CHAPTER 25
INFORMATION TECHNOLOGY OPERATIONAL STANDARDS
[Prior to 1/21/04, see 471—Ch 12]

11—25.1(8A) Definitions. As used in this chapter:

"Information technology" means computing and electronics applications used to process and distribute information in digital and other forms and includes information technology devices and information technology services.

"Information technology device" means equipment or associated software, including programs, languages, procedures, or associated documentation, used in operating the equipment which is designed for utilizing information stored in an electronic format. "Information technology device" includes but is not limited to computer systems, computer networks, and equipment used for input, output, processing, storage, display, scanning, and printing.

"Information technology services" means services designed to do any of the following:

1. Provide functions, maintenance, and support of information technology devices.
2. Provide services including, but not limited to, any of the following:

- Computer systems application development and maintenance.
- Systems integration and interoperability.
- Operating systems maintenance and design.
- Computer systems programming.
- Computer systems software support.
- Planning and security relating to information technology devices.
- Data management consultation.
- Information technology education and consulting.
- Information technology planning and standards.
- Establishment of local area network and workstation management standards.

"Nonparticipating entity" means the office of the governor or the office of an elective constitutional or statutory officer.

"Operational standards" means information technology standards, including but not limited to system design, system integration, specifications, requirements, processes or initiatives that foster compatibility, interoperability, connectivity, and use of information technology devices and services among participating agencies. Operational standards specify:

1. The performance that is required to be acceptable in accordance with specific operational criteria.
2. The technological features with which information technology products or services must comply to ensure compatibility, interoperability or connectivity among state agencies.

"Participating agency" means all executive branch agencies except the following:

1. The state board of regents and institutions operated under the authority of the state board of regents.
2. The public broadcasting division of the department of education.
3. The state department of transportation mobile radio network.
4. The department of public safety law enforcement communications systems and security systems in use for the legislature.
5. The Iowa telecommunications and technology commission, established in Iowa Code chapter 8D, with respect to information technology that is unique to the Iowa communications network.
6. The Iowa lottery authority.
7. A judicial district department of correctional services established pursuant to Iowa Code section 905.2.

"Technology governance board" means the board established by 2005 Iowa Acts, chapter 90, section 3.

11—25.2(8A) Authority and purpose.

25.2(1) The department is required to develop, in consultation with the technology governance board, and implement information technology operational standards through a process as set forth in this chapter. It is the intent of the general assembly that information technology standards be established for the purpose of guiding the procurement of information technology by all participating agencies.

25.2(2) The goal of the department is to develop and implement effective and efficient strategies for the use and provision of information technology for participating agencies and other governmental entities.

11—25.3(8A) Application of standards to participating agencies. Operational standards established by the department, unless waived pursuant to rule 25.6(8A), shall apply to all information technology participating agencies.

11—25.4(8A) Application of standards to nonparticipating entities.

25.4(1) Nonparticipating entities are required to consult with the department prior to procuring information technology.

25.4(2) Nonparticipating entities are also required to consider the operational standards recommended to agencies by the department.

25.4(3) Upon the decision by a nonparticipating entity regarding acquisition of information technology, the entity shall provide a written report to the department.

11—25.5(8A) Development of operational standards.

25.5(1) *Recommendation of operational standards.* The department and the technology governance board shall develop recommended information technology operational standards that shall be subject to consideration through the public input process established pursuant to rule 25.7(8A).

25.5(2) *Implementation of operational standards.* The department and the technology governance board shall jointly approve information technology standards which are applicable to information technology operations by participating agencies, including but not limited to system design and systems integration and interoperability pursuant to Iowa Code section 8A.202. The director is charged with prescribing and adopting information technology operational standards.

25.5(3) *Requirement for operational standards.* Operational standards shall be developed regarding information technology issues that affect multiple participating agencies. Examples of situations where establishing an operational standard would result in potential advantage to the state include, but are not limited to:

a. Promoting knowledge transfer and reducing learning curves for new technology solutions,

b. Protecting and securing the state's information technology infrastructure and data,

c. Reducing the resources applied to technology solutions,

d. Streamlining the state's common information technology systems and infrastructure,

e. Streamlining the delivery of information or services by promoting consistency in the handling, collection, transport, or storage of data and information, or

f. Promoting potential short- or long-term cost savings or cost avoidance.

