Maine State Government
Department of Administrative and Financial Services
Office of Information Technology (OIT)

User Device and Commodity Application Policy

1.0. Statement

Maine State information and communication technology exists exclusively for official Maine State business. The purpose of this Policy is to ensure that Maine State information and communication technology is best positioned to facilitate official Maine State business, while complying with relevant Federal and State laws, as well as general industry best practices. This policy also contains directives regarding allowable applications, both resident on the device, as well as consumed remotely.

2.0. Definitions

2.1. *Adware:* An application that is specifically designed to display advertising content without the consent of the user.

2.2. *Commodity Cloud Application: An* application that is consumed from the Internet, exclusively on the basis of an (most likely, non-negotiable) End-User License Agreement (EULA) or Terms of Service, i.e., without a dedicated and/or negotiated purchasing contract. Could be either free, or against a usage fee.

2.3. *Hypervisor:* An application, firmware, or hardware that allows multiple virtual machines to run on a single physical machine. Also commonly known as a virtual machine monitor (VMM) or virtualizer.

2.4. *Malware:* An application specifically designed to disrupt, damage, or gain unauthorized access to an electronic device.

2.5. *Messaging App:* An app resident on a mobile device that provides the user interface for sending and receiving messages. At a minimum, such apps support the baseline Short Message Service (SMS) features. The two most popular default Messaging Apps are Google Messages[1] for Android devices, and Apple Messages[2] for iOS devices. These default Messaging Apps do *not* offer encryption.

2.6. *Mobile Devices:* Computing and/or communication devices, running a mobile operating system (such as Google Android and Apple iOS), as opposed to a

[1] https://messages.google.com/
[2] https://apps.apple.com/us/app/messages/id1146560473

workstation operating system (such as Microsoft Windows, Mac OS, Ubuntu, etc.). Includes, but is not limited to, smartphones and tablets.

2.7. *Open-Source Asset:* An application which is created using source code that anyone can inspect, modify, and enhance.

2.8. *Self-Service Platform (SSP):* An application platform that allows for rapid, visual development of applications and/or workflows with considerably-less code compared to traditional coding languages. SSPs are geared toward shared development between business users and IT personnel. Examples: Microsoft Power Apps, Salesforce, Chatbot, etc.

2.9. *Short Message Service (SMS):* The technology protocol for exchanging short text content through mobile devices. The universally supported baseline by mobile carriers and mobile device manufacturers is an upper limit of 160 characters, and no encryption, either at-rest, or in-flight.

2.10. *Plug-in Application:* A software component that adds a specific feature to an existing computer program.

2.11. *Terms & Conditions (End User License Agreement, Terms of Service):* General and special arrangements, provisions, requirements, rules, specifications, and standards that form an integral part of an agreement or contract. For the purposes of this Policy, Terms & Conditions, End User License Agreement (EULA), and Terms of Service are used interchangeably.

2.12. *User Device:* Integrated computing and communication device, intended for end-users. Includes workstations, laptops, notebooks, tablets, smartphones, personal digital assistants, etc. For this Policy, divided into two categories: State-issued, and other devices used to conduct State business.

3.0. Applicability

3.1. This Policy applies to:

- 3.1.1. Maine State Executive Branch personnel, both employees and contractors;
- 3.1.2. User devices using the State network, irrespective of whether they are State-issued or located within other State government branches, or other devices used to conduct State business on the State network; and
- 3.1.3. Applications, both resident on the device, as well as consumed remotely.

4.0. Responsibilities

4.1. Agency Management:

- 4.1.1. Ensure that their personnel are aware of, and compliant with, this Policy.
- 4.1.2. The Agency Management responsibility is especially relevant for commodity cloud applications (see Definitions) that are chosen by Agency Business personnel.

4.1.3. Collaborate with OIT in owning, interpreting, executing, and enforcing this Policy.

4.2. OIT Architecture and Policy:
4.2.1. Facilitates the thorough examination of new technology or application solutioning requests.

4.3. OIT Information Security Office:
4.3.1. Collaborates with Agency Management and OIT Architecture and Policy to ensure all IT commodity cloud applications have been thoroughly vetted for security posture and State risk.

