

## What is an Incident? What is a Security Breach?

### What is an Incident?

An incident is any event threatening some aspects of physical or financial security, when financial resources or items valued at \$100 or more are missing or misused, any event violating confidentiality or privacy of information, where data is manipulated or missing, or any event involving unauthorized or unlawful activity.

### Examples of Incidents:

- Missing computer equipment containing non-personal information
- Missing briefcase that contains non-personal information.

### Examples of Material Incidents:

- Missing laptop computer or other mobile device or paper records that do not contain Treasury personal information but do contain confidential or sensitive information
- Missing warrant stock.

### What makes an incident a Security Breach?

An incident becomes a security breach when an unauthorized person gains access to or acquires:

1. Unencrypted or unredacted (data not altered or truncated) personal information, or
2. The encryption key to an area storing personal information.

**Beware:** An incident can become a potential security breach during the investigation process.

### Examples of a Potential/Actual Security Breach:

- Missing laptop computer or other mobile device that contains Treasury personal information
- Missing paper records that contain personal information
- Accessing personal information when there is no business need for it
- Using another individual's User ID and Password to access personal information
- Stealing Treasury records that include personal information
- Hacking into records containing Treasury personal information
- Obtaining Treasury personal information from employees without proper authorization to access the information
- Unauthorized and unescorted persons entering secure areas that house personal information.

### What is Personal Information?

The Identify Theft Protection Act, Public Act 452 of 2004, as amended, defines personal information as information containing the first name or initial of the first name and the last name along with one of the following:

1. Social Security number
2. Driver's License number or State Personal Identification card number
3. Account number; Credit or Debit Card number in

combination with any required security code, access code or password that would permit access to a person's financial account.

Personal information may be in written or printed form or may reside electronically on devices such as mainframes, servers, personal computers (desktops and laptops), CDs, DVDs, tapes, flash drives, memory sticks, USB keys, microfiche, PDAs, Blackberrys, cell phones, or may exist on other state-of-the-art devices that have been or may be developed.

### What should I do if my laptop is missing or if an incident is suspected?

#### Employee must:

1. File a report with local police immediately if asset valued at \$100 or more is missing.
2. Notify immediate supervisor no later than beginning of the next business day.
3. Complete Parts 1 and 2 of Form 4000, *Incident Report* (available on Treasury's Intranet).
4. Forward the Incident Report (with attached police report if applicable) to immediate supervisor and a copy to the Department of Treasury, Security Division.

#### Management Staff must:

1. Report the incident immediately through the chain of command to the Treasury Division Administrator and the Security Division. If personal information is involved, follow the guidelines for Security Breach.

**Exception:** If another state agency/governmental entity, report incident to Treasury Disclosure Officer, Technical Services Division and the Security Division. If contractor or vendor, report incident to Contract Compliance Inspector and the Security Division.

2. The Division Administrator must notify the Bureau Director if it is a material incident or involves non-Treasury information.
3. The Bureau Director must notify the other entity immediately.
4. The Division Administrator must inform the Department of Information Technology (DIT) Agency Services (Treasury) Director right away if incident involves information technology resources.
5. Notify other Treasury divisions/offices that may be affected or should be involved with investigation.
6. Investigate and resolve the incident.
7. Finalize Form 4000\* and submit it to the Department of Treasury, Security Division.

\*Another entity may substitute its internal form for form 4000 if all pertinent information is included.

### What should I do if I witness, discover, or am informed of a potential security breach?

#### Employee must:

1. Report the security breach immediately (no later than beginning of the next business day) to immediate supervisor.

2. Complete Parts 1 and 2 of Form 4000.
3. Forward Form 4000(with attached police report if applicable) to immediate supervisor and a copy to the Department of Treasury, Security Division.

**Management Staff must:**

1. If the breach is ongoing, **CONTAIN IT.**
2. Report the potential breach immediately through the chain of command to the Bureau Director or Deputy Treasurer, whichever is applicable.
3. The Bureau Director or the Deputy Treasurer, whichever is applicable, must notify the Chief Deputy Treasurer immediately if a breach involving a database of personal information.
4. The Bureau Director must notify the other entity if the potential breach involves non-Treasury information.
5. The Division Administrator must inform the DIT Agency Services (Treasury) Director right away if incident involves information technology resources and personal information.
6. Convene appropriate personnel so the scope of the breach can be determined and a plan for appropriate action can be agreed upon.

