NC Department of the State Treasurer Internal Operating Standards

Section: **ALL** Number: **177-03**

Policy Area: **Access Control**

Title: **Handheld Devices Security Standard**

Original Eff. Date: **2/24/2010**

Current Eff. Date: **9/1/2011**

Approved by: **Melissa Waller, Chief of Staff and Bill Golden, CIO**

I. Purpose

The purpose of the Mobile Communication Devices (MCD) Policy is to align cellular, portable computing and paging technologies to the roles and responsibilities of employees who have a job-related need for mobile communication technology. MCDs shall be used by the North Carolina Department of State Treasurer ("DST") to the minimum extent necessary to carry out the agency's mission. DST recognizes certain job functions require employees to be accessible when remotely assigned, away from the primary assigned work location, during times outside scheduled working hours, or during times of emergency. For this reason, DST may provide MCDs to employees for whom access to a MCD is a critical requirement for job performance. The device issued and the plan selected shall be the minimum required to support the employees' work requirements.

II. Definition

A "Mobile Communication Device" is any device that is capable of using the services provided by the public/private cellular networks or WiFi-type networks. These devices include blackberries, pagers, cellular phones with or without data plans, tablet PCs, and laptops with a dedicated air card.

III. Policy

A. Issuance: DST may only provide MCDs to employees for whom access to a MCD is a critical requirement for job performance. The use of an MCD is to be formally requested with a written justification and approved by the appropriate Division Director. The use of an MCD by a temporary employee or contractor must be approved by the Chief of Staff. The device issued and the plan

selected shall be the minimum required to support the employees' work requirements.

B. Usage: State-issued MCDs shall be used only for State business.

C. Tracking and Reporting: Division Directors are responsible for ensuring that all assigned MCDs are appropriately tracked and accounted for. Division Directors will review and report quarterly the need for MCDs and voice and data plans. DST will develop a standard reporting format for all divisions to use. Reports are due to the Chief of Staff, or his or her delegate, on the 15th of September, December, March and June. Each report will list the following information.

1. The number and types of new devices issued since the last report.
2. The total number of mobile devices issued by the division.
3. The total monthly cost of mobile devices issued by the division.
4. The number of each type of mobile device issued, with the total cost for each type.

Division Directors should be aware that all such quarterly information will then be forwarded by DST to each of the required offices at the General Assembly, so that all internal quarterly reports must be received in a timely manner and be as accurate and comprehensive as possible.

D. Periodic Audits and Annual Review

1. Periodic Audits: The Chief of Staff, or his or her delegate, shall conduct periodic audits of the call and usage records of DST-issued MCDs to ensure that users are complying with agency policies and State requirements for their use.

2. Annual Review: The Chief of Staff, or his or her delegate, shall conduct an annual review to re-justify the business need for each state-owned MCD device that has been issued.

IV. Operational Issues

A. Security

1. A wipe-out mechanism shall be employed to be used when devices are lost.
2. All MCDs configured to process electronic mail on behalf of the Department of State Treasurer will be fully managed by the DST Technical Services Team and secured using an enterprise level IT policy rule that will include the following minimum security settings:

- A handheld password will be required.
- Password must be changed every 120 days.
- Password must have a minimum of 4 characters. Users should select a combination of numbers, letters and symbols.
- Maximum password attempts before the handheld data is erased will be set to ten. The device will be configured to self-wipe after 5 failed password attempts.
- Maximum number of previous passwords that the new passwords must be checked against will be set to ten.
- Handheld must automatically lock after 15 minutes of inactivity.
- Content protection will be enabled and a 160-bit public key used to provide good security and performance when the handheld is locked.

B. Disposing and disabling handheld devices

1. All DST handheld devices shall be stored in secure areas when not in use.
2. All DST handheld devices shall be disabled and wiped before disposal.
3. Email accounts shall be disabled prior to employee's last work day.

