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.