pennsylvania
DEPARTMENT OF LABOR & INDUSTRY
OFFICE OF INFORMATION TECHNOLOGY

Lost or Stolen IT Equipment Checklist and Questionnaire

This checklist must be completed by the individual who lost or had their IT equipment stolen. Notification must be sent to the individual's supervisor and to the OIT Security and Compliance Division immediately upon discovery or at the start of the individual's next scheduled shift. Questions should be submitted to the OIT Security and Compliance Division. Failure to submit this checklist, as required by L&I Policy SEC 003 (Lost or Stolen Equipment), may result in disciplinary action up to and including termination of employment or contractor sanctions.

Full Name:
Title:
Commonwealth e-mail:
Commonwealth desk phone number:
Commonwealth cell phone number:
Bureau/Division:
Office location:
Supervisor's name:
Supervisor's title:
Supervisor's e-mail:
Supervisor's commonwealth desk phone number:
Date and time of submission:

Was the IT equipment lost or stolen?

☐Lost ☐Stolen

What IT equipment was lost or stolen? (Check all that apply)

☐Cell phone ☐Laptop
☐Desktop ☐MiFi
☐USB drive ☐Tablet/iPad
☐Paper documents ☐Other:

List make, model and serial number of each device.

Approximate date and time when the equipment was lost or stolen?

When was the equipment last used?

From what address was the equipment lost or stolen?

From where was the equipment lost or stolen (e.g. office space, car, home)?

Was Personally Identifiable Information (PII) stored on any of the IT equipment? (PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. PII includes, but is not limited to, an individual's name, Social Security number, address, phone number, and state-issued ID card number)

☐Yes ☐No

On which device was it stored (e.g. phone, laptop, desktop)?

How many individual records?

Was the information related to department/commonwealth employees or citizens?

How/where was the information stored (e.g. Word, Excel, Access, e-mail)?

Was medical information stored on any of the IT equipment? (Medical conditions, medication, medical history)

☐Yes ☐No

On which device was it stored (e.g. phone, laptop, desktop)?

How many individual records?

Was the information related to department/commonwealth employees or citizens?

How/where was the information stored (e.g. Word, Excel, Access, e-mail)?

Was credit card information stored on any of the IT equipment? (e.g. card number, name, pin, access code)

☐Yes ☐No

On which device was it stored (e.g. phone, laptop, desktop)?

How many individual records?

Was the information related to department/commonwealth employees or citizens?

How/where was the information stored (e.g. Word, Excel, Access, e-mail)?

Is any of the lost or stolen information covered by a state or federal regulation, such as IRS Pub1075, HIPPA, etc.?

Do you have a backup copy of the data that was lost or stolen? If so, where is the backup located?

If a USB drive was lost or stolen, was it a department-issued drive and was it encrypted?

If the equipment was stolen, validate that the police have been notified. (Attach a copy of the police report if available.)

Police report number:
Police department:
Officer:

Have you notified any of the individuals for whom you had information stored on the lost/stolen device? (If you have not notified them, please do not notify them. If a notification is made it will be coordinated with the department's Communication and Press Office.)

Who else has been notified of this incident? (Please include name and title)

Prior to the incident, did you notice any suspicious activity that may be related?