REVIEW/REVISION HISTORY:

Effective: 4/7/04
Revised: 5/10/04
Revised: 8/2/05
Revised: 9/27/07
Revised: 3/5/09
Revised: 9/4/09
Revised: 8/29/11
Revised: 1/14/13
Revised: 6/21/16

SUMMARY OF REVISION/REVIEW:

Major changes to include wireless portable technology allowed/not allowed within the secure perimeter of any Prison. Read carefully!

APPROVED:

Signature on file

RICHARD “DICK” MORGAN, Secretary
Department of Corrections

5/17/16
Date Signed
REFERENCES:

DOC 100.100 is hereby incorporated into this policy; DOC 280.100 Acceptable Use of Technology; DOC 280.250 Acquisition, Disposal, and Licensing of Information Technology; DOC 280.310 Information Technology Security

POLICY:

I. The Department has established guidelines for possession and use of wireless portable technology (e.g., cellular telephones, smartphones, cameras, video equipment, tablets, laptop computers, walkie-talkies) on Prison grounds to maintain order and security, and prevent the introduction of contraband into facilities.

II. The Department will not be liable for loss of or damage to any personal items.

DIRECTIVE:

I. General Requirements

A. Wireless portable technology will be acquired per DOC 280.250 Acquisition, Disposal, and Licensing of Information Technology.

B. Per DOC 280.310 Information Technology Security, personal wireless portable technology will not be connected to the Department network in any manner.

C. Use of wireless portable technology and software not issued by the Department for contract staff must be formally authorized in the contract and follow DOC 280.100 Acceptable Use of Technology and DOC 280.310 Information Technology Security.

II. Facility Issue

A. The Superintendent will designate an employee to maintain tracking of facility issued wireless technology per DOC 280.100 Acceptable Use of Technology.

B. Information pertaining to wireless portable technology will be kept on file with the point of issue to allow for disabling, if necessary.

C. Employees/contract staff will be responsible for returning facility issued equipment to the Superintendent/designee when the equipment is not functioning properly or is no longer needed.

III. Authorization Within Prisons
A. Personal cellular/smart phones and smart watches that have the potential to receive phone calls or act as a Wi-Fi hot spot/access point are not allowed within the secure perimeter of any Prison.

B. Activity trackers (e.g., Fitbit, pedometer) will be allowed on Prison grounds as long as they do not have the capability of acting as a hot spot/access point.

C. Employees/contract staff must have DOC 21-573 Wireless Portable Technology Security Exemption Request signed by the Superintendent/Assistant Secretary for Prisons/designee to take cameras, tablets, or laptop computers not issued by the Department within the secure perimeter of any Prison.

1. Upon approval, employees/contract staff must carry a signed copy of the form with the authorized device while within the secure perimeter.

2. If any wireless portable technology is lost, the Shift Commander will be notified immediately and the service provider will be notified to disable the device, if applicable.

D. Employees/contract staff that have been issued wireless portable technology by the Department may retain and use it within the secure perimeter of a Prison.

1. Wireless portable technology must be logged in at the external facility checkpoint and logged out upon departure.

2. Wireless portable technology must have Wi-Fi and tethering capabilities disabled.

3. Employees/contract staff will ensure they depart the facility with all items/equipment.

DEFINITIONS:

Words/terms appearing in this policy may be defined in the glossary section of the Policy Manual.

ATTACHMENTS:

None

DOC FORMS:

DOC 21-573 Wireless Portable Technology Security Exemption Request