

BRING YOUR OWN DEVICE AGREEMENT

THIS BRING YOUR OWN DEVICE AGREEMENT (“AGREEMENT”) IS ENTERED INTO BETWEEN THE UNDERSIGNED EMPLOYEE (“EMPLOYEE”) AND THE STATE OF OKLAHOMA OFFICE OF MANAGEMENT AND ENTERPRISE SERVICES, INFORMATION SERVICES (“OMES IS”), EFFECTIVE THE DATE THIS AGREEMENT IS EXECUTED BY OMES IS. THE PARTIES AGREE AS FOLLOWS:

INTRODUCTION

The use of a smart device owned by the Employee in connection with State of Oklahoma (“State”) business is a privilege granted to the Employee by the approval of management of the agency for which the Employee works and OMES IS. OMES IS reserves the right to revoke the privilege granted herein if the Employee does not abide by the terms set forth below. The policies referenced herein apply to all State entities and are aimed to protect the integrity of data belonging to the State and ensure the data remains secure. Each Employee who desires to use a smart device owned by Employee in connection with the State must execute this Agreement; however, each agency may also require a separate Bring Your Own Device Agreement be executed in addition to this Agreement. To the extent any provision stated in this Agreement conflicts with and provisions set forth in an agency specific Bring your Own Device Agreement, the provisions set forth in this Agreement herein control except for instances which the conflict is a stricter standard than set forth in this Agreement.

DEFINITIONS

Smart Device: When used in this Agreement, a smart device is defined as a personal computing device that connects directly to the State network services including but not limited to email and calendar services. This definition includes, without limitation, smart phones, PDAs, and tablets.

MDM Solution: An MDM (Mobile Device Management) Solution is the software and service which provides device management, security, and monitoring in order for the smart device to be eligible to connect to the State network.

Nonpublic Information: Nonpublic information is information that the Employee gains during their employment with the State that the Employee knows, or reasonably should know, has not been made available to the public. It includes information that the Employee knows, or reasonably should know:

- Is designated by the State or the agency for which the Employee works as nonpublic information or contains markings such as “Confidential”, “Sensitive”, “Personal”, or similar language;
- Contains Protected Health Information (PHI) or similar nonpublic personal information;
- Is provided to the State or the agency for which the Employee works by customers or third parties under agreement and with the understanding that it will be treated as confidential, nonpublic information; or
- Contains information related to the internal state or agency capabilities and operations that is not available to the public or that an individual could use to negotiate or otherwise circumvent security controls.

ELIGIBILITY

OMES IS reserves the right, without prior notice to the Employee, to disable or disconnect some or all services related to connection of a personal smart device to the State network. The following criteria will be considered by OMES IS, initially and on a continuing basis, to determine if the Employee is eligible to connect a personal smart device to the State network:

- Sensitivity of data the Employee can access;
- Legislation or regulations prohibiting or limiting the use of a personal smart device for State business;
- The personal smart device hardware and operating system version must be supported by the State's MDM solution providers;
- The Employee's adherence to the terms of this Agreement and the Acceptable Use Policies (hereafter defined); and
- Technical limitations and other eligibility criteria deemed relevant by OMES IS.

Reimbursement Considerations

The Employee is personally liable for the smart device and carrier service costs and is not eligible for expense reimbursement for hardware or carrier services. Accordingly, OMES IS will NOT reimburse the Employee for any loss, cost or expense associated with the use or connection of a personal smart device to the State network, including but not limited to:

- Expenses for voice minutes used to perform State business;
- Data charges related to the use of State data services;
- Expenses related to text or other messaging;
- Cost of handheld devices, components, parts, or data plans;
- Cost of replacement handheld devices in case of malfunction whether or not the malfunction was caused by using applications or services sponsored or provided by the State;
- Loss related to unavailability of, disconnection from or disabling the connection of a smart device to the State network; and
- Loss resulting from compliance with this Agreement or applicable State laws, rules or policies.

SECURITY CONSIDERATIONS

Compliance by the Employee with the State of Oklahoma Information Security Policy, Procedures, Guidelines - Mobile Computing Devices: Acceptable Use Policy and the State of Oklahoma Information Security Policy, Procedures, Guidelines – Removable Media: Acceptable Use Policy (“Acceptable Use Policies”) are a prerequisite to and continuing condition of the Employee's privilege to connect a personal smart device to the State network MDM servers. The level of application of the Acceptable Use Policies will depend on the smart device limitations.

Additional considerations to the Acceptable Use Policies include but are not limited to:

- The global password for a Mobile Computing Device that is also a Removable Media Device will consist of a minimum of four (4) non-consecutive, non-repeating characters which shall be changed every 60 days. The grace period for device lock shall be zero minutes and the maximum number of failed attempts shall be three (3); and

- The Employee acknowledges in the event of a remote wipe of the personal smart device to erase State data such remote wipe could impact personal data that is co-mingled within the secure state partition on the personal smart device. OMES IS recommends that the Employee take additional precautions, to backup personal data, and not to co-mingle personal data within the secure partition on the personal smart device and the State will not be responsible for loss of personal data in any event.