C. Lost or Stolen MCD Response

All users are to report lost or stolen MCDs as soon as possible:

- Call the DST Information Security Officer ("ISO"), IT Helpdesk or IT Manager to report the loss event as soon as possible.
- Inform immediate manager/supervisor of loss as soon as possible.

Upon such notice of loss or theft, the DST Technical Services Team will initiate and confirm remote device wiping and will initiate the request to suspend cellular service with appropriate vendor.

V. Public Records

State business conducted on a state-issued MCD is public record. MCD users will be required to provide access to a MCD in response to a public records request. Information on the MCD which may fall under a Public Records Act exception will be redacted prior to DST's response to the public records request.

VI. Enforcement

All DST-issued MCDs are the property of the Agency and as such may be removed from the employee's possession at any time.

Misuse or non-compliance with this policy by DST employees and systems users is a serious matter and will be dealt with on a case-by-case basis. Depending on the severity of violations and applicable statutes, consequences for misuse or non-compliance could result in removal of access rights, repayment of fees for unauthorized or disallowed services, removal of system access, and/or disciplinary action up to and including dismissal. In cases of fraud, misuse, or breach of privacy laws, legal action may be taken. *See* N.C.G.S. §§ 14-454, 14-455, and 14-458.

The Chief of Staff shall have authority to interpret and apply this Policy. This Policy may be modified or amended at any time.

Revision History

Version/ revision	Date Approved	Description of Changes
1.0	2/24/2010	Initial release
1.1	5/1/2011	Added disposal requirement and changed the amount of password characters to four and decreased the self-wipe feature from 10 to 5 failed attempts
1.2	6/3/2011	Updated policy to incorporate all handheld device types – modified requirements on receiving DST emails on personal handheld devices; removed authority for CIO to approve DST email processing on personal devices. Only Chief of Staff will approve those requests – handhelds to be now tracked at the agency level Changed Header to include Original effective date and current effective date
1.3	9/1/11	Updated policy to conform to SL 2011-145

Agency	Type of Device	Model	Manufacturer	Number Purchased	Vendor	Contract Vehicle	ITS Contract (Y/N)	Device Cost	Monthly Cost Per Device**	Total Monthly Cost for Device	Annual Cost per Device	Total Annual Cost for Devices
								(Device + Activation Fee)	(Usage cost)	(Number of Devices x Monthly Cost)	(Monthly cost per device x 12)	(Number of devices x Annual cost per device)
NCDST	Cell Phone	Varies	Blackberry	44	Sprint	State Contract	Yes	$130.66	$55.63	$2,447.72	$667.56	$29,372.64
NCDST	Cell Phone	Varies	Blackberry	9	Verizon	State Contract	Yes	$130.66	$58.13	$523.17	$697.56	$6,278.04
NCDST	iPhone	iPhone	Apple	10	Verizon	State Contract	Yes	$199.00	$74.74	$747.40	$896.88	$8,968.80
NCDST	iPad	iPad	Apple	2	AT&T	Other*	No	$725.00	$29.99	$59.98	$359.88	$719.76
NCDST	iPad2	iPad2	Apple	1	Verizon	State Contract	Yes	$645.74	$38.97	$38.97	$467.64	$467.64
NCDST	Air Cards	Varies	Varies	34	Sprint	State Contract	Yes	unknown	$40.99	$1,393.66	$491.88	$16,723.92
NCDST	Air Cards	Varies	Varies	7	Verizon	State Contract	Yes	unknown	$38.97	$272.79	$467.64	$3,273.48
NCDST	Air Cards	Varies	Varies	9	AT&T	State Contract	Yes	unknown	$72.56	$653.04	$870.72	$7,836.48
Total at 9/30/11				116					$409.98	$6,136.73	$4,919.76	$73,640.76
Notes:												
There were no changes to the Mobile Device policy as of 9/30/11.												
* At the time of purchase, no State Contract was available for this device.												
** Monthly Cost Per Device is estimated based on August 2011 usage. This cost varies based on plan and other activation fees such as international access.												