Enterprise Security Policy Identifying Confidential Security and Emergency Preparedness Data and Information in the Possession of Government Bodies ("Security Policy")

February 23, 2017

1. **Purpose.** Iowa Code section 22.7(50) authorizes a government body to treat as confidential "[i]nformation concerning security procedures or emergency preparedness" when the disclosure of such information could "reasonably be expected to jeopardize" the "protection of governmental employees, visitors to the government body, persons in the care, custody, or under the control of the government body, or property under the jurisdiction of the government body." Such information may only be kept confidential under section 22.7(50) where "[the] government body . . . has adopted a rule or policy identifying the specific records or class of records" containing such information. Id. (b). This Security Policy identifies high-risk, security and emergency preparedness data, information, records, and classes of records (collectively referred to herein as **"Records"**), that fall into this category and authorizes State agencies to keep such Records confidential.

2. **Overview.** "Cybersecurity is a top priority not only in Iowa, but for our nation and throughout the world." *See* State of Iowa Cybersecurity Strategy. Government Bodies within the State of Iowa are responsible for safeguarding security and emergency-preparedness Records. These records, if released or compromised, could jeopardize the security of the State's operations, data systems, infrastructure, and other property, thereby compromising the safety and welfare of citizens, as well as negatively affecting government operations. To safeguard against the improper disclosure of such Records, this Security Policy identifies those high-risk, security and emergency preparedness Records falling into this category and authorizes State agencies to keep such Records confidential.

3. **Scope/Application.** Iowa Code section 8B.21(1)(*f*)(1) authorizes the OCIO to "develop[] and maintain[] security policies and systems to ensure the integrity of the state's information resources and to prevent the disclosure of confidential records." Similarly, Iowa Code section 8B.21(1)(*d*) authorizes the OCIO to "[p]rescrib[e] standards . . . relating to cyber security, . . . which shall apply to all participating agencies . . . ." Iowa Code Ann. § 8B.21. This Security Policy applies to all participating agencies as defined by Iowa Code section 8B.1. Non-participating agencies are encouraged to follow this and other enterprise standards. This Security Policy shall be deemed to have been adopted by all Participating Agencies. Because this is a minimum standard, in addition to this Security Policy, Participating Agencies may adopt standards and policies augmenting but not diminishing this Security Policy, and may identify additional or more specific classes of records that may be treated as confidential under Iowa Code section 22.7(50). In the event of a conflict between this Security Policy and a standard or policy adopted by a Participating Agency, this Security Policy shall govern.

4. **Definitions.** Capitalized terms not defined herein shall have the same meaning as given them in Iowa Code sections 8B.1 and 22.1.

5. **Enterprise Security Policy Identifying Confidential Security And Emergency Preparedness Data and Information in the Possession of Government Bodies.** It is the official policy of the State of Iowa that the following classes of Records, to the extent they constitute information concerning security procedures or emergency preparedness, the disclosure of which could reasonably be expected to jeopardize the protection of governmental employees, visitors to the government body, persons in the care, custody, or under the control of the government body, or property under the jurisdiction of the government body may be withheld from public inspection upon request pursuant to Iowa Code 22.7(50):

   5.1. Computer resource security files containing user names, login identifiers, and passwords of users of computer resources, which must be kept confidential to maintain security for access to confidential records.

   5.2. Data or information collected for the purpose of assessing, analyzing, measuring, preparing for, or responding to suspected, potential, or actual information security threats.

   5.3. Data or information collected for the purpose of assessing, analyzing, or classifying the severity of, nature of, ability to remediate, or ability to migrate data.

   5.4. Detailed security audit information including but is not limited to:

      5.4.1. Security assessment reports;

      5.4.2. Information directly related to vulnerability assessments;

      5.4.3. Information contained in records relating to security measures such as security and response plans, security codes and combinations, passwords, restricted area passes, keys, and security or response procedures;

      5.4.4. Emergency response protocols; and

      5.4.5. Any other information contained in records that if disclosed would significantly increase the vulnerability of critical physical systems or infrastructures of the office.

   5.5. Information security data, information security proposals, or information security assessments compiled, prepared, or developed by a governmental body, or compiled, prepared, or developed by a nongovernment body, and used by another governmental body.

   The foregoing Records may be kept confidential by all State agencies, irrespective of whether the Records were originally prepared by the government body that is now the Lawful Custodian

of the Records, or by another government body or nongovernment body and provided to the government body that is now the Lawful Custodian of the Records in question.

6. **Requirement to Notify and Consult with OCIO.** In the event any of the Records set forth in Section 5, herein, were originally prepared, created, or otherwise originated by or with the OCIO and subsequently provided to a State Agency now receiving a request for such Records, the State Agency receiving the request shall notify the OCIO of the request and consult with the OCIO in determining how to respond to the request.

7. **Updates.** This Security Policy shall be reviewed at least every two years and updated as needed.

8. **Effective Date.** This Security Policy shall be effective February 23, 2017.

9. **Enforcement.** This Security Policy shall be enforced pursuant to Iowa Administrative Code rules 11—25.11 and 11—117.11 and Iowa Code sections 8B.21(1)(*d*), (*f*), and (*h*), 8B.23(1), and 8B.24(1).

10. **Waiver/Variance.** Iowa Administrative Code rules 11—25.11(2) and 11—117.11(3) and Iowa Code section 8B.21(5) provide for variances\waivers from security standards and policies. Requests for a waiver/variance from any of the requirements of this Security Policy shall be submitted in writing to the State's Chief Information Security Officer.