OhioDAS Service · Support · Solutions | Office of Information Technology

Electronic Transaction Report

In accordance with rule 123:3–1–01 of the Administrative Code, please complete this report. Electronic transactions falling within levels C and D must be submitted to:

DAS-OIT USE
Date Received:

Office of Information Security and Privacy
DAS – Office of Information Technology
30 E. Broad Street, 19th Floor
Columbus, OH 43215
Voice: 614-644-9391
Fax: 614-728-0837
Email: State.ISP@das.ohio.gov.

1. Agency	**2. Date**
3. Electronic Transaction (short name)	
4. Contact Name: Title: Email: Phone: Address:	
5. Project Status (check one) o Initial planning stages o Plan developed o Preparing acquisition of technology or service o Implementing technology or service o Electronic transactions are in place	

6. Requesting (check one)

- o Approval
- o Waiver

7. Description

Briefly describe the proposed set of similar electronic transactions in the context of the use of the legally binding electronic record or signature, the objects and nature of the exchange, the technology and security procedures used to assure authentication (the technology and process including the initial registration process used to assure the identity of person purporting to sign the record), integrity (the technology and the process used to assure that the records have not been changed and can be accessed for as long as the law demands) and nonrepudiation (the technology and process used to associate the electronic signature with the record).

8. Domain (check one)

o Internal State o Business o Citizen

See subsection (E) of rule 123:3-1-01 of the Administrative Code. Please briefly describe the person (individual, business, government employee, etc.) who will be using the electronic transaction with your state agency.

9. Security Assessment

See subsection (F) of rule 123:3-1-01 of the Administrative Code. The security assessment identifies the potential **impact** of a security breach and the **probability** of such a breach occurring. Indicate the level of impact and risk for the particular set of similar electronic transactions and provide a brief narrative explaining how the levels were selected. Then determine the required **security level** as established in the matrix provided in the rule.

Impact

A. Please identify the impact of a security breach (check one):

o Low o Medium o High o Very High

Provide a brief narrative applying the criteria of paragraphs (F)(2-3) of rule 123:3-1-01 of the Administrative Code. Please note that the financial thresholds that are listed in paragraph (F)(3) reference the *average* financial impact for the individual transactions that make up the proposed set of similar electronic transactions.

Risk	B. Please identify the probability or likelihood of someone attempting a security breach in order to obtain something of value such as financial gain, unauthorized access to confidential information, or the ability to harass, embarrass or shock. (check one): o Low o Medium o High Provide a brief narrative applying the criteria of paragraph (F)(4) of rule 123:3-1-01 of the Administrative Code.
Security Level	C. Please identify the security level required for the proposed set of similar electronic transactions as determined by the matrix provided in paragraph (F)(5) of rule 123:3-1-01 of the Administrative Code. o Level A o Level B o Level C o Level D

10. Technologies and Security Procedures Summary

Please identify the technology (including hardware and software under consideration and please specify versions or software levels) and security procedure(s) used for the proposed set of similar electronic transactions (check one):

o Approval:

Specifically explain in an attachment how the proposed technologies and security procedures meet the minimum requirements as identified in paragraph (G) of rule 123:3-1-01 of the Administrative Code. Also, provide information on additional technologies and security procedures that affect the level of assurance of authentication, integrity and nonrepudiation. These additional procedures might include but are not limited to out of band communications (e.g., confirmation sent through standard mail), identity proofing procedures (e.g., initial personal appearance or cross-checking information against multiple databases), additional password rules (e.g. lockout rules, periodic required password changes, etc.), the use of shared secrets or other procedures that increase (or decrease) security and comprehensive database access controls ranging from users to developers.

o Waiver:

Provide the information required by paragraph (K) of rule 123:3-1-01. Specifically explain in an attachment how the proposed technologies and security procedures are equivalent to the minimum requirements as identified in paragraphs (F) and (G) of rule 123:3-1-01 of the Administrative Code (establishing the appropriate level of assurance of authentication including the initial registration process, integrity and nonrepudiation). These technologies and security procedures might include secure technologies not identified in the rule, out of band communications (e.g., confirmation sent through standard mail), multiple database checks, password rules (e.g. lockout rules, periodic required password changes, etc.) or other procedures that increase (or decrease) security. Please attach a justification as to why the rule should not apply to the proposed set of similar electronic transactions and why the requirements of the rule should be waived.

11. Security Policies

Please provide a list (including title and date) of documented agency security policies for physical, network and computer security as related to this electronic transaction set. These documents must be clearly referenced, maintained on file and available for audit.

12. Justification for Use of Biometrics

If the electronic transaction uses a biometric, provide a justification as an attachment for the use of the biometric.

13. Definitions

Transaction

The definition of “transaction” under UETA is “an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs” (section 1306.01 of the Revised Code). In the state government context, this covers transactions between a government agency and citizens, business and other government agencies and includes not only financial exchanges but also filings, registrations, etc. The term does not carry the meaning that is often used in the technical field of a change or update to a database.

Electronic Records

The term “electronic records” as referenced in UETA does not carry the same definition or application as the term “public record” as defined in ORC 149.43. The electronic records that UETA references are much fewer in number than the number of public records that are kept in electronic formats. UETA and the subsequent administrative rule apply only to electronic records that relate to an electronic transaction (section 1306.02 of the Revised Code). Furthermore, the application of UETA for use of electronic records and signatures by state agencies should not be read outside of the context of section 1306.06 (or most of chapter 1306) of the Revised Code. Therefore, the requirements of UETA and the administrative rule only apply to records (in electronic format) that either the law requires to be in writing or that agencies want to have a legal effect. Public records under ORC 149.43 are “any record that is kept by any public office” and not excepted by ORC 149.43. This definition is very broad and includes records beyond the scope of UETA. The fact that a public record is in an electronic format alone is not enough to make it fall within chapter 1306 of the Revised Code.