

## More Details on Securing Data

### **Requirements for safeguarding data**

According to the Oregon Identity Theft Protection Act, a security program includes the following and will be considered in compliance with the requirements to maintain reasonable safeguards to protect personal information:

- **Administrative safeguards**
  - Designate one or more employees to coordinate the security program.
  - Identify reasonably foreseeable internal and external risks.
  - Assess the sufficiency of safeguards in place to control the identified risks.
  - Train and manage employees in the security program practices and procedures.
  - Select service providers capable of maintaining appropriate safeguards, and require those safeguards by contract.
  - Adjust the security program in light of business changes or new circumstances.
  
- **Technical safeguards**
  - Assess risks in network and software design.
  - Assess risks in information processing, transmission and storage.
  - Detect, prevent, and respond to attacks or system failures.
  - Regularly test and monitor the effectiveness of key controls, systems, and procedures.
  
- **Physical safeguards**
  - Assess risks of information storage and disposal.
  - Detect, prevent, and respond to intrusions.
  - Protect against unauthorized access to or use of personal information during or after the collection, transportation, and destruction or disposal of the information.
  - Dispose of personal information after it is no longer needed for business purposes or as required by local, state, or federal law by burning, pulverizing, shredding, or modifying a physical record and by destroying electronic media so that the information cannot be read or reconstructed.

Owners of a small business, defined as 200 or fewer employees in manufacturing business or 50 or fewer employees in other types of business, comply with the safeguard requirements if its information security and disposal program contains the administrative, technical, and physical safeguards and disposal measures appropriate to the size and complexity of the business as well as the nature, scope of its activities, and the sensitivity of the personal information it collects including personnel records.