BEFORE THE BOARD OF COUNTY COMMISSIONERS
FOR COLUMBIA COUNTY, OREGON

In the Matter of Adopting the Columbia County Personally Identifying Information Policy	)))	Order No. 79-2017

WHEREAS, the County is required to comply with the Oregon Consumer Identity Theft Protection Act, ORS 646.A.600 to 646A.628; and

WHEREAS, it is in the best interest of the County to establish a policy to protect consumers' personal information that the County receives, handles, and stores, and to comply with the Oregon Consumer Identity Theft Protection Act and related Federal regulations;

NOW, THEREFORE, IT IS HEREBY ORDERED, as follows:

1. That the Columbia County Personally Identifying Information (PII) Policy, which is attached hereto, and is incorporated herein by this reference is adopted.

2. Within thirty (30) days of the effective date, all County employees, volunteers, elected officials, and authorized agents are required to sign a receipt acknowledging each such person has read and understands this Policy.

Dated this 1st day of November, 2017.

BOARD OF COUNTY COMMISSIONERS
FOR COLUMBIA COUNTY, OREGON

By: _____
Henry Heimuller, Chair

By: _____
Margaret Magruder, Commissioner

By: _____
Alex Tardif, Commissioner

Approved as to form

By: _____
Office of County Counsel

Exhibit "A"

Personally Identifying Information (PII) Policy

Policy Adoption Date:_____ Last Revision:_____

Principle:

Establish requirements and procedures for handling, storing and processing personally identifying information ("PII") of individuals.

1.0 Purpose

This policy sets forth the County's requirements for maintaining the privacy of PII in order to prevent identity theft, in accordance with the Oregon Consumer Identity Theft Protection Act, Oregon Revised Statute (ORS) 646A.600 to 646A.628. The purpose of this policy is to protect consumers' personal information that the County receives, handles, and stores, and to comply with the Oregon Consumer Identity Theft Protection Act and related Federal regulations.

2.0 Scope

This policy applies to all County employees, volunteers, and Elected Officials as well as authorized agents of the County.

3.0 Policy Statement:

3.1 General Policy. The County is entrusted with many varieties of sensitive and confidential information. This includes personal information of a variety of consumers including clients, customers, licensees, and employees. As owners and custodians of that information, the County is responsible for protecting those assets from loss or misuse. The loss of personal information can result in substantial harm to individuals, including identity theft or other fraudulent use of the information.

Employees, volunteers, Elected Officials, and authorized agents of the County are responsible for protecting personal information from unauthorized access. Access to personal information shall be restricted to a "need-to-know" basis and available only to those individuals authorized to use such information as part of their duties and with the requirement that they keep the information confidential and use it only for authorized business purposes.

3.2 Definitions.

3.2.1 "Breach of Security" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that the person maintains. "Breach of Security" does not include an inadvertent acquisition of personal information by a person or the person's employee or agent if the personal information is not used in violation of applicable law or in a manner
that harms or poses an actual threat to the security, confidentiality or integrity of the personal information.

3.2.2 "Confidentiality" means a security principle that works to ensure that information

is not disclosed to unauthorized subjects.

3.2.3 Consumer: An individual resident of Oregon or any other state. "Individual" means a person, who has provided Personal Information to the County for use in the County's business, vocation, occupation or volunteer activities. "Individual" includes both members of the public and employees, officers, and agents of the County.

3.2.4 Information: Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

3.2.5 "Person" means an individual, private or public corporation, partnership, cooperative, association, estate, Limited Liability Company, organization or other entity, whether or not organized to operate at a profit, or a public body.

3.2.6 "Personally Identifiable Information" or "personal information" means:

3.2.6.1 Consumer's first name or first initial and last name in combination with any one or more of the following data elements, if encryption, redaction or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has been acquired:

- A consumer's Social Security number;
- A consumer's Driver's license number or state identification card number;
- A consumer's passport number or other identification number issued by the United States;
- A consumer's financial account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a consumer's financial account;
- A consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer;
- Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction;
- Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; and

3.2.6.2 Any of the data elements or any combination of the data elements above, without the consumer's first name or first initial and last name, if: (1) the data element or combination of data elements would enable a person to commit identity theft against a consumer; and (2) encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable.

3.2.6.3 Personal Information and PII does not include information in a federal, state or local government record, other than a Social Security Number, that is lawfully made available to the public.

