Enterprise Malware Protection Security Standard ("Standard")

1. **Overview.** Anti-Malware protection is necessary to help protect agency systems from various forms of Malware. To that end, this Standard establishes minimum requirements Participating Agencies must following in scanning for, identifying, and removing/remdiating Malware.

2. **Purpose.** The incidents of cyber crime and other forms of cyber threats, including Malware, have only increased in recent years. To that end, this Standard establishes the minimum requirements for Malware protection to ensure agency systems are safe from various forms of Malware.

3. **Scope/Application.** This Standard applies to all Participating Agencies. Non-participating agencies are encouraged to follow this and other Enterprise IT Standards. This Standard shall be deemed to have been adopted by all Participating Agencies. Because this is a minimum Standard, in addition to this Standard, participating agencies may adopt standards augmenting but not diminishing this Standard. In the event of a conflict between this Standard and a standard adopted by a Participating Agency, this Standard shall govern.

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 herein, are defined as follows:

   4.1. **"Host-Based Scanning"** means scanning of an individual device for Malware.

   4.2. **"Malware"** is an application that is covertly inserted into another piece of software (e.g., operating system, application) with the intent to steal or destroy data, run destructive or intrusive programs, or otherwise compromise the victim's data, applications, or operating system.

   4.3. **"Network-Based Scanning"** means scanning of network traffic for Malware.

   4.4. **"Non-Persistent Desktop(s)"** means a virtual desktop configured to return to the original starting point when the user logs off.

5. **Enterprise Malware Protection Security Standard ("Standard").**

   5.1. *Anti-Malware Protection*. Anti-Malware protection software shall be installed in accordance with the following requirements:

      5.1.1. All workstations, laptops and servers (excluding mainframes) shall have anti-Malware protection software installed on them.

      5.1.2. Thin clients and mobile devices shall have Malware protection if available.

5.1.3. Non-Persistent Desktops shall include anti-Malware protection if available.

5.2. *Signatures*. Malware signatures shall be updated at least daily.

5.3. *Alerting*.

5.3.1. Central reporting. Anti-Malware protection software alerts shall be centrally reported to the Participating Agency's IT staff.

5.3.2. Metrics/Logging. The following alert information as it relates to Malware shall be collected\aggregated.

5.3.2.1. Date \ time of Malware detection.

5.3.2.2. Device name.

5.3.2.3. Action taken upon detection.

5.3.3. Review.

5.3.3.1. General rule. Malware alerts shall be reviewed at least daily.

5.3.3.2. Real-time alerts. Real-time alerts shall be generated via email or text and immediately be reported to the Participating Agency's IT staff under the following circumstances:

5.3.3.2.1. If Malware is detected.

5.3.3.2.2. If anti-Malware protection software is disabled.

5.3.3.2.3. If signature update failed.

5.4. *Scans*. Host-Based Scanning and Network-Based Scanning shall be conducted. at least weekly.

5.5. *Removable Media*. Removable media shall be scanned for Malware when it connects to a state system including servers, workstations or laptops\tablets.

5.6. *Removal/Reimaging*. Devices shall be removed\isolated or reimaged in accordance with the following requirements:

5.6.1. Devices shall be removed\isolated from the state and agency network if Malware is identified and the anti-Malware protection software installed on the device in unable to disinfect the device.

5.6.2. Devices shall be reimaged if additional Malware alerts are generated after three (3) attempts have been made to clean the device.

5.7. *Email*. Email file attachments shall be scanned for Malware before they are opened by the recipient.

6. **Vendors/Contractors.** Participating Agencies shall make anti-Malware protection contractual obligations of Vendors and Vendor Contractors Information Technology environments.

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

8. **Enforcement.** This IT Governance Document 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, and 8B.24(1), as applicable. Upon a finding of a violation of or noncompliance with this IT Governance Document, the Office may, by way of example only:

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

   8.2. 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;

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

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

9. **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 IT Governance Document shall be submitted in writing to the Office in accordance with the requirements of those statutes and rules, as applicable.

10. **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 IT Governance Document, 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 16:43:29 -06'00'

Chief Information Officer
State of Iowa