Attachment T: PASCO COUNTY BCC
ADMINISTRATIVE POLICIES AND PROCEDURES MANUAL

SUBJECT: Information Security Personally Identifiable Information Policy

SECTION: Information Technology POLICY NUMBER: 600-07

PREPARED: May 3, 2017 REVISED: May 28, 2019

I. PURPOSE:

This policy and supporting procedures are designed to provide a documented and formalized Personally Identifiable Information (PII) policy that is to be adhered to and utilized throughout the organization at all times.

Compliance with the stated policy and supporting procedures helps ensure the safety and security of the County's system resources. PII requires strict measures for ensuring unauthorized parties do not have access to such data, which can be in electronic format and/or paper. Additionally, with the growing cyber security threats and the ever-increasing number of data breaches and security compromises, protecting PII is now more important than ever.

The policies and procedures below help to ensure the overall *confidentiality, integrity, and availability* of highly sensitive confidential information.

II. POLICY:

The County creates, collects, maintains, uses, and transmits personally identifiable information relating to individuals associated with the County including, but not limited to, customers, constituents, vendors, contractors, consultants, commission members and employees. The County is committed to guarding PII against inappropriate access and use in compliance with applicable laws, regulations, and County policy in order to maximize trust and integrity.

Further, this Policy and the Procedures implement reasonable measures to safeguard Protected Personally Identifiable Information and other information the Federal awarding agency or pass-through entity designates or the County designates as sensitive consistent with applicable Federal, state, local and tribal laws regarding privacy and obligations of confidentiality. (2 CFR 200.303(e)).

A. DEFINITIONS

1. ***Personally Identifiable Information (PII)*** [Federal law definition]- information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

a. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example:

i. first and last name,
ii. address,
iii. work telephone number,
iv. email address,
v. home telephone number, and
vi. general educational credentials.

The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

(2 CFR 200.79 Personally Identifiable Information (PII))

2. ***Protected PII*** [Federal law definition]- an individual's first name or first initial and last name in combination with any one or more of the following types of information, including, but not limited to:

a. social security number,
b. passport number,
c. credit card numbers,
d. clearances,
e. bank numbers,
f. biometrics,
g. date and place of birth,
h. mother's maiden name,
i. criminal, medical and financial records,
j. educational transcripts.

THIS DOES NOT INCLUDE PII THAT IS REQUIRED BY LAW TO BE DISCLOSED.

(2 CFR 200.82 Protected Personally Identifiable Information (PII)).

B. IDENTIFYING PROTECTED PII FOR PURPOSES OF FEDERAL AWARDS

1. As described in the definitions above, under Federal law, Protected PII does not include PII that is required to be disclosed.
2. Under the Florida Public Records Laws, generally, everything is required to be disclosed unless the Florida legislature or constitution, or Federal law provides an exemption or for confidentiality. (Section 119.01, Florida Statutes, Article 1, Section 24, Florida Constitution, 2 CFR 200.337)

3. The examples below are Protected PII in Florida because they are exempted from public disclosure by specific exemptions in Florida or Federal law.

    a. *FULL NAME IN COMBINATION WITH* any part that is stored or displayed in conjunction with any of the subsequent listings of data or *INFORMATION IN b. – j. BELOW IS DEEMED PROTECTED PII*.
    b. National Identification information, such as passports, visas, permanent residence cards, voting information, social security number, or any other type of unique identifier used on a national level.
    c. Local and/or state, provincial, etc. information, such as drivers licenses, vehicle registration, or any other type of unique identifier used on a local and/or state or provincial level.
    d. Digital identifiers, such as IP addresses, usernames, passwords, etc.
    e. Facial, fingerprint, iris and all other associated biometric information.
    f. Date of birth and place of birth
    g. Medical records (i.e. Protected Health Information (PHI) and electronically Protected Health Information (ePHI), and all associated data and information contained (electronically or physically) with the medical records.
    h. Criminal records that reveal the identity of victims or witnesses.
    i. Financial and Accounting records, such as banking and tax information, along with credit and debit card information.
    j. Educational information for currently enrolled students, such as classes taken, schedule, grades received, degrees confirmed, disciplinary actions, financial aid, and student loans.

