Arizona Department of Child Safety

TITLE Wireless Security Policy	POLICY NUMBER DCS-05-25	
RESPONSIBLE AREA DCS Information Technology	EFFECTIVE DATE December 18, 2019	REVISION V 1.0

I. POLICY STATEMENT

This policy establishes standards that must be met when wireless communications equipment is connected to the DCS network. The policy prohibits access to networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by Information Security are approved for connectivity to the Department of Child Safety (DCS) equipment network.

II. APPLICABILITY

This policy applies to all DCS wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of the DCS internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to the DCS network do not fall under the purview of this policy.

III. AUTHORITY

NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, April 2013.

HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006.

IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, Revision 11-2016.

IV. DEFINITIONS

Department or DCS: The Arizona Department of Child Safety.

Director: The Director of the Arizona Department of Child Safety.

ISO: Information Security Officer

PII: Personally Identifiable Information

V. POLICY

A. Approved equipment:

1. All wireless LAN access must use State approved vendor products and security configurations.

B. Monitoring of uncontrolled wireless devices:

1. All DCS locations where permanent data networks are installed will be equipped with sensors and systems to automatically detect and classify communication with unapproved wireless access points.
2. In DCS locations where wireless LAN access has been deployed, wireless intrusion detection systems will also be deployed to monitor for attacks against the wireless network. The wireless intrusion detection system shall be integrated with the wireless LAN access system whenever possible.

C. Authentication of wireless clients:

1. All access to wireless networks must be authenticated.
2. The strongest form of wireless authentication permitted by the client device must be used. For the majority of devices and operating systems, WPA or WPA2 with 802.1x/EAP-PEAP must be used. WPA2 is preferred wherever possible.
3. Where 802.1x authentication is used, mutual authentication must be performed. Client devices must validate that digital certificates presented by the authentication server are trusted and valid. Under no circumstances may clients disable validation of server certificates and blindly trust any certificate presented. EAP methods that do not support certificate-based mutual authentication may not be used.
4. EAP methods that exchange authentication credentials outside of encrypted tunnels may not be used. These methods include EAP-MD5 and LEAP.
5. Any DCS user with an account in the DCS Active Directory shall be able to authenticate at any DCS location where wireless access is present. The username and password for the Guest network is available to anyone per DCS management's discretion.

D. Encryption:

1. All wireless communication between DCS devices and the DCS network must be encrypted. Wireless networks providing only Internet access for guest users are exempted from this requirement.
2. The strongest form of wireless encryption permitted by the client device must be used. For the majority of devices and operating systems, WPA using TKIP encryption or WPA2 using AES-CCM encryption must be used. WPA2 with AES-CCM is preferred wherever possible.

3. Client devices that do not support WPA or WPA2 should be secured using VPN technology such as IPSEC where allowed by the client device

E. Access control policies:

1. Access to internal DCS network resources through wireless networks should be restricted based on the business role of the user.
2. Access control enforcement shall be based on the user's authenticated identity, rather than a generic IP address block. This is also known as "identity-based security."
3. The access control system must be implemented in such a way that a malicious inside user is unable to bypass or circumvent access control rules.
4. Access control rules must use stateful packet inspection as the underlying technology.
5. Access control policies must be setup to deny all and permit by exception for all connections.

F. Client security standards:

1. Where supported by the client operating system, the wireless network will perform checks for minimum client security standards (client integrity checking) before granting access to the DCS network. Specifically:

    a. All wireless clients must run DCS approved anti-virus software that has been updated and maintained in accordance with the DCS anti-virus software policy.
    b. All wireless clients must run host-based firewall software in accordance with the Company's host security policy.
    c. All wireless clients must have security-related operating system patches applied that have been deemed "critical" in accordance with the DCS host security policy.
    d. All wireless clients must be installed with DCS standard wireless driver software.

2. Clients not conforming to minimum security standards will be placed into a quarantine condition and automatically remediated.

3. Client operating systems that do not support client integrity checking will be given restricted access to the network according to business requirements.

G. Wireless guest access:

1. Wireless guest access will be available at all facilities where wireless access has been deployed.

2. A single username/password combination will be assigned for all guest access. The password for guest access will be changed quarterly and distributed to local facility managers.

3. Wireless guest access is available 24/7.

4. Guest access will be restricted to Internet access only and not have connectivity to the internal DCS network.

VI. PROCEDURES

None at this time.

VII. FORMS INDEX

None at this time.