# Personally Identifiable Information (PII)

POLICY AND RECOMMENDATIONS

# Training Objectives

At the end of this training you will understand:

- The definition of Personally Identifiable Information
- The risks associated with PII
- How to protect and mitigate the risks associated with PII

# Definition

## Personally Identifiable Information (PII)

- Can be used to trace an individual's identity
- Alone or combined with other data
- And is linked or linkable to a specific individual.

# Two kinds of PII

## Public PII

- Info available in public sources, such as telephone book.
- Examples: Name, address, phone, general education credentials, associations, such as college or clubs, etc.

## Protected PII

- Public info when combined with private info, such as…
- Examples: SSN, passport, credit cards, date/place of birth, mother's maiden name, educational transcripts, etc.

# Example

## Mary Jones (public PII)

- Member of the Workforce Board
- Director of Local Business School
- Work Address
- Work Phone

But if you add <u>just one</u> of these protected PII items, Mary could have her identity stolen.

- SSN
- Date of birth
- Passport
- Credit cards
- Bank numbers
- Mother's maiden name

# Major Breaches of PII

Who does a PII breach effect and where does it occur?

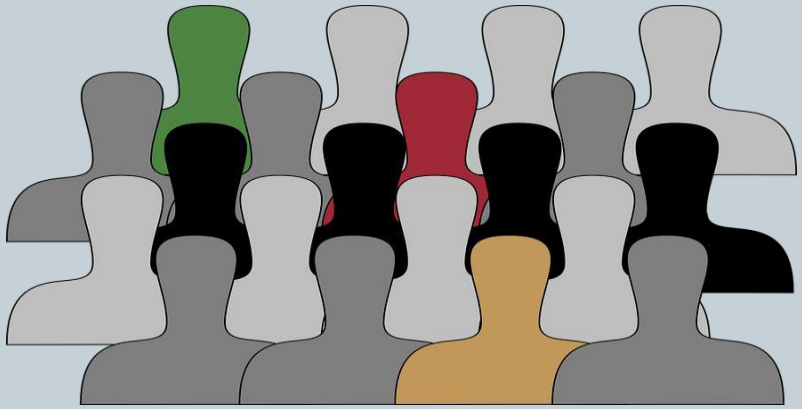
# Major Breaches of PII

## Where might your data be?

- Info available in public sources, such as telephone book.
- Examples: Name, address, phone, general education credentials, associations, such as college or clubs, etc.

# Requirements

**Staff must be trained and sign an acknowledgement that they understand this policy.**



# PII

- All PII must be protected
- No unencrypted data can be sent via email.
- PII and files should not be left unsecured.

# PII


- Restrict access to PII to authorized persons only.
- Process PII data under strictest confidentiality

# EW Policy

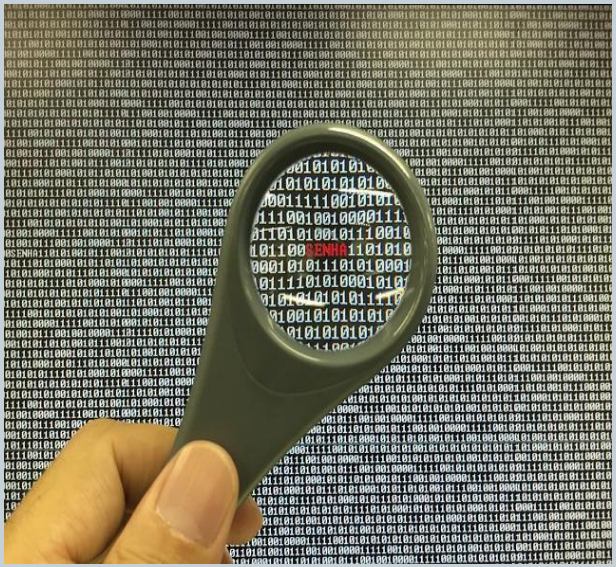
- Ensure PII confidentiality is preserved during transmission.  Use encryption.
- Follow Agency Destruction policies for data destruction.

# Recommendations

**Store PII data obtained in an area that is physically safe from access by unauthorized persons at all times.**

**Store files containing PII in locked cabinets when not in use.**

# Recommendations



- Do not leave records containing PII open and unattended.
- Immediately report any breach to Chief Executive Officer and your supervisor only.

# Penalties

- Failure to comply will  result in disciplinary actions up to and including termination.
- There could be possible civil or criminal sanctions.

# Summary

## What you have learned today

- What is Personally Identifiable Information (PII)
- The risks associated with not protecting PII
- Important to report possible breach
- How to protect PII