4. Exhibit A is a summary of Florida statutory and constitutional exemptions that the County is most likely to be affected by and that deal specifically with personal information. A summary of nearly all Florida statutory and constitutional exemptions from the open public records laws, not just those dealing with PII, is attached as Exhibit B.
5. Examples of Federal laws the County may be affected by and making certain PII information exempt from disclosure are included in Exhibit C.

C. DATA CLASSIFICATION

All PII should be evaluated to determine the PII confidentiality impact level. This assessment will ensure the County applies appropriate safeguards for PII. Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the County should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All County data should be classified into one of two sensitivity levels:

1. ***Level I – Protected Information:*** High risk of significant financial loss, legal liability, public distrust or harm if this data is disclosed.

a. Specific Protected PII information exempt from public disclosure pursuant to Federal law and Florida Statute, for example:

i. Data protected by Health Information Portability and Accountability Act (HIPAA) (i.e. animal bite cases, workers comp cases, emergency services information, etc.)
ii. Data protected by Health Information Technology for Economic and Clinical Health (HITECH) Subtitle D – (addresses privacy and security concerns associated with the electronic transmission of health information, which provides provisions that strengthen HIPAA rules)
iii. Data subject to Payment Card Industry Data Security Standards (PCI DSS) standards (i.e. credit or payment card information)
iv. Data protected by The Family Educational Rights and Privacy Act (FERPA) (i.e. student information including grades, official correspondence, financial aid, scholarship records, etc.)
v. User Names and Passwords (i.e. Windows login, application specific login, etc.)

2. ***Level II – Public Information****:* Low requirement for confidentiality (information is public) and/or low or insignificant risk of financial loss, legal liability, public distrust or harm if this data is disclosed.

a. Information that is publicly available pursuant to Florida Statute or Federal law and not coupled with other PII that would then make it Protected PII, for example:

i. first and last name
ii. address
iii. work telephone number
iv. email address
v. home telephone number
vi. general educational credentials
vii. telephone books
viii. public Web sites
ix. Pasco County listings

D. REGULATORY COMPLIANCE

Regulatory compliance laws, legislation, and industry specific rulings call for the protection of PII, and accordingly, the County is to identify compliance mandates regarding the safety and security of sensitive information, and the applicable measures for enforcement. The County should be familiar with the laws included in Exhibit A.

III. PROCEDURE:

A. GENERAL

All electronic files that contain Protected PII will reside within a protected information system. Protected PII is not to be downloaded to personal workstations or mobile devices (such as laptops, personal digital assistants, mobile phones, tablets or removable media) or to systems outside the protection of the County. Protected PII will not be sent through any form of insecure electronic communication, e.g., E-mail or instant messaging systems. Significant security risks emerge when Protected PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of Protected PII, the physical or electronic file should be shredded or securely deleted. All physical files that contain Protected PII will reside within a locked file cabinet or room when not being actively viewed or modified.

B. DATA CLASSIFICATION

1. All County employees are responsible for:

    a. Understanding what constitutes Protected PII and Public PII; and
    b. Managing Protected PII and Public PII in a manner consistent with the criticality of and the requirements for confidentiality associated with the data in any form (electronic, documentary, audio, video, etc.) throughout the entire information lifecycle (from creation through preservation or disposal).

2. All County Protected PII and Public PII, whether at rest (i.e., stored in databases, tables, email systems, file cabinets, desk drawers, etc.) or in use (i.e., being: processed by application systems, electronically transmitted, used in spreadsheets, or manually manipulated, etc.) must be classified into one of the two data classification levels described in this policy by each department that is the Custodian of Records for that information.
3. The PII confidentiality impact level (I & II) indicates the potential harm that could result to the subject individuals and/or the County if PII were inappropriately accessed, used, or disclosed.