ACCEPTABLE USE

The Employee will use the personal smart device in an ethical manner and will not use the personal smart device in a way not designed or intended by the manufacturer including “jailbreaking” or any other use that could circumvent any controls that separate State data from personal information. The Employee will not allow or install applications on the personal smart device to access the secure State partition on the device.

Use of the personal smart device to remove sensitive information from State networks, attack State assets or circumvent current security settings and policies or violation of the Acceptable Use Policies or any other applicable State policy related to the subject matter of this Agreement will result in a wipe of the secure partition or the entire smart device.

SUPPORT EXPECTATIONS

OMES IS will offer the following limited support for the personal smart device:

1. Connectivity to OMES IS servers including email, calendar and other services as deemed appropriate
2. Security services including policy management, password management and remote wiping in case of loss, theft, device failure, device upgrade or change of ownership.

Employee is responsible for obtaining and paying for all other technical support services from their mobile communications provider or device manufacturer.

OMES IS is not responsible to the Employee for network or system outages that result in a failure of connectivity to the State network.

EMPLOYEE ACKNOWLEDGEMENT & CONSENTS

The Employee acknowledges and consents to OMES IS’ right to exercise and enforce a range of security, privacy, and management controls on Employee’s smart device including, but not limited to the mandatory use of device passwords; timeouts; device and media encryption; geo-location tracking; and, remote wipe of State applications and data. Employee further acknowledges to cooperate with the agency and OMES IS to satisfy legitimate discovery requests arising out of administrative, civil or criminal proceedings which could result in surrounding the personal smart device assigned to the Employee.

The Employee acknowledges and consents to OMES IS’ right to monitor or inspect State applications and data. Employee further acknowledges that, in doing so, the State could inadvertently access personal information on the personal mobile device. As such, Employee should not have any expectation of privacy related to the use of a smart device connected to the State network.

The Employee acknowledges the responsibility to report the loss, theft, or destruction of the Employee's enrolled personal mobile device to the OMES IS Service Desk immediately and to notifying the service desk of an upgrade, repair, or trade-ins 48 hours in advance. The Employee acknowledges violation of this agreement may be cause for disciplinary action, up to and including termination.

EMPLOYEE RESPONSIBILITIES

When the use of personally owned smart devices is necessary to conduct State business and appropriately authorized, Employee assumes certain responsibilities and shall:

- Follow all relevant elements of the Employee's agency and State security/privacy policies and standards when accessing State-provided mobile applications and data;
- Abide by all federal and State laws concerning the use of mobile devices when driving and strict prohibition against using messaging functionality including text messaging, calendar or email functions while operating a motor vehicle or engaging in other activities when the concurrent use of the device could result in the harm of the user or others;
- Ensure timely payment of all fees, taxes, and surcharges associated with the use of Employee-owned devices to connect to and access State-provided systems and data;
- Maintain the device in accordance with manufacturer or carrier recommendations including the prompt implementation of recommended operating system and software upgrades;
- Not "jail break" the device or otherwise install or modify the software that allows the user to alter or bypass standard built-in security features and controls;
- Not enable potentially dangerous mobile services while accessing State information services that can export or transmit nonpublic information to unauthorized devices without the user's knowledge (for example serving as a mobile hotspot or enabling Bluetooth or Near Field Communications (NFC) network services without using PINs and other recommended safeguards that prevent unauthorized devices from connecting while connected to State information services);
- Not modify or disable security features implemented by OMES IS through our mobile device management system(s) (for example geo-location services, password controls and device/media card encryption);
- Not share or otherwise allow access to the device by others;
- Not transfer or allow the transfer of nonpublic information from the smart device to any device not specifically authorized by the State to receive such information including the use of unapproved cloud-based storage locations or synchronization of State data between participating smart devices and other personal computing devices;
- Cooperate with OMES IS in wiping the approved personal smart device of all State applications and data upon termination of employment or Employee decision to "opt-out" of the BYOD program; and
- Cooperate with the agency and OMES IS to satisfy legitimate discovery requests arising out of administrative, civil or criminal proceedings or Open Record Requests.

RELEASE OF LIABILITY AND DISCLAIMER

The Employee's use of the personal smart device as contemplated herein carries specific risks for which the Employee assumes full liability including, but not limited to, an outage or crash of any or all of the State network, programming and other errors, bugs, viruses, and other software or hardware failures resulting in the partial or complete loss of data or which render the smart device inoperable.

The State expressly disclaims, and the Employee releases the State from, all liability for any loss, cost or expense of any nature whatsoever sustained by the Employee in connection with the privilege afforded the Employee under the terms of this Agreement and the State expressly reserves the right to wipe the smart device as set forth in the Acceptable Use Policies or herein.

MISCELLANEOUS PROVISIONS

There are no third party beneficiaries of this Agreement and this Agreement may not be amended except by a writing signed by the Employee, management of OMES IS and management of the State agency for which the Employee works. Paragraph headings are intended for descriptive purposes only and are not intended to infer additional meaning to the terms set forth herein.

[Employee]

Date

[Agency Management]

Date

[OMES IS Management]

Date