off when systems are not in use
    - Performing periodic backups of critical data
    - Using only authorized software and programs (DPS owned devices)
    - Complying with the DPS Remote Access policy
    - Configuration and maintenance by authorized MIS staff (DPS owned devices)
    - Vendor-supplied default and/or blank passwords shall be immediately identified and reset.

5. Mobile devices that have excessive storage capacity (e.g. external hard drives) shall adhere to the following guidelines:

    - Network storage (e.g. SAN) shall be used in lieu of these devices when possible

    - The DPS MIS personnel must review/approve the requisition for these devices

    - Data encryption must be enabled – no exceptions

6. Laptop and mobile device users will take reasonable steps to physically secure unattended systems or media.

7. Users will ensure that all laptop systems are updated and patched, at a minimum, on a monthly basis.

8. The use of wireless devices to access the DPS network must be authorized by the DPS MIS division. Wireless device access must adhere to any state and/or DPS wireless security requirements.

9. Mobile devices such as Blackberries, smartphones, PDAs, etc. that are managed by the DPS MIS division or personal devices that store confidential DPS data will have the following controls enabled when possible:

    - A maximum timeout interval of 10 minutes
    - Password protection with the syntax rules requiring a combination of letters, numbers, and special characters
    - Encryption of stored data
    - Device location enabled
    - Remote wiping enabled

10. In the event of theft or loss, DPS employees shall notify their management and the Information Security Office as soon as the theft is detected. Also, employees shall adhere to DPS policy for reporting misuse and/or theft of State property.

11. Before a thumb/flash drive is connected to a DPS device, employees shall ensure that the appropriate security software (e.g. antivirus, antispyware, etc) is installed and current on the affected DPS device. Thumb/Flash drives with unauthorized/unapproved virtual operating systems are prohibited.