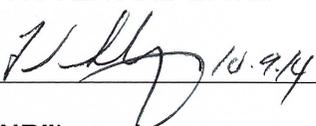


<p style="text-align: center;">STATE OF OHIO</p>  <p style="text-align: center;">DEPARTMENT OF NATURAL RESOURCES</p>	<p>SUBJECT: Electronic Signature Policy</p>	<p>PAGE <u>1</u> of <u>3</u> PAGES</p>
		<p>POLICY #DNR-OIT-0004</p>
	<p>RULE/CODE REFERENCE: OAC §123 et seq. ORC §1306.01 et seq.</p>	<p>SUPERSEDES: N/A</p>
	<p>PURPOSE: To provide for the use of electronic signature technologies by Department staff in accordance with DAS requirements.</p>	<p>EFFECTIVE DATE: 10/15/2014</p> <p>REVISION DATE:</p>
	<p>APPOINTING AUTHORITY: ORC §1501.01 ODNR Director</p>	<p>APPROVER AND DATE:  10.9.14</p>

This policy applies to all Ohio Department of Natural Resources (“ODNR”) employees, and in no way supersedes the negotiated language in the applicable collective bargaining agreements.

I. DEFINITIONS:

TERM	DEFINITION
Authentication	Authentication is the assurance that the electronic signature is that of the person purporting to sign a record or otherwise conducting an electronic transaction.
Electronic transaction	Electronic transaction means the exchange of an electronic record and electronic signature between a state agency and a person to: <ul style="list-style-type: none"> • Consent to release information; • Purchase, sell or lease goods, services, facilities or construction; • Transfer funds; • Facilitate the submission of an electronic record with an electronic signature required or accepted by a state agency; or • Create records formally issued under a signature and upon which the state of Ohio or any other person will reasonably rely including but not limited to formal communication, letters, notices, directives, policies, guidelines and any other record. This subsection does not include informational publications and informal communications.
Integrity	Integrity is the assurance that the electronic record is not modified from what the signatory adopted.
Nonrepudiation	Nonrepudiation is the proof that the signatory adopted or assented to the electronic record or electronic transaction.

II. POLICY:

ODNR is moving to a greater reliance upon the electronic management of records in order to improve the efficiency of ODNR operations and reduce costs. In conjunction with that effort, ODNR Divisions and Offices may wish to perform ODNR operations through means of electronic transactions that rely on electronic signature technologies; however, under Ohio

law, if a state agency creates, uses or receives electronic signatures, the agency must do so in accordance with rules adopted by the Department of Administrative Services (“DAS”). See [ORC §1306.20\(D\)](#). DAS has adopted rules for the use of electronic signature technologies at Ohio Administrative Code [§123:3-1-01](#).

1. Setting Up to Use Electronic Signature

When a division or office of the ODNR desires to use an electronic signature to process a certain type of electronic transactions, the following procedures shall be utilized:

- 1.1 The Division or office Chief shall contact the ODNR Chief Information Security Officer (CISO) and provide a point of contact for completing the necessary forms.
- 1.2 The CISO along with affected Employee shall complete the transaction risk assessment worksheet (MS Excel spreadsheet) and transaction risk assessment form required by DAS pursuant to our statutory obligations prior to using electronic signatures.
- 1.3 The affected Employee shall place the transaction risk assessment into sign-off for the approval of the Director. The sign-off process shall include the Division or office manager, the Division Chief, the Deputy Director of the division, the Chief of OIT, the Department’s Chief Record’s Officer, the Chief Legal Counsel or Designee, and the Assistant Director or the Director.
- 1.4 The CISO shall keep records of all transaction risk assessment forms. If required, the transaction risk assessment form shall be forwarded by the CISO to the State of Ohio, Office of Information Technology (“OIT”) for review and approval. See [OAC 123:3-1-01\(G\)](#) at the following website: <http://codes.ohio.gov/oac/123%3A3-1-01>, for more information regarding when OIT’s approval is required.
- 1.5 Upon approval of the Director and DAS OIT when required, OIT with the assistance of the CISO shall implement the desired level of security for the type of electronic transactions to ensure authentication, integrity, and nonrepudiation of such transactions. Relevant Department security policies, including policies from OIT, can be found on the following website: <http://intranet/dnn/default.aspx?alias=intranet/dnn/oit>
- 1.6 The Chief Records Officer and the ODNR CISO shall annually survey the effectiveness of the chosen security in assuring authentication, integrity and nonrepudiation measures for the type of electronic transactions surveyed. In addition, they shall determine if the transaction risk of any item has changed or is in need of revision. The Chief Records Officer shall inform the division Chief of the need to change any existing procedures for the type of electronic transactions surveyed.

III. RESPONSIBILITIES:

POSITION OR OFFICE	RESPONSIBILITIES
Office of Human Resources	A. To process violations of the policy according to the disciplinary process and grid.

ODNR OIT Chief Information Security Officer	<p>A. Maintains Division specific policies, procedures, directives and Executive Orders, and ensures their periodic review and update, as necessary.</p> <p>B. Monitor workforce, ensure compliance, and report violations to Human Resources.</p> <p>C. Proactively communicate questions, concerns and issues to the appropriate contact listed below.</p> <p>D. Ensure employees have access to and successfully complete any necessary ELM training in a timely fashion.</p>
Employee	<p>A. Read and comply with policy.</p> <p>B. Proactively communicate questions, concerns and issues to the appropriate contact listed below.</p> <p>C. Complete all associated policy training in a timely fashion.</p>

IV. RESOURCES:**V. CONTACTS:**

SUBJECT	OFFICE	TELEPHONE	EMAIL/URL
Policy Issues	Office of Human Resources/Labor Relations	(614) 265-6981	Policy.Coordinator@dnr.state.oh.us
CISO	Office of Information Technology	(614) 265-6854	Office of Information Technology

Related Department Forms:

- Transaction Risk Assessment – Ohio DAS
- Electronic Transaction Report Form – Ohio DAS
<http://das.ohio.gov/Divisions/InformationTechnology/OhioStatutesandAdministrativeRules/tabid/105/Default.aspx>