

## TABLE OF CONTENTS

Chapter 1.	Electronic Transactions General Provisions	1-1
Section 1.	Authority	1-1
Section 2.	Purpose	1-1
Section 3.	Definitions	1-1
Section 4.	Coverage	1-2
Section 5.	Interpretation	1-2
Section 6.	Enforcement	1-2
Section 7.	Policies	1-3
Section 8.	Severability	1-3
Section 9.	Effective Date	1-3
Chapter 2.	Electronic Transactions Standards for the Conduct of Electronic Business	2-1
Chapter 3.	Electronic Transactions Security	3-1
Section 1.	Secure Electronic Procedures and Records	3-1
Section 2.	State Agency and Employee Responsibilities	3-2
Chapter 4.	Electronic Transactions Electronic Signatures	4-1
Section 1.	General Information	4-1
Section 2.	Electronic Signature Authentication Procedures	4-2
Section 3.	Attribution of Signatures	4-3
Section 4.	Electronic Signature Technologies	4-3
Section 5.	Transaction Record Authentication Procedures	4-4
Chapter 5.	Electronic Records Electronic Transactions	5-1
Section 1.	General Information	5-1
Section 2.	Assessment of Impact of Acceptance of Electronic Records	5-1
Section 3.	Integrity of Electronic Records	5-1
Section 4.	Retention of Electronic Records	5-1
Chapter 6.	Electronic Transactions Interoperability	6-1
Section 1.	Authority	6-1

**CHAPTER 1**  
**ELECTRONIC TRANSACTIONS**  
**GENERAL PROVISIONS**

**Section 1. Authority.**

These Office of the Chief Information Officer (OCIO) rules are promulgated in accordance with W.S. §9-2-2501 (Lexis-Nexis 2005), W.S. §§40-21-101 to 119 (Lexis-Nexis 2005).

**Section 2. Purpose.**

Information in all its forms is a valued asset to the State of Wyoming (State). Public information should be available to our citizens and to State government. Disclosure restrictions required by Wyoming law must be observed regardless of the media or characteristics of the record or transaction. The value of public information can be maximized through consistent delivery to and expanded use by the citizens of Wyoming and State government. To ensure continued confidence in and reliance on State agencies and the information they collect and maintain; State agencies must protect the privacy of citizens and ensure the integrity of State information in all forms.

The purpose of these rules is to:

- (i) Facilitate electronic filing, acceptance, preservation, maintenance, and availability, and confidentiality of documents with State of Wyoming (State) agencies; and
- (ii) Promote efficient delivery of services from State agencies by means of reliable electronic records.

**Section 3. Definitions.**

In addition to the definitions in W.S. § 40-21-102, the following definitions apply:

- (a) “Readable” means the quality of a group of letters, numbers or symbols is recognized as words, complete numbers or distinct symbols with a specific meaning.
- (b) “Reliable” means the electronic record copy produced correctly reflects the initial record each time the system is requested to produce that record copy.
- (c) “Structure” means the appearance or arrangement of the information in the record. “Structure” can include, but is not limited to, such elements as heading, body and form.

(d) “Cryptography” or “Cryptographic technology” means technology which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, or prevent its unauthorized use.

(e) “Availability” means assurance that the systems responsible for delivering, storing, and processing information are accessible when needed, by those who need them.

(f) “Confidentiality” means assurance that the information is shared only among authorized persons or organizations.

(g) “Integrity” means assurance that the information is authentic and complete. Ensuring that information can be relied upon to be sufficiently accurate for its purpose.

#### **Section 4. Coverage.**

These rules shall apply to any authority, bureau, board, commission, department, division, institution or officer of the State, except the State legislature and the judiciary. Except as otherwise provided in W.S.§40-21-112(f), these rules do not require an agency of this State to use or permit the use of electronic records or electronic signatures. Nothing in these rules shall preclude a State agency from specifying additional requirements for items that are under the jurisdiction of such agency.

#### **Section 5. Interpretation.**

The OCIO shall be solely responsible for providing official interpretations of these rules when questions arise regarding the application of these rules to specific situations, procedures or policies; or upon the request of an agency head.

