Personally Owned Device Policy Sample

(Required Written Policy if Allowed)

1.0 Purpose

A personally owned information system or device shall be authorized to access, process, store or transmit *[agency name]*, Michigan, or FBI Criminal Justice Information (CJI) only when these established and documented specific terms and conditions are met. This control does not apply to the use of personally owned information systems to access the *[agency name]*'s information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

2.0 Scope

This policy applies to all *[agency name]* personnel, support personnel, and/or private contractors/vendors who are authorized to use personally owned devices to connect to any physical, logical, and/or electronic premise of the *[agency name]* to access, process, store, and/or transmit CJI. This also includes any private contractors/vendors who will conduct maintenance on any network device that processes, stores, and/or transmits CJI.

3.0 Personally Owned Devices

A personally owned device is any technology device that was purchased by an individual and was not issued by the *[agency name]*. A personal device includes any portable technology like camera, USB flash drives, USB thumb drives, DVDs, CDs, air cards and mobile wireless devices such as Androids, Blackberry OS, Apple iOS, Windows Mobile, Symbian, tablets, laptops or any personal desktop computer. Threats to mobile handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services.

The *[agency name]* will maintain management control and authorize the use of personally owned devices. The *[agency name]* shall develop guidelines to define which employees can use their own devices, the types of devices they can use, and which applications and data they can access, process, or store on their devices.

Personally owned devices must:

- Be authorized by *[agency name]* to access, process, transmit, and/or store CJI.
- Be inspected by *[agency name]*'s IT staff and the LASO to ensure appropriate security requirements on the device are up-to-date and meet the FBI's *CJIS Security Policy* requirements prior to use.
- Take necessary precautions when using device outside of a physically secure area. (*See Physical Protection Policy)*.

4.0 Remote Access

The *[agency name]* shall authorize, monitor, and control all methods of remote access to the information systems that can access, process, transmit, and/or store CJI. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency controlled network (e.g., the Internet).

The *[agency name]* shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The *[agency name]* shall control all remote accesses through managed access control points. The *[agency name]* may permit remote access for privileged functions only for compelling operational needs but shall document the rationale for such access in the security plan for the information system.

Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

5.0 Roles and Responsibilities

5.1 Owner Role: The owner agrees to:

1. Follow necessary policy and procedures to protect CJI.
2. Bring the device to work to use during normal work hours and not share the device with anyone else.
3. *[Agency name]* having the authority to erase device remotely as needed.
4. Protect individual's and *[agency name]*'s privacy.
5. Use good judgement before installing free applications. Sometimes free applications track your personal information with limited disclosure or authorization, and then sell your profile to advertising companies.
6. Use good judgement on amount of time applied to personal use of personally owned devices during normal work business hours.
7. Access CJI only from an approved and authorized storage device.
8. Do not stream music or videos using personally owned devices when connected to *[agency name]*'s network to prevent sluggishness.
9. Report lost or stolen mobile or storage devices to the *[agency name]'*s Local Agency Security Officer (LASO) immediately.
10. Review the use of device alerts and update services to validate you requested them. Restrict notifications not requested by looking at your device's settings.
11. Control wireless network and service connectivity. Validate mobile device default settings are not connecting to nearby Wi-Fi networks automatically. Some of these networks, like in airports or neighborhood coffee shops, may be completely open and unsecure.

5.2 Information Technology Role

The *[agency name]* IT support role shall, at a minimum, ensure that external storage devices:

1. Are encrypted when CJI is stored electronically.
2. Are scanned for virus and malware prior to use and/or prior to being connected to the agency's computer or laptop.

The *[agency name]* IT support role shall, at a minimum, ensure that all personally owned devices:

1. Apply available critical patches and upgrades to the device operating system.
2. Are kept updated with security patches, firmware updates and antivirus.
3. Are configured for local device authentication.
4. Use advanced authentication and encryption when CJI is stored and/or transmitted.
5. Be able to deliver built-in identity role-mapping, network access control (NAC), AAA (Authentication, Authorization, and Accounting) services, and real-time endpoint reporting.
6. Erase cached information when session is terminated.
7. Employ personal firewalls.
8. Minimize security risks by ensuring antivirus and antimalware are installed, running real time and updated.
9. Be scanned for viruses and malware prior to accessing or connecting to *[agency name]* CJIS network.
10. Configure Bluetooth interface as undiscoverable except as needed for pairing, which prevents visibility to other Bluetooth devices except when discovery is specifically needed.
11. Be properly disposed of at end of life. (*See Media Sanitation Destruction Policy).* Remove CJI before owner sells their personally owned devices or sends it in for repairs.
12. Evaluate personally owned device age. Older device hardware is too outdated for needed updates. Typical life is two years.
13. Ensure device is compatible with needed network protocols and/or compatible with customized applications developed for access CJI through testing.
14. Deploy Mobile Device Management or SIM card locks and credential functions. The credential functions require a pass code to use [agency name]'s network services. *(Research enterprise mobile device management solutions- see product working successfully in real life scenario with*

the type of mobile device your State/Agency wants to use prior to implementing. The enterprise mobile device solution must be compatible with chosen device products.)

15. Ensure owner and IT staff have mobile backup enabled to an approved *[agency name]* location. Set a daily or weekly schedule to periodically synch data and applications. If backup contains CJI, take appropriate security measures for storage of CJI. (*See Media Protection Policy)*.
16. Retain the ability to secure, control and remotely erase agency data on employee-owned devices in the event of a security breach or if the employee leaves the agency employment or the device is lost or stolen. This remote ability can be done through technology that allows virtual access to company applications.
17. Enable mobile device in a "find my phone" service to allow finding device.
18. Consider adding extra protection such as a total device reset if the PIN is guessed incorrectly a certain number of attempts.
19. Be able to easily identify connected users and devices. Track, log and manage every personally used device allowed to connect to agency technology resources for secure CJI access.
20. Perform pre and post-authentication checks.
21. Ability to allow and deny access. Selectively grant proper network access privileges.

5.3 Local Area Security Officer (LASO)

The LASO will:

1. Identify who is using the personally owned approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

6.0 Penalties

Violation of any of the requirements in this policy by any authorized personnel will result in suitable disciplinary action, up to and including loss of access privileges, civil and criminal prosecution and/or termination. Personally owned information technology resources used may be retained by the *[agency name]* for evaluation in investigation of security violations.

Violation of any of the requirements in this policy by any unauthorized person can result in similar disciplinary action against the device owner, and can also result in termination of services with any associated consulting organization or prosecution in the case of criminal activity.

7.0 Acknowledgement

The *[agency name]*, agency personnel, IT support, private contractors/vendors, and the LASO alike will agree to commit to this personally owned device document (policy).

I have read the policy and rules above and I will:

- Authorize the *[agency name]* to remotely wipe my mobile device.
- Abide by the *[agency name]* Personally Owned Device policy. I understand any violation of this policy may result in discipline up to and including termination.
- Complete the security awareness training and take action to protect *[agency name]* facilities, personnel and associated information systems.
- Report any unauthorized device access to *[agency name]* LASO.

Signature: _____Date:_____/20____

Questions

Any questions related to this policy may be directed to the [agency name]'s LASO:

LASO Name:	LASO Phone:	LASO email:
State CSO/ISO Name:	CSO/ISO Phone:	CSO/ISO email:

Other Related Resources:

- Media Sanitization and Destruction Policy (Required)
- Media Protection Policy (Required)
- Physical Protection Policy (Required)