**AGENCY NAME**

**Title: Security Alerts and Advisories**

**Number: XXX Effective: 6/01/16**

**Amends: XXX**

**Distribution: All**

**Standards**:

Security alerts and advisories are released to IT departments to ensure knowledge of newly discovered threats that may affect Agency Information Systems. The purpose of this policy is to define standards and procedures for security alerts and advisories.

|  |
| --- |
| **Scope** |

This procedure shall apply to all Agency personnel.

|  |
| --- |
| **Discussion** |

The overriding goal of this policy is to comply with the CJIS Security Policy requirements. Due to the evolving nature of the CJIS Security Policy, it is necessary to separately communicate the requirements of the CJIS Security Policy as they are developed and enhanced. These additional requirements are intended to be an enhancement to the existing Standard Operating Procedures of AGENCY NAME. The Agency shall adhere, at a minimum, to the CJIS Security Policy. While the Agency may augment or increase the standards, it cannot detract from the minimum requirements set forth by the FBI CJIS Security Policy.

|  |
| --- |
| **Procedures** |

The IT Department will monitor and/or receive alerts and advisories from the locations listed below. If an alert is determined to be critical or pertinent to Agency infrastructure, the appropriate personnel will be notified. All alerts and related actions will be recorded into an information log for Agency records.

The IT department has signed up for alerts and advisories from the following sites:

[www.us-cert.gov/ncas/current-activity](http://www.us-cert.gov/ncas/current-activity)

<https://tools.cisco.com/security/center/publication>

<https://technet.microsoft.com/en-us/security>

1. The Agency will receive information system security alerts and advisories
2. Once an alert has been received or detected and has been determined to be a credible threat, IT will notify the Agency LASO.
3. IT will take appropriate action depending on the alert. This could include updating security settings and/or issuing information to all relevant Agency personnel with directions to ensure proper handling of the issue.
4. IT will document the details of the alert. The log will remain with IT for a period of four years.

POLICY VIOLATION: Any user who violates any portion of this policy will be subject to the standard disciplinary processes in place with the Agency. Sanctions against staff that violate information systems and or security policies may include formal disciplinary action up to and including termination based on offense severity.