#### **Section 6. Enforcement.**

##### **(a) OCIO Responsibility.**

(i) The OCIO shall ensure that these rules are enforced, and that the provisions of these rules are applied uniformly and fairly throughout the Executive Branch.

##### **(b) Agency Responsibility.**

(i) Agency heads are responsible for the application of these rules within their agency, and shall ensure that all agency employees comply with the provisions of these rules. Agency heads are responsible for the actions of their agency

employees, when the employees are conducting any State agency business electronically on behalf of the agency.

(ii) Agency heads shall ensure that, as necessary, employees of the agency are knowledgeable of pertinent provisions of these rules, when such knowledge is required for proper execution of their duties.

**Section 7. Policies.**

The OCIO may issue written policy statements relating to the interpretation or application of these rules, procedures for the administration of electronic government functions and to other matters which it may consider necessary for proper procedure. Agency heads shall ensure dissemination of, and compliance with, such policy statements.

**Section 8. Severability.**

If any provision of these rules or its application to any person or circumstance is held invalid or in conflict with any other provision of these rules, the invalidity shall not affect other provisions or applications of these rules which can be given effect without the invalid provision or application, and to this end the provisions of these rules are severable.

**Section 9. Effective Date.**

These rules are effective upon completion of all necessary procedures in accordance with W.S. § 16-3-104.

**CHAPTER 2**  
**ELECTRONIC TRANSACTIONS**  
**STANDARDS FOR THE CONDUCT OF ELECTRONIC BUSINESS**

[Reserved]

**CHAPTER 3**  
**ELECTRONIC TRANSACTIONS**  
**SECURITY**

**Section 1. Secure Electronic Procedures and Records.**

(a) An electronic record can be considered secure from a specified point in time to the point of verification if it can be shown that the record has not been altered during that time.

(b) Security procedures shall be:

(i) Commercially reasonable under the circumstances;

(ii) Applied in a trustworthy manner;

(iii) Reasonably and in good faith relied upon by the party utilizing the procedure;

(iv) Capable of providing reliable evidence that an electronic record has not been altered; and

(v) Consistent with the risks and consequences associated with the compromise of the information or transaction.

(c) A security procedure is acceptable for purposes of these rules if the security procedure (including any combination of technology and algorithms it employs) has been generally accepted in the applicable information security or scientific community as being suitable for the intended purpose and capable of satisfying the requirements of these rules as applicable, in a trustworthy manner.

**Section 2. State Agency and Employee Responsibilities.**

(a) State agencies shall protect information against unauthorized access, disclosure, modification or destruction, whether accidental or deliberate, as well as assure the availability, integrity, utility, authenticity, and confidentiality of information for the entire lifecycle of that information. Access to State information resources must be appropriately managed.

(b) All State agencies are required to have information resources security practices consistent with these rules, including adequate controls and separation of duties

for tasks that are susceptible to fraudulent or other unauthorized activity. The agency head is responsible for the protection of information resources.

(c) All State agency employees are accountable for their actions relating to information resources. Information resources shall be used only for intended purposes as defined by the agency and consistent with applicable laws.

(d) Risks to information resources must be managed. The expense of security safeguards must be commensurate with the value of the assets being protected.

(e) The integrity of data, its source, its destination, and the processes applied to it must be assured. Changes to data must be made only in an authorized and documented manner.

(f) Information resources must be available when needed. Continuity of information resources supporting critical governmental services must be ensured in the event of a disaster or business disruption.

(g) Security requirements shall be identified, documented, and addressed in all phases of development or acquisition of information resources.

**CHAPTER 4**  
**ELECTRONIC TRANSACTIONS**  
**ELECTRONIC SIGNATURES**

**Section 1. General Information.**

(a) This chapter applies to all non-verbal electronic communications or transactions conducted with a State agency over the Internet or other electronic network or by another means that is acceptable to the State agency, for which:

(i) The sender of the communication or transaction must be verified;  
or

(ii) The identity of the signer of the communication or transaction must be verified or authenticated; or

(iii) The integrity of the data contained in the communication or transaction must be maintained in verifiable form appropriate to the communication throughout the lifecycle of the data.