3.3 Personal Information/PII Requirements.

3.3.1 Affirmative Obligations. Employees, volunteers, elected officials, and authorized agents of the County must:

3.3.1.1 Be knowledgeable of agency safeguards and follow all procedures and processes established to protect information assets and PII;

3.3.1.2 Protect PII from unauthorized viewing;

3.3.1.3 Properly secure PII both when in use and when stored or filed electronically or in portable format (such as paper, discs, removable storage devices);

3.3.1.4 Obtain written permission from their Department Director to transport personal information outside of the physical boundaries of the agency;

3.3.1.5 Encrypt stored personal information when feasible;

3.3.1.6 Have a valid business purpose to send personal information over the network and a secure way to transmit. Never transmit via email unless encrypted;

3.3.1.7 Have prior written approval from their Department Director to download personal information to any portable or removable device;

3.3.1.8 Immediately report any suspected breach of personal information or loss of a file or device containing PII to a supervisor and/or the Human Resources/Risk Management Office;

3.3.1.9 Comply with HIPAA requirements for protected health information. See County HIPAA Policy (Order No. 25-2003);

3.3.1.10 All Departments that accept credit or debit cards shall comply with PCI requirements.

3.3.2 Prohibited Conduct. Except as provided in 3.3.3, below, employees, volunteers, elected officials, and authorized agents of the County must not:

3.3.2.1 Print an individual's Social security number on any materials not requested by the individual or part of the documentation of a transaction or service requested by the individual that are mailed to the individual, unless redacted;

3.3.2.2 Print an individual's Social Security Number on any card required for the individual to access products or services provided by the County;

3.3.2.3 Publicly post, publicly display, communicate, or otherwise make available to the general public a document containing an individual's social security number, unless redacted;

3.3.2.4 Use more than the last 4 digits of a Social Security Number on

documents unless there is a compelling business reason to use the entire Social Security number. If a document does contain the full Social Security Number, the County employee, will take steps to protect the document from unauthorized disclosure.

3.3.3 Section 3.3.2 does not prohibit the collection, use, or release of a Social Security number as required by state or federal law, or the use or printing of a Social Security Number for internal verification or administrative purposes or for enforcement of a judgment or court order. In addition, the Section does not apply to records that are required by state or federal law to be made available to the public. Finally, the section does not apply to a Social Security number in some Court records.

3.3.4 Breach of Security. The County is required to notify individuals if any electronically stored information or written document that contains personal information about that individual has been subject to a security breach. Any breach of security shall be reported to the person's Department Head. The Department Head shall notify the Office of County Counsel as soon as possible, but no later than the next business day following a breach of security. The County will implement notice requirements required by ORS 646A.604, as amended, including, but not limited to notice to the Attorney General, and other applicable law.

Examples of breaches of security include but are not limited to: loss or theft of an electronic device (such as laptops, Personal Digital Assistants (PDAs), tablets, smartphones, thumb drives) unless the information has been encrypted.

3.3.5 Safeguarding Personal Information. Any County department that collects personal information must develop, and implement reasonable safeguards to protect the security and confidentiality of the information. Employees with access to personal information must take reasonable steps to prevent a breach of information. Reasonable steps include but are not limited to locking file cabinets; monitoring who has access to areas containing personal information, locking computer workstations if leaving the area; maintaining physical control over files, computer workstations and laptops which contain personal information; never saving personal information on the C:drive; never copying or storing personal information on portable media, unless the data is encrypted; securing personal devises with passwords, and never sending emails containing personal information unless the data is encrypted. Employees must also ensure the proper disposal of documents or other media which contains personal information. Any such documents or media must be shredded or wiped/disposed of by IT. If the internet allows the public to access County information, Departments must ensure that personal information acquired as part of the service is not inadvertently made available to the public via the internet or through a Public Records Request. Each Department shall designate a person responsible for security of personal information, and reducing the risk of breach.

3.3.6 PCI Compliance. The County IT & Finance Departments will conduct annual security assessments of personal information in compliance with credit card industry requirements. Such annual assessments will begin as soon as possible. Departments that accept credit or debit cards as forms of payment will assist as requested in the annual security assessments. As noted in the Cash Handling Standards adopted XXXXX, the County Treasurer must be involved in any proposed new credit card or debit card acceptance business processes.

3.4 Effect of Changes to Laws Applicable to this Policy

This policy is intended to be in compliance with any and all applicable laws at the time of the adoption. If applicable laws change, and this policy has not been amended to reflect the impact of such changes, the County shall amend its procedures and the application of this policy to reflect the current

state of the law, even if an amendment to this policy to reflect those changes has not been formally adopted by the County.

3.5 Compliance

Failure to comply with any provisions of this policy may lead to discipline up to and including termination. Every County officer, agent, employee, and volunteer shall review this policy and sign an acknowledgment that they have read and understand public official obligations and prohibitions under this Policy.

Acknowledgment Form

I acknowledge that I have received a copy of the Columbia County Personally Identifying Information (PII) Policy and that I have read and understand the Policy.

_____
Signed

_____
Printed Name

_____
Date