Oregon Consumer Identity Theft Protection Act (SB 583)
Safeguard Best Practices

Agency Safeguard Best Practices

Agencies are entrusted with many varieties of sensitive and confidential information. This includes the personal information of a variety of consumers including clients, customers, licensees and employees. As owners and custodians of that information, agencies are responsible for protecting those assets from loss or misuse.

Effective protection of consumer information requires a foundation of responsible information security practices and standards. Security standards are not "one size fits all." The application of standards will vary, depending on agency size and complexity, geographic locations, line of business, sensitivity of information collected and stored, and use of outside contractors.

To assist in agency implementation of the safeguard provisions of the Oregon Consumer Identity Theft Protection Act, the Department of Administrative Services offers a series of best practices to be considered as agencies implement the required information security programs. These best practices are intended to provide a high-level, non-technical overview of responsible security practices but are not intended as a comprehensive list of all security measures that can be implemented.

The best practices incorporate industry best practices and the requirements of the Oregon Consumer Identity Theft Protection Act. The best practices are divided into three categories, each addressing a specific provision of the Act. They include administrative, technical and physical controls.

- Administrative controls include, for example, implementation of agency-level information security policies, employee training and awareness, risk assessments, and managing vendors.
- Technical controls include managing access to sensitive information, establishing good password practices, and ongoing monitoring to assess threats and vulnerabilities.
- Physical controls include establishing physical access controls, managing physical access, and securing facilities.

The best practices are presented in the form of a checklist so agencies can assess their own risk levels and determine which standards to implement.

Administrative Safeguards Best Practices Checklist

1.0	Security Program Coordination	Required	Optional	N/A
1.1	Appoint one or more employees to coordinate the security program			

2.0	Security Policies	Required	Optional	N/A
2.1	Establish formal, written security policies			
2.2	Ensure policies apply to entire agency			
2.3	Ensure appropriate policies exist to cover various operations of the agency			
2.4	Ensure policies integrate with other enterprise policies			
2.5	Align the policies with other compliance policies such as privacy			
2.6	Determine regulatory compliance needs as relevant to the information and customers			
2.7	Periodically review policies, revising them as necessary based on changing business, technology, and environmental conditions			
2.8	Disseminate policies to all relevant stakeholders within the agency			
2.9	Consider developing an external version of policies for outside stakeholders including contractors			

3.0	Standard Operating Procedures	Required	Optional	N/A
3.1	Establish standard operating procedures			
3.2	Periodically review standard operating procedures, revising them as necessary based on changing business, technology, and environmental conditions			
3.3	Disseminate standard operating procedures to all relevant stakeholders within the agency			

4.0	Security Risk Assessment	Required	Optional	N/A
4.1	Conduct ongoing security risk assessments			
4.2	Identify and prioritize security risk threats and vulnerabilities			
4.3	Consider, at a minimum, risk in these areas: employee training and management; information systems; and prevention, detection, response to attacks or other system failures			
4.4	Periodically review risk assessments and revise them, as necessary, especially in response to business, technology and environmental changes			

5.0	System Security Plan	Required	Optional	N/A
5.1	Develop a system security plan for every major system and network			
5.2	Conduct a periodic review of system security plans and revise them as necessary			

5.3	Ensure plans and policies for security periodic review and control endpoints such as desktop PCs, laptops, PDAs and other devices that connect to sensitive networks or systems			
5.4	Require system interconnection agreements			
5.5	Require user system access agreements			
5.6	Conduct a periodic review of system interconnection agreements and revise them as necessary			

6.0	**Security Audits**	**Required**	**Optional**	**N/A**
6.1	Establish security auditing process			
6.2	Conduct a periodic review of all security controls through internal or external audit			
6.3	Include Web applications as well as host, network and user accounts as part of the audit			

7.0	**Employee Awareness**	**Required**	**Optional**	**N/A**
7.1	Require all employees to undergo basic initial and refresher security training			
7.2	Track and document completion of training			
7.3	Support continuing professional training and education for security specialists			

