




<h1 style="margin: 0;">SENSITIVE INFORMATION POLICY</h1>	
- Effective	September 1, 2008
<input checked="" type="checkbox"/> Purpose	To set forth departmental policy to ensure uniformity and consistency in how sensitive information is used by employees and stored on Department IT resources.
 Authority	Statewide Information Technology Policy ITP B.1 ITP B.7
 Reference	ORC 1347.12
 Resource	Office of Information Technology

Policy

The proper storage, use and security of personal information are important to foster public confidence in the agency as well as protect DNR employees and our customers. Therefore, ODNR employees shall comply with the following provisions:

1. Use of sensitive personal or law enforcement information for other than approved official state business is prohibited.
2. Allowing unauthorized personnel access to sensitive personal or law enforcement information is prohibited.
3. Sensitive personal employee information or customer information shall not be stored on mobile storage devices without written approval from the director or his designee. OIT shall consult with divisions/offices on security techniques and practices. Divisions and offices are discouraged from storing customer name and addresses on mobile storage devices. This data should only be stored when it is business critical and shall be removed from the device as soon as possible after the information is no longer required for business purposes. This excludes phone listings and contact information stored in email applications or cell phones.
4. Sensitive personal or law enforcement information shall not be stored on employee owned personal computers.
5. Sensitive law enforcement information copied to mobile storage devices shall be removed/deleted from the device as soon as possible after the information is no longer required for business purposes.

6. Any lost or stolen departmental mobile storage device must be reported to the Office of Information Technology immediately upon discovery. The division or office that owns the missing device must investigate to determine whether sensitive personal information was stored on it and, if necessary, notify the affected individual(s) of the possible information release within 48 hours of the discovery.

Reference

Penalties

Employees that violate this policy are subject to discipline. Anyone who becomes aware of a violation of these provisions shall report it to his/her supervisor or the violator's supervisor immediately. The supervisor is responsible for notifying the Office of Information Technology chief or assistant chief.

Glossary

1. Mobile Storage Device: any device that can store data e.g., laptops, PDA's, flash drives, external hard drives, CD's and DVD's.
2. Sensitive Law Enforcement Information: sensitive personal information on individuals or law enforcement sensitive information i.e., "law enforcement only", "official use only" or "confidential" information; release of which could adversely affect or jeopardize follow up investigative or law enforcement activities.
3. Sensitive Personal Information: consists of an individual's name, including the last name along with the individual's first name or first initial, in combination with and linked to any one or more of the following data elements:
 - Social security number;
 - Driver's license number;
 - State identification card number issued by the registrar of motor vehicles or a deputy registrar under section 4507.50 of the Revised Code, or an equivalent state identification card number issued by a similar agency in another state;
 - Financial account number;
 - Credit card number;
 - Debit card number; or
 - Health Information