

Treasury Documentation**Subject:** Incident Reporting**For:** EMPLOYEE HANDBOOK**Also See:** BT-03049; PT-03095

Identification	ET-03180 Policy
Effective Date	7-1-2009
Replaces	ET-03180 (11-1-2007)

Page 1 of 4

Each employee is responsible for promptly reporting an incident affecting the Department of Treasury (Treasury), its resources, property, and information for which it has responsibility.

Michigan Civil Service Commission Rule 2-10 provides for protection from reprisal and/or disciplinary action against State classified employees reporting an incident involving public funds or property. The Whistleblower's Protection Act, Public Act 469 of 1980, as amended, provides the same protection for unclassified employees.

An incident, for purposes of this Policy, is an adverse event whereby some aspect of physical or financial security is threatened; confidentiality or privacy of data is violated; data is manipulated, lost, or stolen; financial resources or items of value are lost, stolen, or misused; or used for unauthorized or unlawful activity.

An incident is further classified as a security breach, in accordance with the definition in the Identity Theft Protection Act, Public Act 452 of 2004, as amended, when an unauthorized person gains access to or acquires unencrypted or unredacted personal information or the encryption key to personal information.

The Identity Theft Protection Act defines personal information as the first name or first initial and last name linked to a:

- Social Security number
- Driver's license number or State personal identification card number
- Demand deposit or other financial account number, or credit or debit card number in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.
- Personal information may be written or printed, or may reside electronically on any device.

The Department of Information Technology (DIT) Policy 1340.00, Information Technology Information Security, requires each agency to report and respond to security breaches and incidents "where there is reasonable belief that an unauthorized person may have acquired personal identifying information."

Goals of incident reporting include:

- Facilitating appropriate reporting of incidents
- Confirming or dispelling whether an incident has occurred
- Coordinating response(s) to certain incidents

- Notifying affected parties and consumer reporting agencies of incidents for certain security breaches
- Protecting confidentiality and privacy
- Minimizing disruptions to normal business operations
- Providing accurate reporting and useful recommendations
- Mitigating risks through corrective actions
- Deterring future incidents.

Incidents include but are not limited to threats; missing, lost, stolen, or misplaced negotiable instruments; missing or unauthorized disclosure of confidential, personal, or sensitive information; unauthorized probing and browsing; theft; unlocked secure areas; altered or destroyed input, processing, storage, or output of information; changes to information system software without the knowledge of or approval by the Treasury Business Owner; knowingly causing or spreading a computer virus; or any attack on an information system. They affect the following areas:

- Safety
- Financial resources
- Public trust
- Stakeholder confidence
- Legal liability
- Personal liability.

When an employee discovers or becomes knowledgeable of an incident, he or she must immediately notify his or her supervisor. However, if it is suspected that the incident involves the immediate supervisor, the employee should contact the next level management staff member in the chain of command. Incidents involving potential security breaches of personal information must be reported through the chain of command to the Chief Deputy Treasurer within 24 hours of discovery (see DIT Operating Procedure, How to Handle A Breach of Personal Identifiable/Sensitive Information Incidents) and to the Security Division.

Immediately contact the DIT Helpdesk for suspected or actual computer-related incidents such as spam, viruses, worms, Trojan horses, and other malicious software/source code, then notify the Security Division. DIT staff are responsible for defining appropriate procedures for addressing computer information attacks or denial of service attacks; identifying physical and electronic evidence to be gathered; monitoring, repairing, and mitigating any damage from an information attack; and/or minimizing or eliminating the information technology vulnerability, where possible.

Report human resource incidents to the Office of Human Resources, Civil Service Commission, Department of Management and Budget (DMB), instead of the Security Division. (Refer to Bulletin BT-03049 in the Employee Handbook and PT-03095 in the Employee or Supervisor Handbooks for additional guidance.)

If an incident affects other entities, bureau management staff must promptly notify affected entities so they can take appropriate action. This would include notification of the discovery of a security breach of personal information that is not owned but is maintained by Treasury. When apprising others of the existence of an incident, make every attempt to provide clear and concise information to assist in dissemination of this information within their respective organizations.

If an incident occurs, either suspected or actual, that constitutes an immediate threat to critical resources, materials, or data, follow proper emergency procedures. Management must immediately notify the Bureau Director or Deputy Treasurer through the appropriate chain of command and immediately begin investigation of the reported incident.

Incident Reporting

The Security Division must communicate information and alerts related to an incident having potential widespread implications to all Treasury staff. The Disclosure Officer must immediately notify the Treasury Inspector General for Tax Administration (TIGTA) and the Internal Revenue Service (IRS) Office of Safeguards upon discovery of a possible **unauthorized** inspection or disclosure of federal tax information. Therefore, it is important that the employee prepare Parts 1 and 2 of form 4000 INCIDENT REPORT and submit it to the Security Division for purposes of immediate notification of an incident.

After incident resolution, the Division Administrator or Office Director must prepare and submit a final (completed) 4000 to the Security Division. The report should provide:

- What happened (a description of the incident)
- When the incident occurred or was discovered
- Who was involved
- Location of the incident
- Action taken
- Incident impact (e.g., likely consequences, affect on other agencies or organizations, etc.)
- Post-incident recommendations to lessen the likelihood of a similar incident.

Management should follow up with pertinent staff to educate them about incident prevention.

To improve incident response, management and the Security Division should document and incorporate lessons learned in departmental divisional and office guidelines.

Retain final 4000s in accordance with Records Management Services, Department of History, Arts, and Libraries, Records Retention and Disposal Schedule.

Incident Information Distribution

Always direct legislative, press, or broadcast media inquiries about an incident to the Public Information Officer (Press Secretary) for Treasury. The Press Secretary acts as a single point of contact and response for Treasury.

Subject: Incident Reporting

Identification	ET-03180 Policy
Effective Date	7-1-2009

Page 4 of 4

The Security Division must issue annual reports on incidents occurring within or affecting Treasury. Periodically, the Office of Internal Audit, DMB, must review incident reports to determine whether issues exist that merit further investigation and remediation.

Policy Violation

Violation of this Policy may result in disciplinary action which may include termination for employees and temporary employees; a termination of contractual relations in the case of contractors, vendors, or consultants; or dismissal of interns and volunteers. Individuals remain subject to civil prosecution under the Identify Theft Protection Act for a violation of these provisions, as well as other applicable State or federal law.

End