Workforce Risky Behavior

Standard ID
IOT-CS-SEC-105

Published Date
4/12/2012

Effective Date
4/12/2012

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
13.0 Security Continuous Monitoring (DE.CM)
13.1 DE.CM-1
13.1.1 Network Monitoring
13.3 DE.CM-3
13.3.1 Personnel Activity Monitoring

Purpose
This practice describes the notification process to agencies on risky employee/contractor behaviors identified by IOT through its technical support role and other monitoring activities.

Scope
IOT Supported Entities

Statement
A party recognizing a risky behavior of an individual must report the activity to IOT Security. Examples of risky behavior:

- Repeated history of virus infections or attempted virus infections
- Incidents of failing to recognize spam and/or phishing messages and inappropriately responding
- Findings by IOT technicians while providing support (e.g. inappropriate software, media downloads)
- Discovered incidents of sharing account information (e.g. passwords)
- Agency reported behaviors (e.g. inappropriate web surfing, unacceptable use of email, etc.)
- Failure to maintain current security patches and virus definitions
- Bypassing security measures that have been put in place to reduce risk (e.g. canceling managed scans, bypassing the internet filter, removing security software)
- Misuse of state equipment

IOT will notify the individual’s manager and copy authorized agency contacts of the risky behavior. Information regarding the nature of the issue will be provided.

At the request of the agency, from HR, the manager or other authorized source, IOT will quarantine the user’s Internet access. While quarantined users will only be able to access the State’s Intranet and IN.gov web sites. Requests to quarantine a user should be sent to iotinternetfilter@iot.IN.gov.

Upon direction from the individual’s manager or other authorized agency source IOT will restore standard Internet access for the user.
Standard access should be restored through an email to iotinternetfilter@iot.IN.gov.

**Roles**
All Personnel

**Responsibilities**
All personnel shall use equipment in accordance to State Policy and Standards, while changing work habits to address identified risky behavior. IOT shall notify agency of risky behaviors, assist as requested by the agency to address the behavior.

**Management Commitment**
Management shall ensure the appropriate training and awareness measures are taken to inform personnel of State Policy and Standards relating to the use of information and assets.

**Coordination Among Organizational Entities**
IOT shall work with agencies in addressing risky behavior(s).

**Compliance**
Lack of corrective measures may result in escalations to agency heads and the CIO.

**Exceptions**
No exceptions.