Deschutes County Administrative Policy No. GA-9
Effective Date: May 5, 2008
Updated: XXX, X, 2024

CONSUMER INFORMATION PROTECTION

STATEMENT OF POLICY

It is the policy of Deschutes County to comply with the Oregon Consumer Information Protection Act.

APPLICABILITY

This policy applies to all Deschutes County personnel who have access to social security numbers and personal information. This policy also applies to contractors, subcontractors, agents, intermediaries and others conducting business with the County.

POLICY AND PROCEDURE

General
Deschutes County will adhere to the Oregon Consumer Information Protection Act (ORS 646A.600 *et seq*.) as it currently exists and may from time to time be amended. The purpose of the act and this policy is to provide customers with protection from compromises of their personal information and to establish required steps in the case of a security breach.

This policy supplements current departmental privacy and confidentiality practices. If an applicable federal or state law (such as the HIPAA Privacy Rule) requires greater protection for the security or privacy of personal information, departments shall follow the higher standard. Should an amendment to the Oregon Consumer Information Protection Act conflict with any provision of this policy, the provision(s) of the Act shall take precedence.

Procedure

The Use of Social Security Numbers

- Departments shall not collect or use social security numbers unless there is an appropriate business reason for the use and there are no other practical alternatives.
- Departments are prohibited from using social security numbers on an identification card or other card that is used to obtain service.
- Departments shall not print social security numbers on cards or documents that are mailed to customers or publicly displayed unless the customer has requested information that requires a social security number. For example, a copy of a credit or employment application.
- Social security numbers may be used if the use is required by law, such as tax forms employers are required to send to the IRS.
- Departments are responsible for the proper disposal of social security numbers after there is no longer a business need. This may include shredding or rendering the material unreadable by some other means.
- Public records law permits the County to withhold employees' social security number and other "personal information." The County will not make this information public.

The Use of Personal Information

- "Personal information" for the purposes of this policy is defined in ORS 646A.602(12)(a) and is summarized as a customer's name in combination with one of the following:
    - Social Security number;
    - Driver license number or state identification card issued by the Department of Transportation;
    - Passport number or other United States issued identification number; or
    - Financial, credit or debit card number along with a security or access code or password that would allow someone else to access the person's financial account.
    - Data of an individual's physical characteristics that are used to authenticate one's identity (e.g. fingerprint)
    - Health insurance policy number with another unique identifier
    - Medical and/or mental health history
    - User names and passwords (or similar means to access an individual's accounts)
- Departments are required to establish administrative, technical, and physical safeguards to protect personal information.
    - Administrative safeguards include assigning an employee to coordinate the security program, identifying internal and external risks, and training employees.
    - Technical safeguards include assessing risks in network and software design; assessing risk in information processing, transmission, and storage; and testing and monitoring controls.
    - Physical safeguards include locking the material in file cabinets or storage systems; detecting, preventing, and responding to intrusions; and protecting against unauthorized access to the information.
- Departments are responsible for the proper disposal of personal information after it is no longer needed for business purposes. This may include shredding or rendering the material unreadable by some other means.
- Credit card receipts shall not include the full credit card number of the customer.

Safeguarding Paper and Electronic Documents

Employees shall take the following actions to safeguard paper and electronic personal information:

- Store paper documents in locked cabinets and storage systems, or in locked rooms or locked storage areas.
- If a computer has access to protected information, the computer shall be password protected and include a password protected lock screen.
- Ensure that observable confidential or individually identifiable information is shielded from unauthorized disclosure on computer screens and paper documents.

Breach of Security

- A breach of security is defined as an unauthorized acquisition of "personal information" a person maintains or possesses (as defined in this policy).
- Department Heads are required to immediately report breaches of security (including breaches that occur by contracted venders who maintain, store, manage, process or otherwise access personal information) to the County Administrator upon discovery.
- An incident response team consisting of representatives of Human Resources, County Administration, County Legal Counsel, and the Information Technology Department will investigate reported breaches of security and provide a written report to the County Administrator assessing the situation and recommending action steps and appropriate notifications to reporting agencies, if necessary.
- If a breach of security occurs, the County has a duty (under the Oregon Consumer Information Protection Act) to notify the individual(s) as soon as possible in one of the following manners: written notification, electronic (if this is the customary means of

communication with this customer), or telephone provided that direct contact with the affected customer is made. If notification is provided by telephone, it should be accompanied by written documentation that is maintained by the department/office. Examples include computerized data

that includes a customer's name along with their social security number or credit card number along with the associated security code. All notifications will be coordinated by the County Administrator.

- If the breach of security is unauthorized acquisition of paper-based personal information, the County will notify customers in the same manner as a breach of security related to computerized data.
- The notice shall include at a minimum the required information outlined in ORS 646A.604(5).

Identity Theft Language in Contracts

- All County contracts should include the following sentence: "Contractor and subcontractors shall comply with The Oregon Consumer Information Protection Act."

Approved by the Deschutes County Board of Commissioners XXX

Nick Lelack
County Administrator