TITLE	POLICY NUMBER	
VPN Acceptable Use Policy	DCS-05-26	
RESPONSIBLE AREA	EFFECTIVE DATE	REVISION
DCS Information Technology	January 6, 2020	V 1.0

I. POLICY STATEMENT

This policy establishes standards and guidelines for remote Virtual Private Network (VPN) connections to the DCS network.

II. APPLICABILITY

This policy applies to all DCS employees and 3rd party vendors utilizing a VPN to access the DCS network. This policy applies to implementations of VPN that allow direct access to the DCS State network.

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

VPN: A secured private network connection built on top of a public network, such as the internet.

V. POLICY

A. DCS employees may utilize the benefits of a VPN if approved by their manager.

B. The VPN is an IP only resource. Other protocols are not supported.

C. It is the responsibility of the employee with VPN privilege to ensure that unauthorized users are not allowed access to the DCS State network.

D. VPN access is controlled using ID and two factor password authentication.

E. All traffic traversing the DCS VPN is logged and associated with the user.

1. All DCS employees will be forced to use a full VPN tunnel as part of the configuration, no split-tunneling is allowed unless an exception is granted by management.
2. VPN users will be automatically disconnected from the DCS network after a predetermined amount of inactivity. The user can immediately log on again to reconnect to the DCS network.
3. Users of this service are responsible for the procurement and cost associated with acquiring basic internet.
4. Only DCS provided computers are authorized to connect to the remote access VPN, no personal computer connections are allowed unless specifically approved by management.
5. The DCS remote access VPN firewall is configured to disconnect all active sessions that reach 8 hours in duration.

F. Enforcement:

1. This policy regulates the use of all VPN services to the DCS network and users must comply. To maintain security, VPN services will be terminated immediately if any suspicious activity is found. Service may also be disabled until the issue has been identified and resolved. Any DCS employee found to have intentionally violated the VPN Acceptable Use Policy will be subject to loss of VPN privileges.

2. By choosing to use the DCS VPN, you hereby agree to all terms and conditions listed above.

VI. PROCEDURES

None at this time.

VII. FORMS INDEX

None at this time.