**Note:** If a database of personal information is involved, the Chief Deputy Treasurer must approve the Plan of Action.

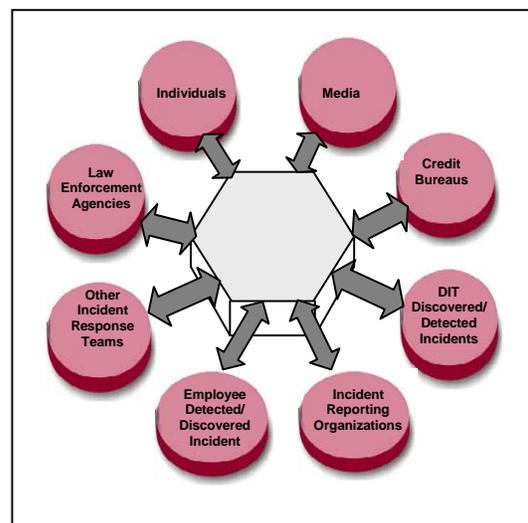
7. If appropriate, issue breach notifications by telephone, in writing, on the Web or by e-mail.
8. Notify the three major credit bureaus of the breach if more than 1,000 residents of the State of Michigan will receive or have received breach notifications.
9. Finalize Form 4000\* and submit it to the Department of Treasury, Security Division.

\*Another entity may substitute its internal form for form 4000 if all pertinent information is included.

**Treasury must protect personal information against risks such as unauthorized access, modification or loss with reasonable security safeguards. Some safeguards are:**

- Do not store confidential, personal or sensitive Treasury information on mobile devices or portable media (including laptops, notebooks, memory sticks, CDs, DVDs, floppies) unencrypted; otherwise ENCRYPT files or the full disk. (Refer to DIT Standard 1340, Storing and Managing Personal Identifying/Sensitive Information on Mobile Devices and Portable Media; also refer to Treasury Policy ET-03169 Data Security).
- Avoid sending or receiving unencrypted confidential, personal or sensitive information via e-mail.
- Avoid sending confidential, personal or sensitive information via fax.
- Secure confidential, personal or sensitive papers on the fax, printer or copy machines.
- Keep conversations at a volume level and/or in a location that will protect information.
- Back up data on a regular basis; make sure data files from an approved portable device are stored on the network server.
- Never store more data than needed.

- Shred documents with confidential, personal or sensitive information (see Treasury Policy ET-03115 Confidential Information, Handle and Discard).
- Have computers and hard drives properly wiped or overwritten when discarding (see DIT Procedure 1350.90, Secure Disposal of Installed and Removable Digital Media and Treasury Policy ET-03169).
- Use a log-in password that is not easily guessed. Make it at least eight characters long, composed of upper- and lower-case letters, numbers and symbols such as “#” (see Treasury Policy ET-03175 on Passwords).
- Never set any log-in dialog box to remember your password (see Treasury Policy ET-03175 on Passwords).
- Use a password-protected screen saver that comes on after a few minutes of inactivity. Initiate screen lock system (if a Treasury employee, press the key with Microsoft Windows logo and “L” on the keyboard) when you leave your office, even for a short period.
- Limit access to confidential, personal or sensitive information to those who need to use it to perform their job duties (see Treasury Policy ET-03164 Access Control).



**For additional information, see the following guidelines in the Security Guide:**

- ET-03180, Incident Reporting
- BT-03084, Security Breach Involving Personal Information
- PT-03253, Incident Reporting and Handling
- CT-03070, Incident/Security Breach Examples
- DIT Operating Procedure, How to Handle a Breach of Personal Identifiable / Sensitive Information Incidents

**Other References:**

- BT-03049, Employee Conduct, General Guidelines
- ET-03140 Workplace Safety
- PT-03246, Potential Dangerous Taxpayer/Debtor, Report
- PT-03095, Theft or Irregularities in Public Funds/Property or Violations of Departmental Policies and Procedures, Report and Investigate

**Contact Information:**

If questions, please contact Division/Bureau Security Liaison or the Security Division at (517) 636-4081.