State of Indiana Policy and Standards

Confidential System Architecture

Standard ID
IOT-CS-ARC-001

Published Date
9/1/2016

Effective Date
9/1/2016

Last Updated
8/25/2016

Next Review Date
8/25/2017

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

Purpose
Isolating critical systems will reduce opportunities for unauthorized access and contain possible incidents or breaches.

Scope
All Executive Branch State Agencies

Statement
For all confidential systems, the architecture must meet the following requirements:

System Hardening
All systems must utilize IOT's secure baseline configuration

- All server operating system(s)
- Database Server/Instances
- System components and features (e.g., .NET, IIS)
- All application and security logs shall be sent and monitored in IOT's Security Information and Event Management (SIEM) system
- All components must utilize IOT's management infrastructure (e.g, AD services, NTP, DNS, Netbackup, software update services)
- Security controls shall be enabled to the level commensurate with the system classification (e.g., confidential)

Access, Isolation and Communication

- No direct user access to servers in any tier in the protected zone
- No direct administrative access to the protected zone (must use IOT's 'Secure Access' Solution)
- No file sharing access between zones (must use IOT's 'Secure File Transfer') solution
- Communication between zones and tiers must be encrypted following IOT's Data Encryption Standard
- Information System tiers must not span Zones
- Interconnection between information systems that are in different zones must go through IOT application or web gateway
- All network traffic shall be denied by default. Only allow the hosts, ports, and services that are explicitly required and all entry points shall be limited based on least functionality (Must adhere to SecureTransport Protocols and Rules standard)

- Agencies shall not use VPN, wireless or tunneling access to any protected zone environment. Must utilize protected zone stateful inspection/application firewall hardware and software
- Information System(s) must consist of a production and non-production domain (environment)
- Production and non-production domain cannot be bridged unless there is an IOT approved change control process in place
- Web servers shall be placed in a presentation tier (DMZ) Virtual Local Area Network (VLAN) allocated by IOT
- External network connection shall connect only through IOT's application gateway or approved proxy services and public access into the State's network shall be denied except for approved communication through IOT's application/proxy and PZ firewall
- Agencies shall not use VLANs between confidential tiers and any other network of a lower security level without traversing through a DMZ and proxy
- Confidential, private and/or sensitive data shall follow State standards per domain