25.5(4) *Basis for operational standards.* Operational standards may be based on any of the following:

a. Best practice guidelines. Standards based on best practice guidelines means that a case study or analysis is used to provide a benchmark for good business and information technology practices in achieving a desired result. The analysis or case study highlights one or several proposed products, technology fields, analytical methodologies or information technology solutions which constitute a good approach for other entities pursuing similar solutions. Best practice guidelines are intended to:

(1) Be informational,

(2) Facilitate knowledge transfer, and

(3) Shorten the learning curve for other entities addressing common technology issues.

b. Policy. Standards based on policy means that the operational standards are based on a description of required or prohibited courses of action or behavior with respect to the acquisition, deployment, implementation, or use of information technology resources.

c. Procedure. Standards based on procedure means that the operational standards are based on a set of administrative instructions for implementation of a policy or standards specifications.

d. Standards specifications. Standards based on specifications means that the operational standards are based on a description of specific required technical approaches, solutions, methodologies, products or protocols which must be adhered to in the design, development, implementation or upgrade of systems architecture, including hardware, software and services, and a description of those prohibited. Standards are intended to establish uniformity in common technology infrastructures, applications, processes or data. Standards may be developed as a subset of, and within the context of, a broader technology policy. Standards may define or limit the tools, proprietary product offerings or technical solutions which may be used, developed or deployed by state government entities subject to compliance with the operational standards specifications.

25.5(5) *Goals for information technology standards.* The underlying purpose of operational standards involving information technology shall be one or more of the following:

a. To promote consistency in the automation of the state's common infrastructure systems;

b. To eliminate duplicative development efforts by multiple state government entities;

c. To ensure continuity of ongoing state operations;

d. To promote administrative efficiencies relating to development and maintenance of common data; and

e. To enable the state to realize its full purchasing power from the use of a statewide, enterprise approach to the selection of technology solutions.

25.5(6) *Evaluating compliance with operational standards.* In evaluating compliance with operational standards, the technology governance board shall consider the following criteria:

a. Current technology. A proposed technology solution should be consistent with the statewide technology direction.

(1) A proposed technology solution should promote the goals set forth in subrule 25.5(5).

(2) A proposed technology solution should be current and reflect industry trends or best practice guidelines.

(3) A proposed technology solution should offer potential for a long life cycle, minimizing the risk of technological obsolescence.

b. Existing technology deployments. When state government entities have already made an investment in the proposed technology solution, the following issues shall be considered:

(1) The size and scope of existing deployments of the technology solution among state government entities (the installed base).

(2) Current fiscal investment associated with the installed base.

(3) Acquisition, development and deployment time frames associated with developing the installed base.

c. Maintenance of ongoing business operations. The proposed technology solution should enhance the ability of state government entities to maintain ongoing business operations.

d. Impact on state resources. Considerations regarding state resources include the following:

(1) Administrative and fiscal resources required to implement the proposed technology solution.

(2) Deployment time frame to implement the proposed technology solution.

(3) The potential for cost savings or cost avoidance.

25.5(7) *Effective date of operational standards.* Operational standards are effective 24 hours after the time of final posting unless otherwise specified.

11—25.6(8A) Waivers of operational standards. Participating agencies may apply directly to the department for a waiver of a current or proposed standard. The director, upon the written request of a participating agency and for good cause shown, may grant a waiver from a requirement otherwise

applicable to a participating agency relating to an information technology standard established by the department.

11—25.7(8A) Review of operational standards by the public and period of public comment.

25.7(1) Interested members of the public may participate in the process of establishing standards by providing written comments to the Enterprise IT Standards Coordinator, Department of Administrative Services, Legal , Rules and Planning, Hoover State Office Building, Level A, Des Moines, Iowa 50319. Comments will be accepted for a period of ten days after the initial posting of the standard by the department on the department's Web site at http://das.ite.iowa.gov/standards/index.html.

25.7(2) Interested members of the public may inquire about standards currently being considered for recommendation by the director by telephoning the enterprise IT standards coordinator at (515)281-6904; in writing to Department of Administrative Services, Legal, Rules and Planning, Hoover State Office Building, Level A, Des Moines, Iowa 50319; or by accessing the department's Web site at http://das.ite.iowa.gov/standards/index.html.

11—25.8(17A) Petition to initiate review of operational standards. Any interested member of the public may petition the department for review of an existing or recommended standard by filing a written or electronic request with the department. The director may grant the petition if the director determines that the petition has merit. If the petitioner does not receive a response within 30 days of receipt of petition by the department, the petitioner may deem the petition denied.

11—25.9(8A) Adoption of enterprise operational standards. Information technology operational standards shall be approved by the technology governance board (board). Once approved, standards shall be posted for public comment for ten days on the department of administrative services, information technology enterprise standards Web site pursuant to rule 11—25.7(8A). All comments shall be provided to the board. The board shall determine if an operational standard should be adopted as originally written or be modified as a result of public comment. Modified standards shall be returned to the board for final approval before adoption.

