



General Assembly

**Substitute Bill No. 677**

February Session, 2008

\* SB00677ET 041508 \*

**AN ACT CONCERNING THE USE OF STATE MOBILE COMPUTING AND STORAGE DEVICES.**

Be it enacted by the Senate and House of Representatives in General Assembly convened:

1 Section 1. (NEW) (*Effective from passage*) (a) For the purposes of this  
2 section, (1) "confidential or restricted state data" means personally  
3 identifiable information that is not in the public domain and, if  
4 improperly disclosed, could be used to steal an individual's identity,  
5 violate an individual's right to privacy or otherwise harm an  
6 individual. Such data includes, but is not limited to, organizational  
7 information that is not in the public domain and, if improperly  
8 disclosed, might cause a significant or severe degradation in mission  
9 capability, result in significant or major damage to organizational  
10 assets, result in significant or major financial loss, or result in  
11 significant, severe or catastrophic harm to individuals; (2) "mobile  
12 computing devices" means any portable or mobile computing and  
13 telecommunications devices that can execute programs; (3) "mobile  
14 storage devices" means mobile computing devices, diskettes, magnetic  
15 tapes, external or removable hard drives, flash cards, thumb drives,  
16 jump drives, compact disks and digital video disks; (4) "secure mobile  
17 device" means a mobile computing or storage device that has a  
18 sufficient level of access control, protection from malware and strong  
19 encryption capabilities to ensure the protection and privacy of state  
20 data that may be stored on such mobile computing or storage device;

21 and (5) "users" means all executive branch agencies and employees,  
22 whether permanent or nonpermanent, full or part-time, and all  
23 consultants or contracted individuals retained by an executive branch  
24 agency with access to state data.

25 (b) There is established a policy on security for mobile computing  
26 and storage devices, as described in this section. Such policy shall  
27 apply to all users.

28 (c) No confidential or restricted state data shall reside on any mobile  
29 device, except as set forth in subsection (d) of this section. Each  
30 executive branch state agency shall utilize secure remote data access  
31 methods, as approved by the Department of Information Technology,  
32 in support of mobile users.

33 (d) In the event that utilization of secure remote access methods is  
34 not possible, the executive branch agency shall adhere to the following  
35 restrictions and requirements: (1) Such agency head shall authorize  
36 and certify in writing to the Chief Information Officer, in advance, that  
37 the storing of restricted and confidential state data on the mobile  
38 device is necessary to conduct agency business operations; (2) the  
39 agency head, or the agency head's designee, shall determine and  
40 certify in writing to the Chief Information Officer that reasonable  
41 alternative means to provide the user with secure access to such state  
42 data do not exist; (3) such agency head, or such agency head's  
43 designee, shall assess the sensitivity of the data to reside on a secure  
44 mobile device and determine that the business need necessitating  
45 storage on the mobile device outweighs the associated risks of loss or  
46 compromise; and (4) such agency head, or such agency head's  
47 designee, shall authorize, in writing, the storage of specific state data  
48 on a secure mobile device and the acceptance of all associated risks.

49 (e) State data that an executive branch agency head has authorized  
50 to be stored on a secure mobile device, pursuant to subsection (d) of  
51 this section, shall be: (1) The minimum data necessary to perform the  
52 business function necessitating storage on the mobile device; (2) stored

53 only for the time needed to perform the business function; (3)  
54 encrypted using methods authorized by the Department of  
55 Information Technology; (4) protected from any and all forms of  
56 unauthorized access and disclosure; and (5) stored only on secure  
57 mobile devices in accordance with Department of Information and  
58 Technology policies, standards and guidelines.

59 (f) Any state data placed on a mobile device shall be documented,  
60 tracked and audited by the authorizing executive branch agency. The  
61 information tracked shall include: (1) The identification of the  
62 individual authorizing storage of the data on the mobile device; (2) the  
63 authorized user of the mobile device; (3) the asset tag of the mobile  
64 device; (4) information about the stored data; and (5) the final  
65 disposition of such data.

66 (g) Executive branch agencies shall configure mobile devices to  
67 allow only the minimum features, functions and services needed to  
68 carry out agency business requirements.

69 (h) Executive branch agencies shall ensure that mobile computing  
70 devices are configured with approved and properly updated software-  
71 based security mechanisms including anti-virus, anti-spyware,  
72 firewalls and intrusion detection. Users shall not bypass or disable  
73 such security mechanisms under any circumstances.

74 (i) Users in the possession of state-owned mobile devices during  
75 transport or use in public places, meeting rooms and other unprotected  
76 areas shall not leave such devices unattended at any time, and shall  
77 take all reasonable and appropriate precautions to protect and control  
78 such devices from unauthorized physical access, tampering, loss or  
79 theft.

80 (j) Executive branch agencies shall establish and document  
81 reporting, mitigation and remediation procedures for lost or stolen  
82 mobile devices containing state data and for state data that is  
83 compromised through accidental or nonauthorized access or  
84 disclosure.

85 (k) In the event that a mobile device containing state data is lost,  
86 stolen or misplaced or the user has determined unauthorized access  
87 has occurred, the user shall immediately notify his or her agency of the  
88 incident. The affected agency shall immediately notify the Department  
89 of Information Technology Help Desk of the incident in order to  
90 initiate effective and timely response and remediation.

91 (l) Executive branch agencies shall develop and implement a formal,  
92 documented security awareness and training program sufficient to  
93 ensure compliance with the policy set forth in this section.

94 (m) Executive branch agencies shall obtain a signed, formal  
95 acknowledgement from users indicating that they have understood  
96 and agreed to abide by the provisions of the policy set forth in this  
97 section.

98 (n) All executive branch agencies and users shall comply with the  
99 policy set forth in this section and any associated procedures.

100 (o) In accordance with the state Network Security Policies and  
101 Procedures, each executive branch agency shall be responsible for the  
102 assessment and categorization of such agency's data as confidential or  
103 restricted.

This act shall take effect as follows and shall amend the following sections:		
Section 1	<i>from passage</i>	New section

**GAE**      *Joint Favorable Subst.*

**ET**        *Joint Favorable*