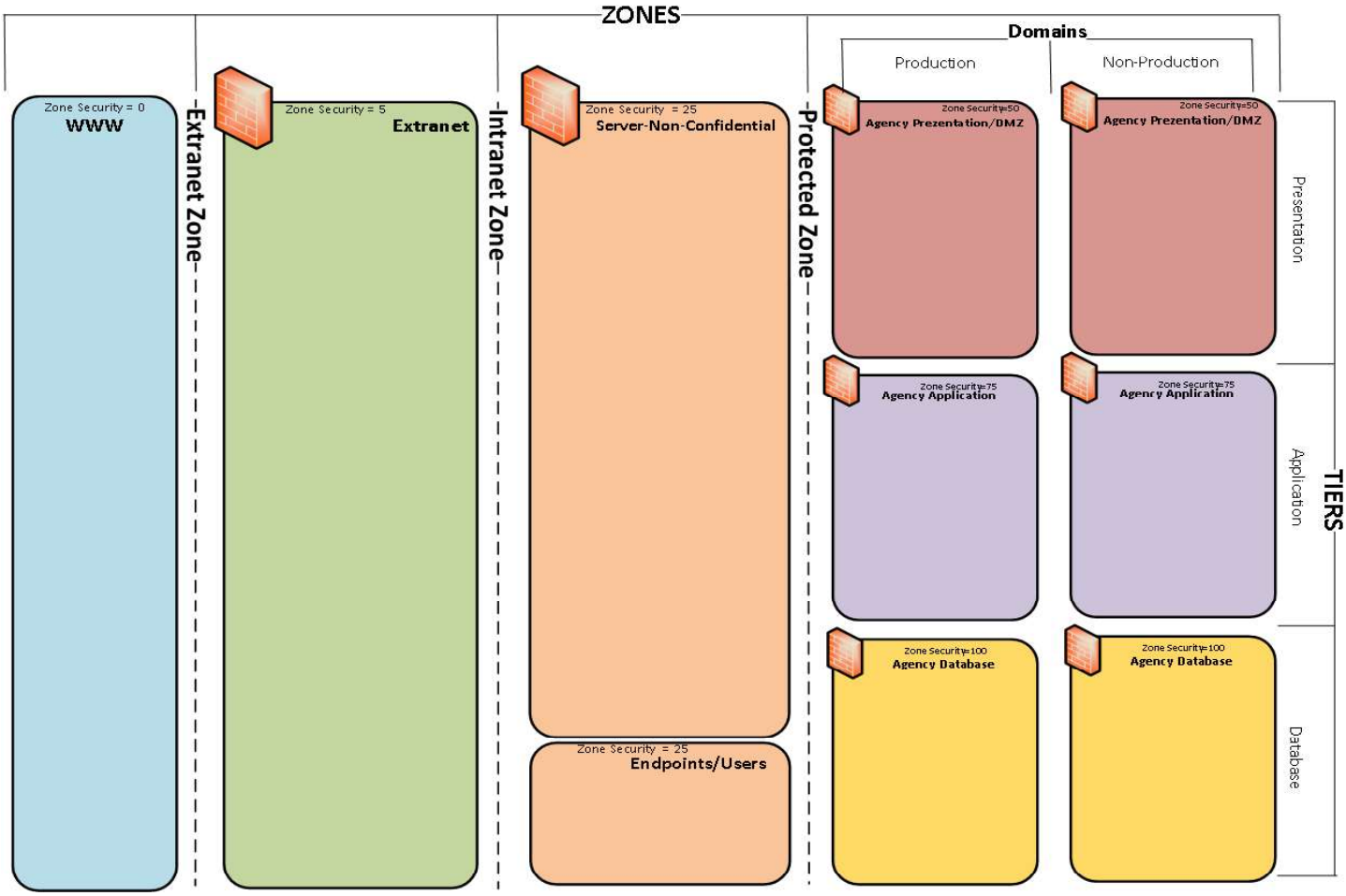
Administration

- Data sharing between agencies must have a Memorandum of Understanding (MOU) in place to disclose the security implications between agencies.
- All vendor system support must use a support gateway disabled until the specific time they are needed. (e.g, Oracle Exadata, SAP HANA, EMC)
- All file content moving in and out of the PZ must use IOT's Secure File Transfer Solution
- All administrative access must use IOT's Secure Access solution
- All information system security tools, mechanisms, and support components associated with the system shall be maintained on a bastion host (jump box) separated on a PZ isolated VLAN that only has access to perform specific administrative functions, based on least functionality principles
- All administrative functions must use elevated credentials

New and Upgraded Systems

For all new systems brought into the State environment, the architecture must meet all of the above requirements, in addition to the requirements listed below:

- Information System(s) shall be partitioned into a three-tier architecture that consists of a presentation, application and a database tier where one VLAN is used for each tier per domain
- Application Development should adhere to three tier architecture, secure application development (DISA APPLICATION SECURITY AND DEVELOPMENT) and follow SDLC process.



Roles
Information Asset Owners/System Owners

Responsibilities
Information Asset Owners/System Owners must work with Agency Management to determine what systems are required to be in the Protected Zone and appropriately configure them to maximize security while conserving required functionality. IOT shall work with agencies to architect the systems that meet the State's security requirements.

Management Commitment
Management shall ensure that all confidential systems are segmented appropriately.

Coordination Among Organizational Entities
Agencies shall coordinate with the IOT Architecture team for placing the system in the PZ.

Compliance
Agencies shall review the Information Systems Inventory (ISI), the authoritative source of system information to understand all confidential systems related to their agency. All confidential systems must be appropriately isolated.

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