Enterprise Authentication Security Standard ("Standard")

1. **Overview.** This Standard establishes the minimum requirements relating to Authentication for Participating Agency Information Technology systems and applications.

2. **Purpose.** The State of Iowa maintains a variety of data and information in its IT systems, including but not limited to confidential information, personally identifiable information, and other sensitive or regulated information. In order to protect this data, information, and systems, it is necessary to adequately Authenticate individuals prior to granting them access to such systems and applications. This ensures such individuals are the true individuals who are authorized to access State systems and applications and the data and information stored, processed, and accessed by and through the same.

3. **Scope/Application.** This Standard applies to all Participating Agencies and any State Personnel of the foregoing. Non-Participating Agencies are encouraged to follow this Standard and other Enterprise IT Governance Documents. This Standard shall be deemed to have been adopted by all Participating Agencies. Participating Agencies may adopt Governance Documents augmenting but not diminishing this Standard. In the event of any conflict or inconsistency between this Standard and a Governance Document adopted by a Participating Agency, this Standard shall prevail.

4. **Definitions.** Capitalized terms not defined herein shall have the same meaning as the corresponding defined term in the following sources, as may be amended from time to time, in the following priority order: Iowa Code Chapter 8B, Iowa Administrative Code Chapter 129; and the Information Technology Governance Document Taxonomy (**"Taxonomy"**). In addition to any other terms specifically defined elsewhere in this Standard, select terms used in this Standard are defined as follows:

   4.1. **"Administrator Account(s)"** means an account with full\elevated privileges on a computer\device, system, or application.

   4.2. "**Authentication"** means the process of establishing confidence in the identity of users of information systems through one of the following methods:

      4.2.1. Something the user knows (*e.g.*, password);

      4.2.2. Something the user has (*e.g.*, phone); or

      4.2.3. Something the user is (*e.g.*, fingerprint).

      Collectively referred to as **"Methods**."

   4.3. "**Digital Certificate(s)"** means a software token containing the user's private key.

   4.4. "**Multi-factor Authentication"** means Authentication using two, or more, Methods. *E.g.*, Google two-factor Authentication.

   4.5. "**Remote"** means an information exchange between network-connected devices where the information cannot be reliably protected end-to-end by a single

organization's security controls. Any exchange across the internet is considered remote.

4.6. "**System Account(s)"** means an account that allows the direct connection of two or more IT systems or applications for the purpose of sharing data and other information resources.

4.7. "**User Account(s)"** means an account with limited privileges to a computer\device, system, or application.

5. Sharing/Display.

5.1. User Accounts shall be assigned to a single individual, not a group or entity.

5.2. Authentication information, including but not limited to passwords, shall not be shared with other State Personnel (including but not limited to co-workers, managers, or help desk staff), Personnel, or any other third parties.

5.3. Authentication information, including but not limited to Passwords, for User Accounts shall not be openly displayed, and systems and applications shall be configured to mask passwords during entry.

6. User Names/Passwords.

6.1. Default administrative and initial passwords for all computers/devices, systems, and applications shall be changed during initial setup/use.

6.2. Social security numbers or other similar identification numbers shall not be used as a user ID or password.

6.3. Passwords shall be:

6.3.1. At least eight (8) characters for User Accounts (except for mobile devices, *see* Enterprise Mobile Device Security Standard).

6.3.2. At least ten (10) characters for accounts with elevated privileges, such as Administrator Accounts or System Accounts.

6.3.3. Comprised of a mixture of numbers, upper and lower-case letters, with at least one special character.

6.4. Passwords shall **NOT** be:

6.4.1. Comprised of a single instance of a dictionary word. Concatenating multiple dictionary words (recommended three (3) or more), is acceptable.

6.4.2. Comprised of or include, in whole or in part, a user's name or username/login.

6.4.3. The same any password used by the user on any personal systems/applications (*e.g.*, banking, shopping, social networking).

6.4.4. Displayed when entered.

6.5. *Password Changes*.

6.5.1. Password Changes: Passwords must be changed whenever the user possesses a reasonable belief their password may have been compromised. For example, if:

6.5.1.1. The user, in either the employment context or in their personal life, has recently been the subject of a phishing attack or other cyber event;

6.5.1.2. The user has lost a device, whether State-issued or personal, on which their password was or other similar passwords were stored, or that contained information that could otherwise be used to discern a password;

6.5.1.3. The password has been or reasonably may have been stolen.

6.5.2. System & Administrator Accounts. Passwords for System and administrator Accounts should be changed at least every ninety (90) days.

6.5.3. Reuse. If/when any password is changed, any new password must be substantially different from the previous six (6) passwords used in connection with that account.

7. Multi-factor Authentication.

7.1. Multi-factor Authentication shall be used for Remote network connections (*e.g.*, VPN or remote desktop), and Remote administrator tasks.

7.2. Multi-factor Authentication shall be used for all cloud-based email accounts as it relates to all users with a State-issued cell phone.

7.3. Multi-factor Authentication shall include a user ID and password\PIN **plus** one or more of the following:

7.3.1. Digital Certificate;

7.3.2. Token\Smart card;

7.3.3. Biometrics; or

7.3.4. One-time authorization code (*e.g.*, pre-printed codes, codes sent via text message, Google 2-step, email or phone call).

