DELAWARE COUNTY BOARD OF COMMISSIONERS
ELECTRONIC SIGNATURE POLICY AND SECURITY PROCEDURE

I. PURPOSE

The purpose of this Electronic Signature Policy and Security Procedure ("Policy") is to facilitate the usage of electronic signatures for any and all records and documents where practicable. In order to increase efficiency in matters requiring signature authorization, the Delaware County Board of Commissioners (the "Board"), either directly or through its authorized representatives, may require or permit a person to use an electronic signature in lieu of a handwritten signature in order to sign certain records or documents.

II. APPLICABILITY

This Policy applies to the Board, including all departments, offices, employees, and volunteers under the Board's appointing authority, the Board's vendors and contractors, and any other person conducting business with the Board or one of its departments if the business conducted requires the execution of a record or document.

III. AUTHORITY

This Policy is adopted pursuant to Chapters 304 and 1306 of the Revised Code. The Board authorizes the County Administrator to perform the following functions: (1) contract for the provision of computer programs, information processing systems, software, and other means to implement this Policy; (2) require or permit, on behalf of the Board, the use of an electronic signature on a record or document; and (3) appoint, in writing, other executive or administrative employees of the Board that may initiate electronic transactions requiring or permitting an electronic signature in accordance with this Policy.

IV. DEFINITIONS

The definitions set forth in sections 304.01 and 1306.01 of the Revised Code, as may be amended from time to time, shall apply to this Policy and are, by this reference, incorporated herein.

V. POLICY CONDITIONS

A. Form of Transaction: The Board and its authorized representatives reserve the right to determine whether to conduct a transaction utilizing this Policy or via hard-copy records or documents with handwritten signatures.

B. Official Initiation: In order for a person to use an electronic signature as permitted in this Policy, the transaction must first be initiated by an employee authorized to initiate electronic transactions utilizing the program the County Administrator designates. Any

electronic signature submitted without official initiation as stated herein may be rejected; provided, however, the Board reserves the right to accept as authentic any record or document submitted with an electronic signature.

C. External Records and Documents: Any person that is entering into an agreement, a contract, or another transaction with the Board that requires execution of a record or document may use an electronic signature, subject to the requirements of this Policy.

D. Internal Records and Documents: Any employee of the Board that is required or permitted to execute a record or document in the course of the employee's official duties may use an electronic signature, subject to the requirements of this Policy. Any employee of the Board that is required or permitted to execute a record or document as a condition of, or otherwise related to, employment (e.g., the acknowledgment of receipt of policies, human resources forms, etc.) may use an electronic signature, subject to the requirements of this Policy.

E. Binding Effect: Pursuant to section 1306.06, an electronic signature shall be binding on the person and have the same force and effect as a handwritten signature.

VI. SECURITY PROCEDURES

A. Software Program: The County Administrator shall designate one or more programs through which electronic signatures shall be processed in accordance with this Policy. The designated programs shall, at a minimum, include individual user accounts with unique usernames and passwords or other access control measures, document encryption and identification keys, secure transmission of records or documents, alteration detection, and audit reports or trails.

B. Administrative User Accounts: Any employee authorized to initiate electronic transactions shall have an individual administrative user account that allows for the creation and distribution of the electronic record or document for electronic signature. The employee with an administrative user account shall be responsible for managing the entire transaction, including document creation, collection and verification of all signatures, confirming that the document is complete without alteration, distribution of the completed record or document, and properly retaining the record or document. Signature verification shall be made through a program authorized pursuant to this Policy using each signer's current, authentic, and regularly-monitored email address that is capable of independent verification. The administrative user shall, in the event an email address is not independently verified, confirm the authenticity of any electronic signature through telephone or in-person signer acknowledgment.

C. Signer Accounts: User accounts shall not be required for persons required or permitted to sign a record or document with an electronic signature, but each person shall adopt an electronic signature and is responsible for reviewing and confirming all uses thereof. The person shall use a current, authentic, and regularly-monitored email address that is capable of independent verification. Employees of the Board shall use their Delaware

County email address, if they have been assigned one.

D. Alteration: A person to whom a record or document is submitted for electronic signature shall not modify or alter the original record or document, except for the addition of that person's electronic signature and, if applicable, date/time stamp.

E. Employee Prohibited Conduct: Employees of the Board shall not use an electronic signature on behalf of another employee, absent express authorization from the employee and the employee's supervisor, or designee, with such authorization to sign on behalf of another documented in writing. Employees of the Board shall immediately report any suspicious or fraudulent activity related to the use of electronic signatures to the employee's supervisor or Human Resources. Any employee who falsifies an electronic signature or in any other way violates this Policy may be subject to discipline, up to and including termination, as well as potential criminal prosecution, if applicable.

F. Audit Reports or Trails: Each record or document signed in accordance with this Policy shall have attached to it a secure, computer-generated audit report or audit trail that records independently the following information: the document title, file name, and unique identifier; the date, time, and identification of all user actions that create, modify, or delete electronic information contained in the record or document; the date and time of all electronic signatures, with identification of the user by name, email address, and/or IP address; and any other information for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record or document.

G. Monitoring: Each employee with an administrative user account shall review the audit reports of each record or document and immediately report any irregularities to their supervisor or department director. The County Administrator shall coordinate with the Delaware County Data Center to conduct regular tests and evaluations of the security procedures under this Policy and to address any errors or deficiencies with Data Center staff and program vendors.

H. State and County Audits: The Ohio Auditor of State is required to inquire into the method, accuracy, and effectiveness of these security procedures. Therefore, all Board employees shall fully cooperate with any review or audit conducted by the Delaware County Auditor or Ohio Auditor of State with respect to this Policy.

VII. EFFECTIVE DATE

This Policy shall be effective immediately upon adoption and continue in force and effect until amended, superseded, or rescinded.