**Mobile and Non-State Device Agreement**

**Please read carefully prior to signing**

*Please place the completed, signed form on file with the employee’s Agency Information Security Officer (ISO) or ISO designee.*

**Employees cannot be coerced to use personal devices, and management cannot require any employee use personal devices to conduct State business.**

This agreement between the agency and employee identified below serves to authorize the use of a Mobile Device (MD) on and within State of Nevada network and IT facilities, **whether personally owned by the employee, or issued to the employee by the agency.** This agreement also serves to authorize the use of a non-mobile personal device on and within the State network and IT facilities.

Any change in the particulars of this agreement, including change of device, change to email address, name changes, or significant change of authorized applications and/or data, require that this agreement be renewed and re-executed.

|  |  |  |  |
| --- | --- | --- | --- |
| Agency: |  |  |  |
| Employee Name: |  | Employee Email Address: |  |

This agreement covers the following Device(s):

|  |  |  |  |
| --- | --- | --- | --- |
| Device Type | Manufacturer/Model | Serial Number | Personal or State Provided? |
|  |  |  |  |

The **Agency Manager** is responsible to:

* Authorize the employee’s Device in support of the approved application(s) and data.
* Understand and enforce all provisions of PSP S.4.02.02 – Mobile and Non-state Device Security Management.
* Work with the employee to establish appropriate physical and data security controls for Devices that are approved to contain state data.
* Maintain an inventory of all Devices issued to, or allowed to be used under this agreement, by the employee, whether in use or not.
* Ensure established security controls are consistently utilized by the employee.
* Assure that a security incident form is generated and appropriately filed in the event of an IT security-related incident.

The **Employee** is responsible to:

* Understand and adhere to all provisions of PSP S.4.02.02 – Mobile and Non-State Device Security Management.
* Completely fill out this form and submit to the agency manager for signature.
* Protect the Device and data from loss, destruction, unauthorized access or modification, or disclosure.
* Ensure storage encryption is enabled on the Mobile Device and anti-malware software is present and kept updated.
* Immediately report loss or theft of the Device, or suspected IT security breach to the agency ISO and agency manager.
* Review PSP S.4.02.02 annually and renew this Mobile and Non-State Device Agreement.
* Understand the Mobile Device may be remotely reset to factory defaults or wiped of information in the event of a suspected security incident or risk of data loss.

The following State software programs, and their data, are authorized to be installed on the Device:

|  |
| --- |
|  |
|  |
|  |

**The parties hereto represent and acknowledge that they have decided to enter into this Agreement voluntarily, knowingly, and without coercion of any kind.**

|  |  |
| --- | --- |
| **Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  |
| (Employee Signature)  |  (Date)  |
| **Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  |
| (Agency Manager Signature)  |  (Date)  |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  |
| (Agency Manager Printed Name)  | (Telephone Number)  |
|  |  |
| **Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  |
| (Agency ISO Signature)  |  (Date)  |
| **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | **\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  |
| (Agency ISO Printed Name)  | (Telephone Number)  |

\*The signatures above indicate understanding and acceptance of the document by the agency and employee.