**Executive Order 2008-10**
**Mitigating Cyber Security Threats**

**WHEREAS**, the State must endeavor to protect confidential information it acquires from its citizens and businesses; and

**WHEREAS**, the protection of such information, as well as of the State's information technology infrastructure, is an integral part of the efforts of the Arizona Statewide Information Security & Privacy Office (SISPO); and

**WHEREAS**, State agencies that maintain confidential information on unencrypted portable devices such as laptops, disks, thumb drives, and the like run a greater risk of inadvertently disclosing such information inappropriately; and

**WHEREAS,** unless otherwise required by law, confidential information from Arizona citizens should be redacted from documents subject to public dissemination to protect citizen privacy as well as government infrastructure; and

**WHEREAS**, Arizonans have a right to know that the State is exercising its best efforts to protect their confidential information, as well as to be informed if and when, despite such efforts, their confidential information has been compromised in a cyber security incident; and

**WHEREAS**, the resources required to redress a cyber security incident once it has occurred far exceed the resources required to prevent a cyber security incident from occurring; and

**WHEREAS**, by following IT Security best practices, the risks of a cyber security incident can be significantly mitigated; and

**WHEREAS**, A.R.S. § 41-3507 requires agencies to report cyber security incidents to the Statewide Information Security and Privacy Office;

**NOW, THEREFORE**, I, Janet Napolitano, Governor of the State of Arizona, by virtue of the authority vested in me by the Constitution and laws of this State, hereby order and direct all State Executive Branch agencies to:

1. Appoint an Agency Information Security Officer or designated liaison responsible for ensuring cyber security and working with the SISPO, ADOA, and its vendors;

2. Appoint an Agency Privacy Officer or designated liaison (who can be the person appointed as the Agency Information Security Officer) to help the agency ensure the privacy of sensitive personal information within the agency's possession;

3. Work with the SISPO to develop and implement strategies, policies and procedures to protect all confidential information resources, including electronic, paper and other media;

4. Deploy encryption technology for all information resources deemed confidential and/or that contain personally identifiable information;

5. Review and update policies and procedures for employees who telecommute or who otherwise use laptops, home computers and/or mobile storage devices, to ensure proper and adequate physical and logical security has been implemented to prevent compromise;

6. Develop and implement a process for all public documents to ensure compliance with A.R.S. § 41-4172 and that confidential information is not shared inappropriately;

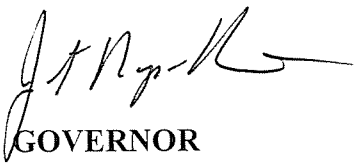
7. Promptly report all security incidents immediately upon discovery to the Statewide Information Security & Privacy Office (SISPO);

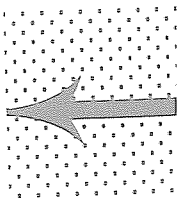
8. Develop and implement a procedure for prompt notification of any data breaches to affected parties;

9. Ensure Agency physical locations are properly secured against cyber crimes;

10. Create and implement training programs that detail each employee's responsibility for protecting information and technology resources in their care and ensure each employee receives and understands their responsibilities, including consequences for non-compliance.

**IN WITNESS WHEREOF,** I have hereunto set my hand and caused to be affixed the Great Seal of the State of Arizona.





**GOVERNOR**

DONE at the Capital in Phoenix, Arizona this ___ day of January Two Thousand Eight and of the Independence of the United States the Two hundred and Thirty-Second.

**ATTEST:**

**SECRETARY OF STATE**