MESA POLICE **Department Policy Manual**	**Telecommuting Protocols**	**DPM 1.10.100** Effective 02/20/2013 Revised 06/20/2018
Approved by: **Chief of Police**	**Chapter:** Information Technology	**Page:** **1 of 3**

1. PURPOSE

This policy provides Mesa Police Department (MPD) members with telecommuting protocols and procedures for implementing City of Mesa (COM) Management Policy 327 Teleworking at MPD where remote access to the MPD network and/or City Local Area Network (LAN) is required.

2. GENERAL

A. This policy applies to all Department members, reserves, volunteers, and Cadet post members.
B. This policy does not replace COM Management Policy 327 Teleworking. It establishes policies and procedures for MPD that will allow members remote access and remain in compliance with agreements with NCIC, ACIC, and other Criminal Justice agencies.
C. All telecommuting requests shall be approved by the Chief of Police.

3. APPROVALS, ACCESS AND PROCESS

3.1 Off-Site Telecommuting Approvals

A. All requests for off-site telecommuting remote access to the COM network and police domains shall be approved by the Chief of Police or Executive Officer.
   1. Use only COM or MPD authorized software or computer equipment.
   2. Comply with all NCIC, ACIC, and MPD guidelines, policies, regulations, orders and laws.

3.2 Approved Access

A. Direct dial in access to police domains is generally prohibited by Arizona Department of Public Safety (DPS) regulations.
B. Remote access to police domains is through a secure website that is subject to DPS security guidelines.

3.3 Off-Site Telecommuting Process

A. The MPD Information Technology (PDIT) Unit coordinates all requests for remote access to the police station.
B. If access to COM network is necessary, PDIT will coordinate with the COM Information Technology Division (ITD) and Security Administration to enable access.

C. Any required software license fees are the responsibility of the member's unit. These fees are based on license agreements with the vendors and where the software actually runs in the remote environment.

D. Members being granted remote access shall not share their User ID, password, RSA token passcode, or record the information where it would be available to family, friends or other unauthorized person.

   1. Do not store the User ID and password in the log on dialog box to eliminate the typing of the User ID and/or password at time of log on.

E. The telecommuter is responsible for absorbing any costs related to the initial set-up (e.g., remodeling, furniture) of their designated workspace. Refer to COM Management Policy 327 Teleworking.

F. Telecommuters shall not extract or copy and store information from criminal justice systems or files on any PC not owned by MPD.

4. REMOTE ACCESS

4.1 Requesting Remote Access

A. Complete the "Telecommuter Agreement" request for Off-Site (Telecommuting) Work as outlined in COM Management Policy 327 Teleworking.

B. The request will be routed through member's chain of command to the Chief of Police or designee.

C. Upon approval and the completion of the "Telecommuter Agreement" request the Chief of Police or designee forwards a copy of the request approval to the PDIT Security.

D. Include the following information or attachments on request for approval of Off-Site (Telecommuting) Work:

   1. Justification for need of remote access to the COM network and police domains.
   2. Completion of the "Telecommuter Agreement" and approval of the Chief of Police or designee.
   3. Address of location of PC to be used for remote access and phone number.
   4. Technical description of the PC, operating system and anti-virus program running the PC.
      a. Basic security software, such as anti-virus programs, is required on the member's PC and shall be kept up to date.
      b. The PD remote access secure website uses software to enforce the use of basic security software, including anti-virus programs.
   5. List application and server areas needed for telecommuting.

6. Description of method the member will use to secure the computer system from use by other individuals and/or access to city and criminal justice that resides on computer system.

E. Access is granted at the level of service being provided by ITD and PD network infrastructure to applications and network areas approved by the appropriate owner and Chief of Police or designee.

4.2 Oversite of Remote Access

A. PDIT uses available tools to monitor use of remote access and compliance with NCIC, ACIC, MPD and COM guidelines, policies, regulations, orders and laws.

B. All violations of NCIC, ACIC, MPD, and COM guidelines, policies, regulations, orders and laws are documents on a compliant form and forwarded to the affected Division Commander/Manager.

1. Depending upon the seriousness of the charge, the PDIT Security may immediately remove the member's access pending investigation and review of the complaint.

C. PCs used for Telecommuting are subject to unscheduled audits as directed by the Chief of Police or designee.

4.3 Telecommuting Access Support

A. Computer support for remote access to COM computers is limited to normal business hours, Monday through Friday.

1. COM owned equipment will be returned to the member's work area for maintenance.

REFERENCES

- City of Mesa Management Policy 327 Teleworking