8. Encryption. Passwords and password recovery information shall be encrypted at rest and in transit both inside and outside of the Participating Agency.

9. Unsuccessful Login Attempts. User Accounts and Administrator Accounts shall be set to lock after five (5) consecutive unsuccessful login attempts. Such Accounts shall remain locked until they are reset by an individual authorized to do so through an Administrator Account.

10. Account Reset\Recovery. Before an administrator may reset/recover an account/password on behalf of a user or other administrator, the user or administrator for whom account

recovery/reset is sought shall be verified as the individual who is authorized to access/use such account.

10.1. Account administrators shall **NOT** request the following as verification information:

10.1.1. Social security number.

10.1.2. Employee ID number.

10.1.3. Mother's maiden name or answers to personal questions, such as "what was your first car?", which answers can be easily found via social media or social engineering.

10.2. Account administrators may request and confirm the following or deploy the following methods as verification of a user's identity. Account administrators must utilize **at least two (2)** verification methods, including, by way of example only:

10.2.1. Request the user send a text message from a State-issued cell phone provisioned to that specific user;

10.2.2. Request the user place a call from a State-issued phone provisioned to that specific user;

10.2.3. Request the user send an email from a State-issued email account provisioned to that specific user;

10.2.4. Request the user have his or her supervisor/manager do any of the foregoing and through such communication confirm the identity of the user initiating the request;

10.2.5. Request the user provide an answer to a lookup secret (something a user has) previously distributed to the user.

11. Training. State Personnel, including but not limited to directors, officer, employees employees, interns, and board and commission members, and Vendor Personnel shall receive security awareness training covering passwords, social engineering\phishing, malware threats and reporting incidents.

12. Storage.

12.1. Smart cards, and tokens shall not be stored with the corresponding computer\mobile device to which they unlock/permit access.

12.2. Tokens\smart cards shall be secured when not in use.

12.3. Except for hard copy emergency Administrator Account Authentication Information, which information shall be stored in a locked/secured area and restricted to authorized individuals, Authentication information shall not be written down.

12.4. Users shall not use the "remember password" feature, or other similar feature, in any web browser or other system or application.

12.5. Users shall not use any "password keeper," "password wallet," or other like software or application, unless such software has been pre-approved by the Office of the Chief Information Officer for use by Participating Agencies.

13. **Cookies.** Wherever possible, cookies shall be set to expire.

14. **Disabling Accounts.** User Accounts and Administrator Accounts shall be disabled when:

    14.1. The user leaves employment or has been placed on administrative leave.

    14.2. The accounts are inactive for more than ninety (90) days.

15. **Inactivity Timeout.**

    15.1. User Accounts shall timeout after fifteen (15) minutes of inactivity requiring the user to re-Authenticate to access the account.

    15.2. Administrator Accounts shall timeout after five (5) minutes of inactivity requiring the user to re-Authenticate their password to access the account.

16. **Logging.** Logging of Authentication attempts, whether successful or failed, shall be in accordance with the Enterprise Logging Standard.

17. **Vendors/Contractors.** Agencies utilizing Vendor Contractors or Vendor Personnel shall make compliance with this Standard contractual obligations of such Vendor Contractors or Vendor Personnel.

18. **Amendment.** This Standard shall be reviewed at least every two (2) years and amended as needed. This Standard may be amended in the sole discretion of the CIO, taking into consideration the advice and input of the TLG and its various Subcommittees.

19. **Enforcement.** This Standard shall be enforced pursuant to Iowa Administrative Code rules 11— 25.11 and 11—117.11 and Iowa Code sections 8B.21(1)(d), (f), and (h), 8B.23(1), 8B.23(1), and 8B.24(1), as applicable. Upon a finding of a violation of or noncompliance with this Standard, the Office may, by way of example only:

    19.1. Bar or otherwise limit a Participating Agency's use of Contracts entered into by the office;

    19.2. Remove or bar State Personnel of a Participating Agency from participating on IT Governance Subcommittees, work groups, or task forces established, organized, or managed by the Office;

    19.3. Report such violations or noncompliance to the department of management, office of the governor, or auditor of state;

    19.4. Recover administrative fees commensurate with any increased fees incurred by the Office or other Participating Agencies as a result of the violation or noncompliance.

20. **Waiver/Variance.** Iowa Administrative Code rules 11—25.11(2) and 11—117.11(3) and Iowa Code section 8B.21(5) provide for variances\waivers from IT Governance Documents. Requests for a waiver/variance from any of the requirements of this Standard shall be submitted in writing to the Office in accordance with the requirements of those statutes and rules, as applicable.

21. **Dispute resolution.** If a dispute arises between the Office and a Participating Agency as it relates to compliance with or the administration or enforcement of this IT Governance Document, such dispute shall be resolved as provided by Iowa Code section 679A.19.

IN WITNESS WHEREOF, the CIO has caused the CIO's duly authorized representative to execute this Standard, which is effective as of the date of signature below.

Robert von Wolffradt

Digitally signed by Robert von Wolffradt
DN: cn=Robert von Wolffradt, o=State of Iowa, ou=Chief Information Officer, email=cio@iowa.gov, c=US
Date: 2019.01.02 16:42:31 -06'00'

Chief Information Officer of the State of Iowa,
Office of the Chief Information Officer of the State of Iowa