8.0	**Outsourced Activities**	**Required**	**Optional**	**N/A**
8.1	Establish special procedures for outsourced IT or information management activities			
8.2	Obtain certification from the vendor that they are in compliance with the agency's privacy and information assets protection obligations as required by law or stated policies			
8.3	Impose contractual controls over vendors' information asset use and practice			
8.4	Whenever feasible, determine the adequacy and competence of the outsourced vendor's key personnel, especially those individuals who are responsible for handling or managing sensitive personal information			

Technology Security Best Practices Checklist

1.0	Access Control to Storage Devices	Required	Optional	N/A
1.1	Control access to information that resides on data storage devices such as servers, desktop PCs, laptops and PDAs			
1.2	Use unique ID or username for all system users. Ensure that neither Social Security nor account numbers are used as an ID or username			
1.3	Use authentication mechanisms such as passwords, tokens and biometrics			
1.4	Require system administrators to use regular user accounts for work that does not need enterprise-wide system or security administration privileges			
1.5	Assign access privilege based on a need to know; the level of access should only relate to job function and not be based on agency position or rank			
1.6	Whenever feasible, utilize a two-factor authentication procedure before granting access to a consumer's sensitive information			
1.7	When possible, implement a method for online service requests concerning changes in usernames and passwords			
1.8	Force appropriate session timeouts such as 15 minutes or less, if idle			

2.0	Passwords	Required	Optional	N/A
2.1	Establish a password usage policy that encompasses the following rules:			
2.2	Whenever feasible, use a minimum of eight-digit alphanumeric format			
2.3	Instruct users to create such passwords during a periodic password change process			
2.4	Prohibit passwords based on account number, username, real name, Social Security number or publicly available personal details such as birthdays, names of children or pets, etc.			
2.5	Restrict password reuse			
2.6	Establish a formal user authentication process for resetting passwords; when possible, make password change or reset option available from the login page			
2.7	Allow users to update their password hints or questions			
2.8	When sending a registration confirmation or other type of welcome email, provide only the username within the email and implement a password reset feature on the Web site			
2.9	Username and passwords should not be sent together within the same email			
2.10	Force password expiration			
2.11	Establish lost/stolen laptop procedures, including password cancellation			

3.0	Access Control to Information	Required	Optional	N/A
3.1	Control access to information that can be displayed, printed or downloaded to			

	external storage devices, especially desktop PCs, laptops or PDAs			
3.2	Have operating controls that restrict downloads of sensitive information without proper identification			
3.3	Have screen savers and screen shields to minimize the display of sensitive information to unauthorized users			
3.4	Have shutdown controls when computers are idle or inactive			
3.5	As much as possible, limit the use of personally identifiable information on laptops, PDAs, PCs and other system when there is not a direct business need for doing so. Where such use is essential, ensure that information is encrypted or, at a minimum, that such laptops are protected by something stronger than a password			

4.0	**Monitor**	**Required**	**Optional**	**N/A**
4.1	Monitor user accounts to identify and eliminate inactive users, specifically:			
4.2	Accounts that have been inactive for 30 days should be disabled and automatically terminated after 60 days			
4.3	Accounts of terminated employees and contractors should be shut down within 24 hours			
4.4	Regularly monitor for newly created accounts			
4.5	Regularly cross-check user accounts against HR records to ensure that access by former employees has been terminated			

5.0	**Transmission and Storage of Information**	**Required**	**Optional**	**N/A**
5.1	Use reasonable encryption methods when transmitting or receiving sensitive information, especially when sent or received over the public Internet			
5.2	When feasible, use an industry-vetted wireless encryption protocol (e.g. WPA or WPA2) when transmitting or receiving sensitive information from PDAs, Web phones, laptops, and emerging devices that use Bluetooth connection technologies			
5.3	Use wireless authentication to validate the identity of wireless users in conjunction with encryption whenever possible			
5.4	Use reasonable encryption methods for storage, especially when maintaining sensitive information on servers, desktop PCs, and laptops and portable media (e.g. backup tapes, thumb drives, USB hard drives)			
5.5	Use VPN software to authorize and encrypt traffic from authorized devices and ensure that VPN access has adequate controls and is monitored			
5.6	Use configuration monitoring tools to flag storage devices that are removed from the network or enterprise system			
5.7	Restrict the downloading of sensitive personal information from central storage devices onto personal computers or wireless storage devices or other portable media/devices			

