DATA INCIDENT RESPONSE

INDEX CODE: 505
EFFECTIVE DATE: 12-01-03

Contents:

I. INCIDENT TRIAGE

In the event of an incident, the user must first identify what type of incident occurred in order to identify the best way to proceed. If there are any questions during the process, or if the user is unsure of the type of incident, contact the Risk Hotline at (410)260-6083 or hotline@comp.state.md.us. Definitions and additional explanations regarding data classification can be found in POLICY 1.2 Data Classification & Stewardship in the Policy Section on COIN.

Triage Steps:

1. If this incident is a computer incident, contact the Annapolis Data Center (ADC) Help Desk immediately. Refer to Section II.
2. If this incident involves, or potentially involves, confidential information, contact the Compliance Manager or the Risk Hotline immediately. Refer to Section III. If this incident is also a computer incident, the first step is always to contact the ADC Helpdesk and the second step is to contact the Compliance Manager. In this scenario, section II and III will run concurrently.
3. If this incident was not a computer incident, and only involved public information, contact supervisor. Refer to Section V.

II. COMPUTER INCIDENT

If an electronic security incident may have occurred or may be imminent, the user must immediately contact his/her supervisor/manager and the ADC Help Desk at (410)260-7400.

All available incident information must be given to the ADC Helpdesk. This information will be used to complete a Security Incident Reporting Form to be submitted to IT Administrative Services. The following information should be reported:

- Name (unless reporting anonymously)
- What happened (the nature or type of incident)
- When it happened
- Where it happened
- Impact of the incident

Supervisor can assist in the reporting of the incident information to the ADC Help Desk. See ADC Help Desk Procedures for more information regarding computer security incidents. If the computer incident involved confidential information, continue to Section III.

III. INCIDENT – CONFIDENTIAL INFORMATION

Upon discovering a possible improper inspection or disclosure of confidential information, the custodian should immediately contact his/her supervisor, manager, or division director (COM Management) and the Risk Hotline at (410) 260-6083 or hotline@comp.state.md.us.

COM Management should assist the custodian in documenting and reporting the required information on the Data Incident Response Form (see Appendix 1). Division personnel are responsible for ensuring that the information provided is reported accurately and timely to the Compliance Manager.

Note: Timely notification is the most important factor, not the completeness of the incident information. Additional information will be secured via conversations between the impacted division and the Compliance Manager.

The focus of the Compliance Manager's review of the data incident will be to identify processes, procedures, or systems within COM with inadequate security controls. Based upon the analysis of the incident, COM Management may be recommended to modify security policy, procedure, or controls to more appropriately protect its data. The Compliance Manager will coordinate with division personnel to ensure appropriate follow-up actions taken by COM have been completed to ensure continued protection of COM data.

Once the situation has been appropriately reported on the Data Incident Response Form, the Compliance Manager will complete the Incident Review section by meeting with the custodian and COM Management.

IV. INCIDENT - FTI

Upon discovering a possible improper inspection or disclosure of FTI, the custodian should immediately contact COM Management (their supervisor, manager, or division director) and the Compliance Manager in the Office of Risk Analysis via the Risk Hotline at (410) 260-6083 or hotline@comp.state.md.us. COM Management must also notify the Deputy Comptroller.

COM Management should assist the custodian in documenting and reporting the required information on the Data Incident Response Form. COM Management is responsible for ensuring that the required information is reported accurately and timely to the Deputy Comptroller and Treasury Inspector General for Tax Administration (TIGTA). The Compliance Manager may also assist in this reporting process. COM Management should refer to IRS Publication 1075, Section 10.2 for guidance. COM Management will contact TIGTA and the IRS Office of Safeguards immediately, but no later than 24 hours after the identification of a possible issue involving FTI. The Risk Hotline and the Deputy Comptroller should be kept apprised of all information reported to TIGTA and the IRS Office of Safeguards. COM Management should not wait to determine if FTI was involved. If FTI may have been involved, the agency must contact TIGTA and the IRS immediately.

Note: Timely notification is the most important factor, not the completeness of the Data Incident Response Form. Additional information will be secured via conversations with the IRS Office of Safeguards.

COM Management will cooperate with TIGTA and the IRS Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident. The focus of the IRS Office of Safeguards' investigation of the unauthorized access or data breach incident will be to identify processes, procedures, or systems within COM with inadequate security controls. Based upon the analysis of the incident, COM may be required by the IRS Office of Safeguards to modify security policy,

procedure, or controls to more appropriately protect FTI in the possession of COM. The IRS Office of Safeguards will coordinate with COM to ensure appropriate follow-up actions taken by COM have been completed to ensure continued protection of FTI in the possession of COM.

Once the situation has been appropriately reported the Compliance Manager will meet with custodian and COM Management to complete the Incident Review section of the Data Incident Response Form.

V. INCIDENT – PUBLIC INFORMATION

If there is an incident involving public information, the supervisor should report the incident to the division director. These incidents should be investigated and resolved within the appropriate division.

For public information incidents, a COM Incident Review may be performed by the Compliance Manager at the discretion of COM Management.

VI. NOTIFICATION OF AFFECTED INDIVIDUALS

Based on the details of the incident, it may be necessary to notify affected individuals. COM Management will decide what type of notification will be required based on the details of the incident.

If the incident involved FTI, COM must inform the IRS Office of Safeguards of notification activities undertaken, preferably before released to the impacted individuals. In addition, COM must inform the IRS Office of Safeguards of any pending media releases, including sharing the text, prior to distribution.

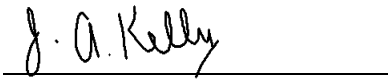
VII. COM DATA INCIDENT REVIEW

The COM Data Incident Review will be coordinated by the Compliance Manager in the Office of Risk Analysis, but the actual review will involve many different individuals. Depending on the nature of the incident, multiple divisions may need to be involved. The Compliance Manager will work closely with the Chief Information Security Officer (CISO) to ensure that any breakdown of security controls or system protections are rectified as soon as possible.

At a maximum of 30 days after the resolution of an incident involving confidential information, an incident review must be conducted. This will be performed in order to ensure that COM Policies and Procedures are appropriate to protect COM information and assets. The incident review will include an analysis of all aspects of the incident, including security policies and procedures, controls in place, and incident response policies and procedures. Based on the analysis performed, COM may decide to modify policies, procedures, and/or controls to more thoroughly protect COM data. Any identified deficiencies in the incident response policies and procedures should be resolved immediately. Additional training on any changes to the incident response policies and procedures should be provided to all employees, including contractors, as soon as possible.

The report will be sent to COM Executive Management and Division Management of the impacted divisions, as well as the CISO. See ADC Helpdesk procedures for the computer incident review process. For public information incidents, an incident review may be performed at the discretion of management.

VIII. CANCELLATION: None.



Jeffrey A. Kelly, Director