4.4. OIT Management:
4.2.1. Collaborate with Agency Management in owning, interpreting, executing, and enforcing this Policy.
4.2.2. The OIT Account Managers are liaisons with the Agency business partners.

4.3. DAFS IT Procurement Office:
4.3.1. Collaborates with Agency Management and OIT Architecture and Policy to ensure all IT commodity cloud application Terms & Conditions have been thoroughly vetted.

5.0. Directives

5.1. Any personal use of a State-issued user device (see Definitions) must be incidental in nature and must not interfere with official Maine State business.

5.2. Access to State of Maine information assets is only allowed from a State-issued or State-managed user device, approved multi-factor authentication (MFA) option, and approved virtual private network (VPN), if applicable. The use of any personal peripheral device(s) (keyboard, mouse, headphones, monitor, etc.) is allowed ONLY in support of remote telework agreements for State of Maine personnel. Use of personal peripheral device(s) is NOT allowed in State of Maine offices. More information on personal peripheral devices use can be found by searching for the Peripheral Equipment Guide on the MaineIT SharePoint Site (Internal users only).

5.3. Any State-issued user device may be monitored and audited for many purposes, including protecting against unauthorized usage, and ensuring the security and optimal functioning of the Maine State network.

5.4. The operating system of a State-issued workstation is a currently-supported Microsoft Windows client.

5.5. Certain classes of applications are prohibited from use on State-issued user devices. At a minimum, such classes include, but are not limited to, Anonymizers, Peer-to-Peer Utilities, Unauthorized Remote-control Agents, Hypervisors, and Unauthorized Cloud Transfer and Storage applications.

5.5.1. Use of Windows Update Delivery Optimization (WUDO)[3] on State-issued user devices *is* permitted.

5.6. Any unauthorized use of a State-issued user device may result in discipline, up to and including, dismissal.

5.7. Unless instructed to do so in the performance of official duties, State-issued user devices must not be used to create, record, store, copy, transmit, distribute, image, modify, print, download, or display inappropriate or unprofessional materials that demean, denigrate, or harass individuals, or groups of individuals, on the basis of race, ethnic heritage, religious beliefs, disability, sexual orientation, or gender, regardless of whether it was intended to demean, denigrate, or harass any employee or group of employees. This prohibition applies regardless of whether the personnel is on-duty or off-duty.

5.8. Unless instructed to do so in the performance of official duties, State-issued user devices must not be used to create, record, store, copy, transmit, distribute, image, modify, print, download, or display materials that involve nudity, are sexually explicit, or pornographic in nature. This prohibition applies regardless of whether the personnel is on-duty or off-duty.

5.9. State personnel shall not use any State-issued user device for any commercial, outside business, or for-profit activity.

5.10. No State business may be conducted through non-Maine.gov account(s). This prohibition applies irrespective of whether the device is State-issued, or otherwise.

5.11. Unencrypted SMS is *not* suitable for Sensitive (TLP: Amber) or Restricted (TLP: Red) content. Unencrypted SMS is only suitable for transactional communication, such as setting up, and/or confirming, appointments, etc. Under certain circumstances, just name and address may be considered Public (TLP: White) data, unless overridden by Federal and/or State laws, statutes, rules, and regulations. All SMS content is subject to the Maine State Archives records management policy and retention schedules,[4] and the Maine Freedom of Access Act (FOAA).[5] Usage of any special Messaging App (i.e., a Messaging App that is *not* natively bundled with the device operating system) for state business is subject to the appropriate OIT vetting (Item 5.19 of this policy). Details on data classification are defined in the Data Classification Policy.[6]

5.12. Users do not have administrative access to the State-issued user devices assigned to them.

[3] https://cmma.org/cmma-blog/the-pros-and-cons-of-windows-update-delivery-optimization/
[4] https://www.maine.gov/sos/arc/records/state/index.html
[5] https://www.maine.gov/foaa/
[6] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataExchangePolicy.pdf

5.13. A State-issued user device is intended for the exclusive use of designated State personnel. Any use of the State-issued user device by family or friends of the designated State personnel is strictly prohibited.

5.14. A State-issued user device must be returned unconditionally upon the request of the issuing Agency. Typical circumstances include, but are not limited to, termination of employment, conclusion of telework authorization, etc. Violation of this provision may result in referral to law enforcement.