6.0	Configuration of Servers, Desktop PCs and Laptops	Required	Optional	N/A
6.1	Disable unused ports			
6.2	Know what processes are running on your systems and log new processes to be validated against change management processes			
6.3	Install/enable automatic screen locks to prevent access after a certain period of inactivity			
6.4	Change all vendor-supplied default passwords			
6.5	Ensure that an appropriate wireless encryption protocol is enabled prior to allowing wireless devices to be connected to enterprise systems or networks			
6.6	Treat all internal wireless connections as external connections			
6.7	Routinely check for unauthorized external access capability, including wireless access points			
6.8	Confirm that default software installations and configurations are appropriate for agency security needs including, as appropriate, changing default passwords and appropriately adjusting security parameters			

7.0	Configuration of Firewalls	Required	Optional	N/A
7.1	Firewalls should be configured to provide maximum protection over information, balancing business needs with reasonable security			
7.2	Establish a formal process for approving and testing all external network connections			
7.3	Establish a firewall at each Internet connection			
7.4	Establish a firewall between any DMZ and intranet connection			
7.5	Utilize multi-layered firewall configurations to protect sensitive information			
7.6	Validate firewall configurations with vulnerability tools available from vendors			
7.7	Conduct application-level assessments to ensure application and database security			
7.8	Whenever possible utilize intrusion detection and intrusion prevention systems (IDS/IPS) to assist in the detection and prevention of network-based incidents			
7.9	Know what network traffic is “normal” for your network			

8.0	Anti-Spyware Software	Required	Optional	N/A
8.1	Install and configure anti-spyware software to provide maximum protection of sensitive information on all servers, desktop PCs and laptops			
8.2	Ensure automatic downloads and updates to enterprise systems or networks			
8.3	Ensure automatic downloads and updates to desktop PCs, laptops and PDAs that are connected to enterprise systems or networks			
8.4	Perform frequent scans of information storage using enabling technologies to detect, quarantine and remove viruses, worms and Trojans			

8.5	Instruct employees not to download unknown attachments that could contain viruses, worms, spyware or keystroke loggers potentially giving unauthorized individuals access to the agency's network. This applies to the user of any computer that has access to the agency's network including the home computer of a telecommuting employee or a traveling employee logging in from a hotel or other public access point.			
8.6	Be careful to avoid potentially infected Web sites			

9.0	**Software Updates and Patches**	**Required**	**Optional**	**N/A**
9.1	Implement security software updates and patches in a timely manner			
9.2	Install security patches as soon as practical after the release date			
9.3	Establish a process to identify newly discovered vulnerabilities by subscribing to alert services that report current external threats			
9.4	Ensure that all servers are up to date with respect to application version and security patches			
9.5	Scan servers for configuration issues			
9.6	Implement a configuration process			

10	**Software Development**	**Required**	**Optional**	**N/A**
10.1	When developing software, create and implement security-focused application development procedures			
10.2	When possible, use desktop tools to validate and correct code issues			
10.3	Filter all user inputs prior to screening input data for size, type, format and conformance to business rules			
10.4	Reject input that does not validate rather than try to sanitize the data before processing, displaying or saving the supplied input			
10.5	Encode all user output			
10.6	When connecting to other systems or databases utilize least privilege			
10.7	When feasible, do not run applications as root, administrator, system or other identity with elevated privileges			
10.8	Ensure error messages do not disclose information that could be used to compromise the application or its environment			
10.9	Classify the application and data based on the sensitivity of information stored or processed by it			
10.10	Implement quality assurance and testing procedures; this would include detecting, measuring, and managing security defects as part of QA			
10.11	Include training on security tools as part of the software development life cycle			
10.12	Develop procurement and acceptance procedures to apply when purchasing third part software			
10.13	Validate vendor and third party code for acceptable risks			

10.14	Develop staging and integration procedures; make sure project owners evaluate application risks before public release			
10.15	Conduct ongoing application assessments for existing production code and one for each maintenance cycle release			
10.16	Integrate security throughout the system life cycle, including requirements definitions, design/procurement procedures, and testing and maintenance procedures			