C. APPLYING SAFEGUARDS

The County departments that are the Custodians of Records for specified information should apply appropriate safeguards to protect the confidentiality of PII based on the PII confidentiality impact level.

1. Develop comprehensive standards of operating procedures for protecting the confidentiality of Protected PII.
2. Create training materials and require that all individuals receive appropriate training before being granted access to systems containing Protected PII to reduce the possibility that Protected PII will be accessed, used, or disclosed inappropriately.

3. De-identify records by removing enough Protected PII so that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. Identifying and de-identifying records can be used when full records are not necessary, such as for examinations of correlations and trends.
4. Control access to Protected PII through access control procedures and define and create access enforcement mechanisms, such as access control lists.
5. Prohibit or strictly limit access to Protected PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices.
6. Protect the confidentiality of transmitted Protected PII. This can be implemented by encrypting data communications or by encrypting the information before it is transmitted.
7. Monitoring and reporting events that affect the confidentiality of Protected PII, such as inappropriate access to Protected PII.

D. EXCEPTIONS

If there is an operational or business need to store Protected PII outside the County, please contact the Information Security Team for approval and assistance in securing the information.

E. INCIDENT REPORTING

In the event of a real or suspected unauthorized disclosure of Protected PII data the Information Security Team must be notified as soon as reasonably possible. Unauthorized disclosure includes but is not limited to misplacing a paper report, loss of a laptop, mobile device, or removable media containing Protected PII, accidental email of Protected PII, possible virus, or malware infection of a computer containing Protected PII or a breach of security. Be prepared to provide information that will provide a clear definition of the breach involving Protected PII. Also, if the information relates to a Federal or State Grant award, then the appropriate funding agency must be notified promptly of any breech of the Protected PII. The following information is helpful to obtain from employees who are reporting a known or suspected breach involving Protected PII.

1. Person reporting the incident
2. Person who discovered the incident
3. Date and time the incident was discovered
4. Nature of the incident
5. Name of system and possible interconnectivity with other systems
6. Description of the information lost or compromised
7. Storage medium from which information was lost or compromised
8. Controls in place to prevent unauthorized use of the lost or compromised information
9. Number of individuals potentially affected
10. Whether law enforcement was contacted

F. NOTICE OF BREACH OF SECURITY

The County Information Security Officer shall provide notice of a breach of security of Personal Information to the State of Florida Department of Legal Affairs as required pursuant to subsection 501.171(3), Florida Statutes (2016).

Under the direction of the County Information Security Officer, the County shall provide the notice to individuals affected by a security breach of Personal Information and to Credit Reporting Agencies as required by subsection 501.171 (4) and (5), Florida Statutes (2016).

In the event of a breach of security of a system maintained by a third-party agent of the County (such as a credit card processor), the third-party agent shall notify the County of the breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred. Upon receiving notice from a third-party agent, the County, or the third party entity upon direction from the County, shall provide the notices required above.

Based on circumstances and severity of a paper data breach, the Information Security Officer will determine if notification must be issued to those that are affected.

G. AUDITS

Periodic audits of County equipment and physical locations may be performed by the Information Security Officer or delegates to ensure that Protected PII is stored in approved information systems or locations. The purpose of the audit is to ensure compliance with this policy, safeguard Protected Personally Identifiable Information and to continuously improve County business practices.

H. COMPLIANCE

Users found to have violated this policy may result in loss of privileges and/or subject to disciplinary action up to and including termination of employment. Criminal or civil action may also be initiated if appropriate.

I have read, understand, and agree to comply with the Information Security Personally Identifiable Information Policy specified above. Signature indicates acceptance.

RESPECTFULLY SUBMITTED:

Authorized Signature: _____

Printed Name and Title: _____

Telephone: _____