State of Indiana Policy and Standards

Exceptions to Information Security Policy and Standards

Standard ID
IOT-CS-SEC-004

Published Date
9/1/2016

Effective Date
9/1/2016

Last Updated
9/1/2016

Next Review Date
9/1/2017

Policy
00.0 Introduction

00.5 Policy Exceptions

Purpose
Agencies may require a temporary exception to information security policy and standards. This standard provides the formal requirements for exception(s).

Scope
IOT Supported Entities

Statement
Technical or business requirements may indicate the need for exemption from the State’s Information Security Policy and Standards, for specific matters. Following an appropriate risk assessment, the Chief Information Security Officer or their appointed designee, can acknowledge and/or escalate exception requests. The CISO may ask that the agency reconsider aspects of the exception, but does not formally approve or deny requests. IOT Security will store the exception in the State’s Governance, Risk and Compliance tool.

Requests for exceptions must use the appropriate form and be signed by a State employee that is an IT/MIS Director or above, prior to submission. Further, the request must document:

- The Control Standard(s) for which the exception is needed
- The business justification and impact
- The additional risks identified as a result of needing the exception
- The compensating controls that are planned or implemented to reduce the additional risk to a tolerable level

All exceptions to State Policy and Control Standards must be documented with IOT Security. Exceptions must be re-evaluated on a periodic basis and extension requests are required after one year.

Roles
All Personnel

Responsibilities
Personnel shall notify agency management and executive management where agencies are not able to meet State policy and standards. Agency Management and/or Executive Management shall provide approval and own the risk(s) associated with the inability to meet State policy and standards.

Management Commitment

Management shall ensure that all exceptions are adequately documented and signed-off by the appropriate parties.

Coordination Among Organizational Entities

Agencies must submit the exception to IOT Security and work to develop and implement the appropriate compensating controls.

Compliance

All exceptions must follow the requirements of this standard. In cases where failures to notify are found, the issue will be escalated to the State CIO. Agencies that do not review and extend their exception requests in the allowed timeframe will be considered out of compliance.

Exceptions

No exceptions.