11	**Data Backups**	**Required**	**Optional**	**N/A**
11.1	Establish formal data backup processes			
11.2	Ensure data backups include the maintenance of current access controls			
11.3	Conduct periodic reviews and tests of data backup processes and revise them as necessary			

12	**System and Network Configurations**	**Required**	**Optional**	**N/A**
12.1	Document all system and network configurations			
12.2	Establish a formal configuration/change control process, including vulnerability identification and patching, with pre-production testing			
12.3	Document and classify all sensitive information (information asset inventory)			
12.4	Document formal and appropriate rules of behavior, acceptable use and confidentiality agreements for all personnel with access to sensitive information			
12.5	Document all appropriate separation of duties, e.g., system administrators and security administrators should not be the same person			
12.6	Document routine and emergency termination procedures			

13	**Incident Response**	**Required**	**Optional**	**N/A**
13.1	Document a formal incident response capability			
13.2	Establish a formal, written incident response plan			
13.3	Establish clear roles and responsibilities for incident response			
13.4	Develop a process for reporting and escalating incidents			

Physical Controls Best Practices Checklist

1.0	Monitor Use and Access	Required	Optional	N/A
1.1	Conduct surveillance of unusual Internet activities, such as Web browsing or use of peer-to-peer file sharing software; consider any applicable legal restrictions on monitoring			
1.2	Conduct surveillance of unusual email			
1.3	Perform periodic or random reviews of documents and software contained on agency-issued laptop computers and PDAs			
1.4	Monitor software licenses for inactive or pirated copies			

2.0	Physical Access Controls	Required	Optional	N/A
2.1	Establish physical access controls			
2.2	Install PIN devices, smart cards and biometric readers at physical entrances			
2.3	Restrict physical access to the data center to only those people who have a legitimate business need			
2.4	Establish a method to recognize employee access rights and privileges			
2.5	Keys and passes, especially master keys, should be carefully controlled with frequent reviews and reconciliation			
2.6	Establish a method to terminate access rights once employee or contractor illegal activities are detected or strongly suspected			
2.7	Establish a method to differentiate employees from contractors			

3.0	Secure Checkpoint Review and Monitoring	Required	Optional	N/A
3.1	Install secure checkpoint review and monitoring procedures			
3.2	Implement a security or reception desk, especially at the entrance where sensitive or confidential information is house or is accessible			
3.3	Implement a formal process for granting access to those areas and for maintaining the list of people with physical access			
3.4	Identify and monitor the movement of all visitors by using temporary badges or machine readable devices			
3.5	Take appropriate security precautions in areas where access to sensitive information may be had; these can include special locks, security personnel, access controls, and other features			
3.6	In the most sensitive areas, such as data center, consider installing motion detectors, micro-switches and pressure pads or other equipment or measures to indicate when doors are opened or rooms entered			

4.0	Secure the Facility	Required	Optional	N/A
4.1	Secure the facility include all storage devices and computer equipment			

4.2	Locate loading docks or delivery areas in a remote area of the building far away from areas where processing or storing confidential information			
4.3	Control or limit access to junction boxes and telecommunications lines that enter or exit the data center			
4.4	Rooms that house especially sensitive equipment should have no external walls, doors, windows or skylights			
4.5	The area designated for enterprise systems or networks should be designed and built to support the agency's requirements for information security			
4.6	Secure cages and racks should be used to protect sensitive equipment; these should be locked routinely and keys carefully controlled			
4.7	Use locked cabinets to store printouts containing sensitive or confidential information			
4.8	Require documented approval by the data center's management before disconnecting or removing storage devices from the central IT configuration or system network			
4.9	Maintain logging procedures for all removable storage devices and media, including magnetic tapes			
4.10	Keep unused laptops and other mobile devices in a locked location to prevent theft			
4.11	Consider technologies and implementations that can effectively terminate remote access in case of compromised mobile equipment			

5.0	**Environmental Protections**	**Required**	**Optional**	**N/A**
5.1	Install and maintain reasonable environmental protections			
5.2	Install and maintain fire detection and suppression systems			
5.3	Implement uninterruptible power supplies (UPS)			
5.4	Use surge protectors on all equipment			