5.15. Only applications that satisfy *all* of these criteria may be installed on State-issued user devices:
- 5.15.1. Agency agreement on business-relevance;
- 5.15.2. Certified safe by OIT from a cybersecurity standpoint;
- 5.15.3. Certified for usage by DAFS IT Procurement (who also verifies with the Attorney General's Office, as needed);
- 5.15.4. Proof-of-purchase, or appropriate free-use license;
- 5.15.5. Availability of the native operating system installer; and
- 5.15.6. Availability of the license key.

5.16. Should there arise any difference of opinion regarding the business-relevance of an application, the OIT Management will conduct a review with Agency Management. If Agency Management agrees on the business-relevance of that application, then that application will be allowed, contingent on fulfillment of the other criteria.

5.17. All applications installed on State-issued user devices must be kept current under the support regime of the original vendor.

5.18. All risk associated with using an end-user application is explicitly borne by the user, and the sponsoring agency.

5.19. This item is about the use of commodity cloud applications for State business and applies irrespective of the user device.

- 5.19.1. Commodity cloud applications that purport to be "free" to individual consumers may not actually be free to Government consumers. Also, many such applications follow the so-called "freemium" model, where a basic version is free, but as the user gets used to the application, certain additional features are charged a fee. Another variant is to make the application free until an arbitrary usage threshold is reached, beyond which a fee is triggered. Either way, any application used for State business must always be compliant with its licensing terms, including all applicable usage fees.

- 5.19.2. Security is foundational to everything else. A commodity cloud application may be a carrier of adware (See Definitions) or malware (see Definitions). If security controls of the commodity cloud application do not meet the minimum requirements of the data being transacted by the application, then

such an application cannot be used for State business. The OIT Chief Information Security Officer (CISO) remains the final arbiter on the suitability of a commodity cloud application for State business.

5.19.3. It is critical to thoroughly review the Terms & Conditions (see Definitions), and all IT applications must be vetted through the DAFS IT Procurement Office before accepting them.

5.19.3.1. The boilerplate Limitation of Liability, Indemnification (State held harmless), and Legal Jurisdiction for dispute resolution are more likely to be in favor of the vendor, as opposed to the State. In most cases, the vendor may be unwilling to modify any of these provisions. This presents an intrinsic risk which any user/agency of the application must assume and may require verification with the Office of the Attorney General if that is acceptable.

5.19.3.2. The OIT Remote Hosting Policy[7] (Section 5.2) explicitly demands that "Data residency always remains within the Continental United States."

5.19.3.3. Data remains a strategic asset for the State, and the State always retains sovereign ownership of its own data. At the end of the engagement, it must be possible to retrieve State data back from the application vendor.

5.19.3.4. Privacy is foundational. Therefore, special attention must be paid to the Privacy provisions of the application vendor. It is common for the vendors of commodity cloud applications to outsource certain functions to other parties. If that is the case, then it is essential to interrogate the Privacy Polices of these other parties as well.

5.19.3.5. All relevant Federal and State Laws, Regulations, Statutes, and Rules remain in full force, including, but not limited to, FOAA[8], Retention[9], and Notice of Risk to Personal Data[10].

5.19.3.6. By default, most vendors enable auto-renewal on a monthly basis. However, it may not always be in the best interests of the State to do so. Therefore, caution must be exercised.

5.20. This item relates to requests for new technology and application solutioning requests for State business and applies irrespective of the user device.

5.20.1. Whenever an agency/user would like to add or purchase a new technology or application, they must either:

5.20.1.1. Send an email to the MaineIT New Technology Requests inbox (MaineIT.NewTechRequests@maine.gov); or

5.20.1.2. Submit a request to the OIT Enterprise Ticketing System, assigned to MaineIT New Tech Requests.

[7] https://www.maine.gov/oit/policies/RemoteHostingPolicy.pdf
[8] http://www.mainelegislature.org/legis/statutes/1/title1ch13sec0.html
[9] https://www.maine.gov/sos/arc/records/state/index.html
[10] http://www.mainelegislature.org/legis/statutes/10/title10ch210-bsec0.html

5.20.2. The email or ticket must include the business justification describing why the new technology or application is necessary for business purposes. The supervisor of the requesting user/agency must be copied on the email to ensure the approval of the request.

