Citrix Confidential System Administrative and Client Application Access

Standard ID
IOT-CS-TEC-001

Published Date
11/1/2016

Effective Date
1/2/2017

Last Updated
10/31/2016

Next Review Date
10/31/2017

Policy
06.0 Access Control (PR.AC)
    06.5 PR.AC-5
        06.5.1 Network Segmentation

Purpose
Support secure agency administrative access to Protected Zone confidential servers.

Scope
IOT Supported Entities

Statement
In an effort to increase security with agency administrative access and client server applications, IOT supports the Citrix XenApp double-hop solution as the approved access gateway for agencies to utilize when accessing confidential systems located within the Protected Zone (PZ). All other administrative access to confidential servers is prohibited.

Below are the requirements for using the Citrix solution to access the PZ:

- All agency applications will need to be reviewed and approved by IOT prior to any implementations being made with the Protected Zone. IOT will work with the agency to design a solution which can include a designated IOT Project Manager on larger projects, provide a well-defined scope for the project and identify an agreed time-line by both the agency and IOT Operational Staff.

- Production Systems - Two or more Citrix Virtual Delivery Agent (VDA) Servers will be hosted in the agency’s Presentation Zone to provide published tools and applications that allow access to the agency’s Production systems.

- Non-Production Systems - One or more Citrix VDA Servers will be hosted in the agency’s Presentation Zone to provide published tools and applications that allow access to the agency’s Non-Production systems.

- IOT and agency administrators will require elevated credentials when using Citrix in the Protected Zone. Agency users are expected to use non-elevated accounts when they are accessing applications and performing non-administrative functions within the Protected Zone.

- Prior to gaining access, all users and or administrators will be required to use Multifactor Authentication also known as (MFA) or Microsoft Phone Factor to satisfy the two-factor authentication requirement set forth by the IOT Security Team.

- Agency applications that have satisfactorily met the software requirements guidelines and that have been successfully
implemented within the Protected Zone (PZ), will be added to a whitelist to reflect compliance of the Authorized Software Security Standards.

- Authorization to applications will be granted through Active Directory security groups which will be managed and approved by agency designated Security Coordinators.

- In the event an agency's software is not supported or deemed NOT suitable for hosting by the IOT Citrix Team, the IOT Citrix Team will work with the agency to provide an alternative method to access the agency’s systems located in the Protected Zone.

- IOT requires application testing prior to any migrations taking place. A comprehensive user pilot test-group must be created and tasked with thorough testing. The agency is required to sign-off that adequate testing has been achieved before moving forward with the migration. IOT Citrix Servers can only communicate with agency systems that are located within the protected zone.

- There will be absolutely no data traversing the Citrix environment. Any data that enters the Protected Zone or leaves the Protected Zone must follow proper IOT standard for transferring data in and out of the Protected Zone.
  - All client printers will be disabled.
  - Clipboard redirection will be disabled.
  - All file transfers shall be routed through IOT’s Manage File Transfer solution.
  - Session disconnected after two minutes.
  - Session inactivity will be reset after two hours.

- Logging into Citrix will use the "user Principal Name" (UPN) from your elevated or user account depending on your role (login name@domain name)

Roles
Information Asset Owners/System Owners

Responsibilities
Information Asset Owners/System Owners shall understand and use Citrix XenApp for access to confidential system in the Protected Zone (PZ).

Management Commitment
Management shall ensure that Citrix is the only solution used to access confidential systems in the Protected Zone.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT to receive authorized access to Citrix solutions.

Compliance
IOT and Agencies shall review who has access to confidential systems in the Protected Zone and how they are administering the solution.

Exceptions
Exceptions will be handled on a case by case basis through the Director of Risk & Compliance, State CISO and the IOT Operations Team.