(b) This chapter does not apply to:

(i) The receipt of electronically filed documents pursuant to Wyoming statutes or other applicable statutory law where the purpose of the written electronic communication is to comply with statutory filing; or

(ii) The processing of electronic transactions under rules adopted by the Wyoming State Auditor's Office pursuant to applicable law; or

(iii) The use of e-mail to conduct business with the State where the conditions in Section 1(a) do not apply; or

(iv) As otherwise excluded by Wyoming Statute, or applicable statutory law.

(c) Any agreements entered into between a sender and the receiving State agency after the effective date of these rules must comply with these rules.

(d) Prior to accepting a non-verbal electronic communication, a State agency shall ensure that the level of security used to identify the sender of a message and to authenticate the electronic signature is sufficient for the transaction being conducted.

(e) A State agency that accepts non-verbal electronic communications may not effectively discourage the use of non-verbal electronic communications by imposing unreasonable or burdensome requirements on persons wishing to use non-verbal electronic communications sent to the State agency.

(f) A State agency shall not be required to accept an electronic signature for specific transactions if the State agency:

(i) Determines that the expense or resources required by the State agency to accept such an electronic signature are unreasonable; and

(ii) Provides reasonable notice to all interested persons of the fact that such electronic signatures will not be accepted, and of the basis for the determination that the expense or resources required for acceptance are unreasonable.

(g) A State agency shall review and consider any applicable guidelines and recommendations that have been adopted by the OCIO in determining whether and to what extent the State agency shall accept an electronic signature.

(h) A State agency shall ensure the following are retained by the State agency as necessary to comply with applicable law pertaining to audit and records retention requirements:

(i) All non-verbal electronic records received by the State agency and electronic signatures authenticated in accordance with Section 2 and Section 5 below; and

(ii) Any information resources necessary to permit access to the written electronic communications.

## **Section 2. Electronic Signature Authentication Procedures.**

For purposes of this Chapter an acceptable electronic signature authentication procedure is one that demonstrates, in a trustworthy manner, that the electronic signature:

(a) Is unique to the signer within the context in which it is used;

(b) Can be used to objectively identify the person signing and transmitting the electronic record;

(c) Provides reasonable assurance the electronic signature created by such identified person cannot be readily duplicated or compromised; and

(d) Is linked to the electronic record to which it relates, in a manner such that if the record or the signature is intentionally or unintentionally changed after signing the

electronic signature is invalidated.

### Section 3. **Attribution of Signatures.**

Except as provided by another applicable rule of law, a secure electronic signature is attributable to the person to whom it correlates, whether or not authorized, if:

(a) The electronic signature resulted from:

(i) acts of a person that obtained the signature device or other information necessary to create the signature from a source under the control of the alleged signer, or

(ii) the access or use occurred under circumstances constituting a failure to exercise reasonable care by the alleged signer.

(b) The receiving party relied reasonably and in good faith to their detriment on the apparent source of the electronic record.

### Section 4. **Electronic Signatures Technologies.**

The technology or technologies selected by an agency for use of electronic signatures may change over time. Existing technologies shall be implemented in a manner consistent with the requirements of these rules. The types of technologies acceptable for use for electronic signatures include:

(a) Non-Cryptographic technology that employs the use of passwords, personal identification numbers (PIN), smart card or similar technology.

(i) The agency is responsible for establishing adequate guidelines and procedures for the management and administration of non-cryptographic technologies that are consistent with the risks and consequences associated with the compromise of the information or transaction.

(b) Cryptographic technology that employs principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, or prevent its unauthorized use.

(i) The agency is responsible for:

(A) Establishing adequate guidelines and procedures for the management and administration of cryptographic technologies that are consistent with the risks and consequences associated with the compromise of the information or transaction;  
or

(B) Using a qualified cryptographic technology service provider for the management and administration of cryptographic technologies that are consistent with the risks and consequences associated with the compromise of the information or transaction.

#### **Section 5. Transaction Record Authentication Procedures.**

For purposes of this chapter an acceptable transaction record authentication procedure is one that demonstrates, in a trustworthy manner, that the transaction record data:

- (a) Is maintained in such a manner that the original data can be verified throughout the lifecycle of the record;
- (b) Provides reasonable assurance the transaction record data cannot be readily compromised;
- (c) Is linked to the electronic signature to which it relates, in a manner such that if the original transaction record data or the signature is intentionally or unintentionally changed after signing the transaction record is invalidated.