Operational standards approved by the board shall be adopted by posting on the department of administrative services, information technology enterprise standards Web site and notifying affected agencies of the standard and the effective date.

11—25.10 Reserved.

11—25.11(8A) Assessment and enforcement of security operational standards. The director shall designate a state chief information security officer for the department who is responsible for assessment of information security standards adopted by the technology governance board. The chief information security officer, or designee, shall assess compliance with security standards and seek recommendations for enforcement from the board when agencies are found to be noncompliant.

25.11(1) *Requests for additional time to comply with security standards.* An agency may request additional time to comply with adopted security standards by sending a written request to the chief information security officer. The written request must include the reason for the request, a description of what the agency will do to achieve compliance, and a time line for achieving compliance. The chief information security officer, or designee, shall approve or deny the request in writing to the agency within 15 calendar days of receipt of the request. The agency may modify and resubmit the request within 30 calendar days of receipt of notification of the decision. The chief information security officer shall approve or deny the resubmitted request in writing to the agency within 15 calendar days of receipt of notification. If the resubmitted request is denied, the agency may request review by the board at its next regularly scheduled meeting.

25.11(2) *Requests for a variance in security standards.* An agency may request a variance in the application of operational standards for security by sending a written request to the chief information security officer. A variance allows the agency to implement security measures different from the standard if the different measures, as determined by the chief information security officer, provide an equal or

greater balance between security and service delivery. The written request must explain any change in risk to information technology resources within the agency and to resources managed by others which would result from the variance. Within 30 calendar days of receipt of the request for variance, the chief information security officer, or designee, shall approve, deny or propose an alternative to the request in writing to the agency. The agency may request review by the board at its next regularly scheduled meeting.

25.11(3) *Compliance assessments.* The chief information security officer shall periodically assess agency compliance with security standards. Agencies shall provide appropriate access and assistance to complete the assessments. Agencies may request the acceptance of results of like assessments conducted by third parties in lieu of an assessment by the chief information security officer.

25.11(4) *Determination of noncompliance.* If the chief information security officer determines that the agency is noncompliant, the chief information security officer shall send to the director of the noncompliant agency, the director and the board written notification of the finding and the steps that the agency must take to become compliant. Within 30 calendar days of receipt of the noncompliance notification, the agency shall submit to the chief information security officer a written plan describing the actions the agency will take to achieve compliance or submit a written request for a variance from the standard pursuant to subrule 25.11(2). Within 15 calendar days of receipt of the agency's plan or request for variance, the chief information security officer, or designee, shall approve, deny or propose an alternative to the request in writing to the agency. The agency may request review by the board at its next regularly scheduled meeting.

25.11(5) *Remedies.* When an agency is determined to be noncompliant by the chief information security officer, or designee, and all requests for review by the board have been exhausted, the chief information security officer may seek enforcement recommendations from the board for action by the director.

The board's recommendations shall reduce risk to acceptable levels and include considerations for cost and impact on service delivery. When other measures do not reduce risk to an acceptable level, the board may recommend the disconnection of all shared services, including access to shared data, until compliance is achieved or a remediation plan for achieving compliance is approved by the board. If the noncompliant agency is unable to implement the recommended remediation plan and the board determines that the noncompliance continues to represent an unacceptable risk to state resources, the board may submit to the governor a written recommendation for the department's information technology enterprise to assume responsibility for the management of the noncompliant agency's information technology systems. The noncompliant agency shall reimburse the information technology enterprise for services at the published rates.

25.11(6) *Emergency remediation.* When an information technology incident is determined by the chief information security officer to be a threat to critical state information resources or information resources outside state government, the director, the chief operating officer of the department's information technology enterprise, or a designee will request the immediate shutdown or disconnection of the agency technology services that are contributing to the threat. If the agency does not immediately comply, the information technology enterprise, Iowa communications network or other body may disconnect the agency from all shared services. The agency will be reconnected to shared services when the chief information security officer determines there is no longer a critical threat.

These rules are intended to implement 2003 Iowa Code Supplement chapter 8A.

[Filed 8/21/01, Notice 5/30/01—published 9/19/01, effective 10/24/01]
[Filed 12/31/03, Notice 11/26/03—published 1/21/04, effective 2/25/04]
[Filed 10/22/04, Notice 9/15/04—published 11/10/04, effective 12/15/04]
[Filed 12/29/05, Notice 11/23/05—published 1/18/06, effective 2/22/06]
[Filed 10/4/06, Notice 8/30/06—published 10/25/06, effective 11/29/06][◊]

◊ Two or more ARCs