


# FORT SMITH POLICE DEPARTMENT

## POLICIES AND PROCEDURES

<b>SUBJECT</b>	<b>Mobile Device Usage and Agreement Policy</b>		
<b>NUMBER</b>	<b>1109.05</b>	<b>EFFECTIVE DATE</b>	<b>August 28, 2008</b>
<b>Scheduled Review Date</b>	<b>Annually beginning October 1</b>	<b>ISSUE DATE</b>	<b>August 28, 2008</b>
<b>Date Reviewed</b>		<b>REVISION DATE</b>	<b>January 7, 2022</b>
<b>APPROVED BY</b>		<b>CALEA STANDARDS</b>	<b>L.E. 41.3.7</b>

### I. Purpose

- A. The purpose of this policy is to define standards, procedures, and restrictions for connecting to the Fort Smith Police Department's internal network(s) or related technology resources via any means involving mobile devices. This policy applies to any personal digital assistant (PDA) hardware and related software that could be used to access corporate resources, even if said equipment is not departmentally owned or supplied. The overriding goal of this policy is to protect Fort Smith Police Department technology-based resources (such as sensitive data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attacks. This policy applies to all users employing mobile device-based technology to access Fort Smith Police Department technology resources.

### II. Scope

- A. This policy applies to all Fort Smith Police Department (FSPD) employees, including full and part-time staff, volunteers, contractors, and other agents who utilize company-owned, personally-owned, or publicly-accessible mobile device-based technology to access the department data and networks. Access to enterprise network resources is assigned on an as-needed basis.
- B. The addition of new hardware, software, and/or related components to provide additional mobile device-related connectivity within department facilities will be managed at the discretion of the Chief of Police, or the Chief's designee. Non-sanctioned installations of mobile device-related hardware, software, and/or related components to gain access to department computing resources are strictly forbidden.
- C. This policy is complementary to any other policies dealing specifically with network access, wireless access, and remote access to the department network.

### III. Supported Technology

All mobile data devices and related connectivity points within the department firewall will be centrally managed by the Fort Smith Police Department Information Technology (IT) staff and will utilize encryption and strong authentication measures. Although IT is not able to manage the public network to which wireless-enabled mobile devices and smart phones initially connect, end-users are expected to adhere to the same security protocols while

Page 1 of 4	Effective Date: 08-12-08
Subject: Mobile Device Usage and Agreement Policy	Number: 1109.05

utilizing this equipment. Failure to do so will result in immediate suspension of all network access privileges. Personally owned devices may not be allowed access to department wireless networks.

#### **IV. Eligible Users**

- A. All Fort Smith Police Department employees, both full and part-time.
- B. Volunteers.
- C. Employees may use privately-owned mobile data devices (must be supported by IT) for business purposes. If this is the case, the Fort Smith Police Department IT staff must approve the specific handheld and connection as being secure and protected. However, the IT department will not technically support third-party wireless hardware or software, or any other unapproved remote email connectivity solution.

#### **V. Policy and Appropriate Use**

- A. It is the responsibility of any FSPD employee who connects to the department network via mobile data device to ensure that all components of this connection remain as secure as network access within the office. It is imperative that any wired (sync cord, etc.) or wireless connection, including, but not limited to, mobile data devices and service, used to conduct Fort Smith Police Department business, be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account and disciplinary action. The following rules must be observed:
  - 1. Employees using mobile data devices and related software to connect to Fort Smith Police Department technology infrastructure will use secure remote access procedures, including RSA and Two-Factor Authentication. This will be enforced through strong and encrypted passwords in accordance with the Fort Smith Police Department password policy.
  - 2. All mobile data devices used for business interests, whether personal or company-owned, must display reasonable physical security measures. Users are expected to secure all handhelds and related devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, power-on passwords. Any non-corporate computers used to synchronize with PDAs will have installed whatever antivirus software deemed necessary by the Fort Smith Police Department IT department. Antivirus signature files must be updated in accordance with existing policy.
  - 3. Prior to initial use for connecting to the FSPD network, all mobile device-related hardware, software, and related services must be registered with IT.
  - 4. Remote users using non-department network infrastructure to gain access to department resources via their mobile device must employ for their devices and related infrastructure a department-approved personal firewall, virtual private network (VPN), or other security measure deemed necessary by the IT department. VPNs supplied by the wireless service provider should also be used, but only in conjunction with Fort Smith Police Department's additional security measures. IT will support its sanctioned hardware and software, but is not accountable for conflicts or problems whose root cause is attributable to a third-party product.
  - 5. Any mobile data that is configured to access Fort Smith Police Department

Page 2 of 4	Effective Date: 08-12-08
Subject: Mobile Device Usage and Agreement Policy	Number: 1109.05

resources via wireless or wired connectivity must adhere to the authentication requirements of the Fort Smith Police Department's IT department. In addition, all hardware security configurations (personal or company-owned) must be approved by the Fort Smith Police Department's IT department.

6. Employees, contractors, and temporary staff will make no modifications of any kind to departmentally-owned and installed hardware or software without the express approval of the Fort Smith Police Department's IT department. This includes, but is not limited to, installation of mobile device software on company-owned desktop or laptop computers, connection of sync cables and cradles to company-owned equipment, and use of departmentally-owned wireless network bandwidth via these devices.
7. Employees, contractors, and temporary staff with a Fort Smith Police Department sanctioned wireless-enabled mobile device must ensure that their computers and handheld devices are not connected to any other network while connected to the Fort Smith Police Department's network via remote access.
8. All connections that make use of wireless mobile device access will be forced a "time-out" setting. In accordance with FSPD security policies, sessions will time out after thirty (30) minutes of inactivity, and will terminate after eight (8) hours of continuous connection. Both time-outs will require the user to reconnect and re-authenticate in order to re-enter Fort Smith Police Department networks through a wireless mobile device connection.
9. The mobile-based user agrees to immediately report any incident or suspected incidents of unauthorized access and/or disclosure of departmental resources, databases, networks, etc., to a supervisor.
10. Anyone accessing and/or connecting to Fort Smith Police Department networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.
11. Any/all expenses associated with personally owned mobile devices, and monthly wireless data services, will not be reimbursed by the department.
12. All expense forms for reimbursement of cost (if any) incurred due to the need for mobile data-based access for business purposes must be submitted to the appropriate supervisor. Financial reimbursement processing for mobile data devices and related equipment is not the responsibility of the IT staff. If you foresee an upcoming need for mobile data use in a business context, ask your supervisor to help you with the business request.
13. The department IT Network Manager reserves the right to turn off, without notice, any access port to the network that places the department's systems, data, users, and clients at risk.
14. Browsing the Internet using mobile devices configured by the department will be subject to the department's Internet Filtering policy as outline by the Internet Global Default policy.

## **VI. Policy Non-Compliance**

Page 3 of 4	Effective Date: 08-12-08
Subject: Mobile Device Usage and Agreement Policy	Number: 1109.05

- A. Failure to comply with the Mobile Device Usage and Agreement Policy may result in disciplinary action as well as the suspension of any or all remote access privileges.

Page 4 of 4	Effective Date: 08-12-08
Subject: Mobile Device Usage and Agreement Policy	Number: 1109.05