## **CHAPTER 5**

### **ELECTRONIC TRANSACTIONS**

#### **ELECTRONIC RECORDS**

##### **Section 1. General Information.**

State agencies shall assess the impact of agency operations prior to initiating electronic procedures and records. The assessment includes but is not limited to examining electronic procedures for receipt, storage or transmission of agency information.

##### **Section 2. Assessment of Impact of Acceptance of Electronic Records.**

State agencies shall perform an assessment of the benefits, level of effort, and risks that are associated with various categories of records that may be accepted in electronic form. In addition, a State agency shall review and consider any applicable guidelines and recommendations that have been adopted by the OCIO in determining whether and to what extent the State agency shall accept electronic records.

##### **Section 3. Integrity of Electronic Records.**

(a) An agency shall adopt procedures where necessary to provide safeguards to protect the reliability, authenticity, integrity, and usability of those records.

(b) To accept, create, and store an electronic record, a State agency must ensure the integrity of the information from the time it is first received and accepted, throughout the entire life cycle of the record. The criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement or other information that arises in the normal course of communication, storage and display. The standard of reliability required to ensure that information has remained complete and unaltered should be consistent with the risks and consequences associated with the compromise of the information or transaction.

##### **Section 4. Retention of Electronic Records**

State agencies shall comply with all statutes and rules relating to public records.

(a) For public records created and/or stored exclusively in electronic format, a State agency shall:

(i) Maintain those records so they are accessible, accurate, authentic, reliable, legible, and readable throughout the record life cycle.

(ii) Document policies, assign responsibilities, and develop appropriate formal mechanisms for creating and maintaining those records throughout the record life cycle, including documentation of hardware and software technologies.

(iii) Prescribe a procedure for converting information transmitted electronically to paper and certifying the paper copy for persons requiring paper copies.

(iv) Maintain confidentiality or restricted access of those records, including limiting access only to those persons authorized by law, administrative rule or established agency policy.

(v) Use information systems that accurately reproduce those records.

(vi) Document authorization for the creation and modification of those records and, where required, ensure that only authorized persons create or modify those records.

(b) For electronic records that are relied on to preserve legal rights, a State agency shall:

(i) Ensure that sufficient information on the content, context, structure, and presentation of those records is retained to preserve the validity of the document including, where necessary, verifiable procedures for migrating records to newer hardware and software systems to maintain access.

(ii) Maintain either:

(A) Adequate documentation of the record's validity, gathered at or near the time of record signing, including the processes in place at the time the record was electronically-signed, along with the electronically-signed record itself; or

(B) The capability to re-validate electronic signatures, along with the electronically-signed record itself, and related information used to validate the signature, for the entire lifecycle of the record.

(c) Where a rule or statute requires that certain documents, records or information be retained, that requirement is met by retaining electronic records of such information in a trustworthy manner, provided that the following conditions are satisfied:

(i) The electronic record and the information contained therein are accessible so as to be usable for subsequent reference at all times throughout the life cycle of the record;

(ii) The information is retained in the format in which it was originally generated, sent, or received or in a format that can be demonstrated to represent accurately the information originally generated, sent or received; and

(iii) Data that verifies the authenticity and integrity of the information, and the date and time when it was sent or received is retained for the entire lifecycle of the record.

(d) For permanent records requiring signatures, State agencies must ensure that the printed name of the electronic signer, as well as the date when the signature was executed, be included as part of any eye readable form (such as electronic display or printout) of the electronic record.

(e) If necessary, conversion to other media will be in accordance with guidelines and procedures as published by Wyoming State Archives.

(f) Limitation. Nothing in this chapter shall preclude a State agency from specifying additional requirements for the retention of records that are subject to the jurisdiction of such agency.

**CHAPTER 6**  
**ELECTRONIC TRANSACTIONS**  
**INTEROPERABILITY**

**Section 1. Authority.**

The state chief information officer in adopting standards may encourage and promote consistency and interoperability with similar requirements adopted by other governmental agencies of this and other states and the federal government and nongovernmental persons interacting with governmental agencies of this state. If appropriate, those standards may specify differing levels of standards from which governmental agencies of this state may choose in implementing the most appropriate standard for a particular application.