



# Ohio

Department of  
Taxation

## POLICY

John Kasich, Governor  
Joseph Testa, Tax Commissioner

30 E. Broad St., 22nd Floor  
Columbus, Ohio 43215

(614) 466-2166  
Fax (614) 466-6401

Policy: Password	Number: ODT-303	Effective: August 5, 2013
Issued By: Joseph Testa (Original signature on file with Internal Audit)	Published By: Information Services Division	Four Year Review Date: August 5, 2017

### 1. Authority

The Tax Commissioner issues Ohio Department of Taxation (herein referred to as the "Department") Policy ODT-303 in accordance with Ohio Revised Code (O.R.C.) § 5703.05. O.R.C. § 5703.05 grants the Tax Commissioner powers, functions, and duties including the authority to manage and direct the Department's operations.

### 2. Purpose

The purpose of this policy is to ensure the integrity of all assigned IT assets by establishing parameters by which passwords are created.

### 3. Applicability

This policy applies to all Department employees and contractors.

### 4. Policy

#### 4.1. Computer Systems that Contain Confidential Information

Hard disk encryption, network/LAN, and Department tax administration applications are systems that contain confidential information. These systems are only stated as examples and should not be construed as an exhaustive list.

Password parameters for systems that contain confidential information are as follows:

- 4.1.1. Passwords are not displayed when entered.
- 4.1.2. Passwords must be a minimum of eight characters in length.
- 4.1.3. Passwords allow for non-alphabetic characters (based on system capability).
- 4.1.4. Passwords allow for special characters (based on system capability).
- 4.1.5. Passwords cannot be reused for a period of 18 months (based on system capability).
- 4.1.6. User-level passwords expire in 60 days or less.

- 4.1.7. User accounts will be locked after a maximum of three unsuccessful attempts to gain access. Exceptions are documented and on file in the ISD Security Office.
- 4.1.8. User accounts that have not been used in 30 days will be disabled/revoked (based on system capability).

#### **4.2. Computer Systems that do not Contain Confidential Information**

Outage Database and TrAX are systems that do not contain confidential information. These systems are only stated as examples and should not be construed as a complete and exhaustive list.

Password parameters for systems that do not contain confidential information are as follows:

- 4.2.1. Passwords must be a minimum of eight characters in length.
- 4.2.2. Passwords allow for non-alphabetic characters (based on system capability).
- 4.2.3. Passwords allow for special characters (based on system capability).
- 4.2.4. Passwords do not automatically expire but can be changed by the user as needed.

#### **4.3. Smartphones**

The Department has a system in place to deliver email to smartphones. Access to this system is granted on approval of the applicable Department Deputy Commissioner.

Password parameters for smartphones are as follows:

- 4.3.1. Passwords must be a minimum of four characters in length.
- 4.3.2. Passwords allow for non-alphabetic characters (based on system capability).
- 4.3.3. Passwords allow for special characters (based on system capability).
- 4.3.4. User accounts will be locked after a maximum of ten unsuccessful attempts to gain access. Data will be automatically removed from the device after the tenth unsuccessful attempt to gain access.
- 4.3.5. Passwords do not automatically expire but can be changed by the user as needed.

#### **4.4. Password Management of User Accounts**

- 4.4.1. Department users can contact the Service Desk to obtain a password reset. User accounts that are disabled due to extended periods of absence or inactivity will require a service request be completed prior to access reinstatement.
- 4.4.2. User accounts are associated with a single individual and will not be established for use by more than one person. Exceptions will be made for a very limited number of accounts for generic use have been established for general/public user PCs, Test Lab PCs, and Interview Testing PCs.
- 4.4.3. User accounts of state employees and contractors that have been terminated or transferred to other work units will be deactivated not later than the end of business on

the effective date of the transition. User accounts associated with involuntary terminations will be deactivated immediately upon notification.

- 4.4.4. Passwords sent via email must be sent using secure email (or other approved encryption method). Contact the ISD Security Unit for assistance as needed.

#### **4.5. Password Protection**

- 4.5.1. Passwords are to be treated as sensitive, confidential information.
- 4.5.2. Do not share passwords with anyone, including administrative personnel, IT personnel, or supervisors.
- 4.5.3. Do not use the “Remember Password” or “Save Password” features offered on applications and websites.
- 4.5.4. Written passwords must not be kept within the workspace or with the device. All written passwords must be stored in a secure location (e.g., purse, wallet, etc.).
- 4.5.5. Any password believed to be compromised must be changed immediately. Contact the ISD Service Desk or the ISD Security Unit for assistance.

#### **4.6. System Administrator Responsibilities**

Employees and contractors with administrator access levels are required to sign a Responsibilities Acknowledgement Form indicating their understanding of the responsibilities associated with their elevated level of access. Signed forms will be kept on file in the ISD Security Unit and updated annually.

### **5. Administrative Consequences for Violations**

Employees and contractors may be held civilly or criminally liable for violating laws related to unauthorized disclosure of sensitive information. Employees or contractors may also be subject to disciplinary action, up to and including termination or contract termination, for failure to follow this and other policies related to Departmental networks, email or other IT resources.