5.20.3. OIT facilitates new technology or application requests by completing with subject-matter experts:
- 5.20.3.1. A thorough interrogation of the new technology or application security posture; and
- 5.20.3.2. A thorough interrogation of the new technology or application Terms & Conditions and End User License Agreement.

5.20.4. For all new technology requests with a user base of five (5) users or fewer across the enterprise, OIT, at its discretion, may provide provisional use without a complete review and approval through the Low Volume Low Risk (LVLR) process.
- 5.20.4.1. The complete form for the LVLR review process is included within the OIT Enterprise Ticketing System. An agency supervisor must approve prior to proceeding.
- 5.20.4.2. New technology requests that fail to pass all LVLR criteria will be subject to a full vetting through the new technology solutioning process described above in 5.19.
- 5.20.4.3. OIT may amend or withdraw provisional use notice at any time with or without notice should conditions change, risks be discovered, or new information be identified.
- 5.20.4.4. OIT communicates the outcome for provisional use of all LVLR new technology or application requests back to the agency/user who initiated the request.

5.21. This item relates to the use of plug-in applications (see Definitions) for State business and applies irrespective of the user device.

5.21.1. Whenever an agency/user would like to add an extension or plug-in to an OIT-approved product, they must either:
- 5.21.1.1. Send an email to the MaineIT New Technology Requests inbox (MaineIT.NewTechRequests@maine.gov); or
- 5.21.1.2. Submit a request to the OIT Enterprise Ticketing System, assigned to MaineIT New Tech Requests.

5.21.2. The email or Ticketing Request must include the business justification describing why the extension or plug-in is necessary for business purposes. The supervisor must be copied on the email to ensure the supervisor has approved the request.

5.21.3. OIT reserves the right to immediately deny the request based on obvious weaknesses or the determination that the extension or plug-in is not

necessary for business use, in which case the rejection will be communicated to the requestor within five (5) business days.

5.21.4. Otherwise, as long as the core (or main, or underlying) product is kept fully updated with patches and/or upgrades, any extension or plug-in that does not require an independent operating system installation is granted provisional approval. However, depending upon how the extension or plug-in behaves with respect to other compensating controls resident on OIT-managed devices, and the general opinion of the industry at-large regarding these extensions or plug-ins, and the discretion of the CISO, this provisional approval may be rescinded downstream.

5.22. For any open-source asset (see Definitions), the quality, reliability, privacy, and security of the application is contingent upon the pace and thoroughness with which the open-source community responds to issues as they arise, as opposed to a corporate service level agreement. This presents an intrinsic risk which any user/agency of open-source products must assume. Should a vulnerability with respect to an installed open-source product come to the attention of OIT, OIT reserves the right to uninstall and/or otherwise remediate that product, and/or mandate an alternative product.

5.23. OIT endorses the adoption of a Self-Service Platform (SSP) (See Definitions) by agency (i.e., non-OIT) personnel, if **both** of the below conditions are satisfied:

5.24. The SSP supports the productivity of an individual, and/or the agency workgroup to which this individual belongs; and

5.25. The transacted data is classified at either TLP: Green or TLP: White (See the Data Classification Policy[11]).

5.26. Agency personnel are **not** authorized to adopt SSPs unless both of the above conditions are simultaneously satisfied.

6.0. Document Information

6.1. Initial Issue Date: 22 January 2020
6.2. Latest Revision Date: 11 December 2024
6.3. Point of Contact: Enterprise.Architect@Maine.Gov
6.4. Approved By: Chief Information Officer, OIT
6.5. Legal Citation: Title 5, Chapter 163: Office of Information Technology[12]
6.6. Waiver Process: Waiver Policy[13]
6.7. Distribution: Internet[14]

[11] https://www.maine.gov/oit/sites/maine.gov.oit/files/inline-files/DataClassificationPolicy.pdf
[12] https://legislature.maine.gov/statutes/5/title5ch163sec0.html
[13] https://www.maine.gov/oit/policies/waiver.pdf
[14] https://www.maine.gov/oit/policies-standards