BRING YOUR OWN DEVICE AGREEMENT

THIS BRING YOUR OWN DEVICE AGREEMENT ("AGREEMENT") IS ENTERED INTO BETWEEN THE UNDERSIGNED EMPLOYEE ("EMPLOYEE") AND THE OKLAHOMA MUNICIPAL ASSURANCE GROUP ("OMAG"), EFFECTIVE THE DATE THIS AGREEMENT IS EXECUTED BY OMAG. THE PARTIES AGREE AS FOLLOWS:

INTRODUCTION

The use of a smart device owned by the Employee in connection with OMAG business is a privilege granted to the Employee by the approval of the director of the department for which the employee works. OMAG 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 of OMAG and are aimed to protect the integrity of data belonging to OMAG and ensure the data remains secure.

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

When used in this Agreement, the "OMAG network" is defined as any technology services, whether cloud-based or on-premises in the OMAG headquarters, that are used by OMAG staff for communication, file storage, applications and databases, and other business functions.

ELIGIBILITY

OMAG 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 OMAG network. The following criteria will be considered, initially and on a continuing basis, to determine if the Employee is eligible to connect a personal smart device to OMAG network:

- Sensitivity of data the Employee can access;
- Legislation or regulations prohibiting or limiting the use of a personal smart device for OMAG business;
- The personal smart device must be listed on the supported device list;
- 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 OMAG Technology Services.

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, except for any existing cell-phone stipends provided to OMAG Exempt employees only. Accordingly, OMAG will NOT reimburse the Employee for any loss, cost or expense associated with the use or connection of a personal smart device to the OMAG network, including but not limited to:

- Expenses for voice minutes used to perform OMAG business;
- Data charges related to the use of OMAG 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 OMAG;
- Loss related to unavailability of, disconnection from or disabling the connection of a smart device to the OMAG network; and
- Loss resulting from compliance with this Agreement or applicable State laws, rules or policies

SECURITY CONSIDERATIONS

Compliance by the Employee with all OMAG policies, including but not limited to the Acceptable Use Policies, the Employee Handbook, and the Remote Access Device Policy for Non-Exempt Employees are a prerequisite to and continuing condition of the Employee's privilege to connect a personal smart device to the OMAG network. 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) characters.
- The Employee is responsible to ascertain if, in the event of a remote wipe, the personal smart device allows only OMAG data to be erased or if personal data is vulnerable. OMAG recommends that the Employee take additional security precautions and OMAG will not be responsible for loss of personal data in any event.
- At any point, Technology Services, the CEO, and the Department's Director may require certain software be utilized on an employee's personally owned smart device that provides the following capabilities to protect OMAG's data assets and ensure compliance:
    - Remote-wiping or remote data destruction capabilities, should the phone be lost or stolen
    - Encryption of data on the device, which may not be limited to email, calendaring, or other OMAG data.
    - Remote monitoring of device logs and system activity, the device's location, and other device data required for any Mobile Device Management software or policies.

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 OMAG data from personal information.

The Employee will inform OMAG Technology Services, pursuant to the Acceptable Use Policies, within 48 hours if the personal smart device is lost, stolen, destroyed, upgraded, or a change of ownership has occurred.

Use of the personal smart device to remove sensitive information from OMAG, attack OMAG assets or circumvent current security settings and policies or violation of the Acceptable Use Policies or any other applicable OMAG policy related to the subject matter of this Agreement will result in an initiation of a remote wipe or an account lockout of the device to protect OMAG assets. In addition, such use or

violation is cause for immediate termination, without notice to the Employee, of this Agreement by OMAG and could subject the Employee to disciplinary action, termination, and legal action.

SUPPORT EXPECTATIONS

OMAG Technology Services will offer the following limited support for the personal smart device:

1. Connectivity to OMAG Email servers including email and calendar and
2. Security services including policy management, password management and remote wiping in case of loss, theft, device failure, device upgrade or change of ownership.

OMAG Technology Services is not responsible to the Employee for network or system outages that result in a failure of connectivity to the OMAG network.

The level of support for the Employee's smart device offered by any third-party software, if any, can be provided upon request.

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 OMAG 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.

OMAG expressly disclaims, and the Employee releases OMAG 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 OMAG 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 OMAG Technology Services and management of the department 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.