



  
**POLICY**  
*Ohio Department of Taxation*

**Policy Description:**  
Securing Laptops

---

**Policy No:** ODT – IT - 011

---

**Authorities:**

IRS Publication 1075 – Tax Information Security Guidelines for  
Federal, State and Local Agencies and Entities

ITP-B.9 – Portable Computing Policy

ODT-HR-004 – Progressive Discipline

**Division With Primary Responsibility:**

Information Services Division

**Pages:** 2 Pages

---

**Effective Date:** April 6, 2009

**Revised Date:**

---

## 1.0 Purpose

With the continued distribution of laptop computers, the exposures to the possibility of theft, damage or unauthorized use of state property grows. All employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties (hereinafter all collectively referred to as “ODT representatives”) have an obligation to safeguard and securely maintain the state’s property, and must exercise reasonable precautions to prevent theft, damage or the unauthorized use of ODT laptops. The purpose of this policy is to outline the precautions that must be taken to ensure the safety and security of ODT’s laptop computers.

## 2.0 Scope

This policy applies to all ODT representatives who have either been assigned, or share the use of ODT provided laptop computers.

## 3.0 Policy

It is the policy of ODT that all laptops shall be secured using the precautions outlined below.

### 3.1 Encryption

All ODT laptops are configured with full hard disk encryption and are required to be fully encrypted before they can be removed from an ODT facility.

Laptops must be powered off before being removed from an ODT facility. Locking the computer or placing it in a hibernate and/or standby status does not allow the encryption software to activate.

### 3.2 Passwords

Passwords must not be written down and kept with the laptop or the key fob (SecurID token). If you must write a password down, put it in a secure place like your purse or wallet.

### 3.3 Locking Computer Security Cables

A computer security cable is issued with each ODT laptop.

While in an ODT facility, all unattended laptops must be properly secured. They must be 1) locked in a cabinet, OR 2) secured to a fixed object such as a cabinet or desk using a computer security cable.

### **3.4 Traveling with a Laptop**

#### **3.4.1 Automobile Travel**

During automobile travel, the laptop must be placed in a secure in a location that is not visible from the car windows (e.g., trunk of car).

**Laptops must NOT be left unattended in a vehicle overnight.**

*Note: These items in section 3.4.1 do not apply to computers that are securely installed in ODT Enforcement vehicles.*

#### **3.4.2 Air Travel**

During air travel, the laptop can not be checked baggage or left with airline/airport personnel. It should be kept as close to the traveler as possible, and remain in sight of traveler whenever possible. If it becomes necessary to place the laptop in an overhead bin during travel, the traveler is responsible for regaining possession of the laptop as quickly as practical at the end of the flight.

#### **3.4.3 Off-site Laptop Use**

While working on a laptop off-site, take care to ensure the safety of the laptop and ODT data. 1) Be aware of people lurking about in an attempt to view the information on your screen; 2) lock your computer screen when not in use; 3) secure the laptop to a fixed object when left unattended; AND 4) power off the laptop before you pack it in order to transport it elsewhere.

### **3.5 Reporting Loss/Theft**

The ODT representative is responsible for reporting laptop loss or theft immediately upon discovery to their Division Administrator, who in turn must immediately report the loss to ISD Security.

### **4.0 Discipline**

Failure to comply with this policy may result in the imposition of discipline in accordance with ODT work rules including, but not limited to, Neglect of Duty, Insubordination, and/or Ohio Revised Code Section 124.34.