


Policy Title:	Confidentiality of Personal Identifiable Information		
	OFFICE OF THE CHIEF ADMINISTRATIVE OFFICER	Category	Human Resources
		Administrative Policy #	
		Revision #	N/A
		Review Frequency	As Needed – no less frequently than triennially
Administrative Division	Human Resources	Reviewed By	Chief Administrative Officer, General Counsel, Human Resources Director
BOWC Approval		Last Reviewed/Update Date	5/24/19
Implementation Date			

1. OBJECTIVE

- 1.1. To protect the integrity of DWSD customer and employee Personal Identifiable Information from unauthorized use or modification and from accidental or intentional damage or destruction by persons authorized to access DWSD confidential information.

2. PURPOSE

- 2.1. To establish guidelines and responsibilities for information security to maintain the confidentiality, integrity, and availability of DWSD employee and customer Personal Identifiable Information. The DWSD recognizes its need to maintain the confidentiality of Personal Identifiable Information (PII) and understands that such information is unique to each individual. The PII covered by this policy may come from various types of individuals performing tasks on behalf of the DWSD and includes employees, applicants, independent contractors and any PII maintained on its customer base.

3. DEFINITIONS

“Confidential” or “Personal Identifiable Information (PII)” means first and last name, home or other physical address, contact information including a postal, e-mail, or Internet protocol address or telephone or facsimile number, social security number, taxpayer identification number, driver’s license, state ID or any other information including date of birth, medical documentation, racial or ethnic background, or religious affiliation that would serve to identify an individual.

4. SCOPE

- 4.1. This policy applies to all DWSD employees, contractors, student interns, volunteers, and other persons authorized to access confidential information of DWSD’s records.

5. RESPONSIBILITIES

5.1. Human Resources Director

- 5.1.1. The Human Resources Director is responsible for publishing this policy; communicating this policy to all employees; review, approval and publishing of divisional standard operating procedures; and for updating this policy as necessary.
- 5.1.2. The Human Resources Director, or delegate, is responsible for interpreting and enforcing this policy; ensuring that PII resource is in compliance with Departmental policies and standards.

5.2. Human Resources

- 5.2.1. Supporting the need for appropriate PII controls within the Human Resources division, supporting DWSD PII security awareness and education program efforts.
- 5.2.2. Providing direction and support for the continual development, implementation, and maintenance of DWSD-wide confidentiality of PII policy and procedures.
- 5.2.3. Providing information as necessary to DWSD about existing and emerging legal and compliance requirements and about best practices associated with PII security as well as reviewing exceptions to this policy to ensure their appropriateness and legality.

5.3. Management

- 5.3.1. Management is responsible for monitoring work areas for compliance and addressing any incident(s) of noncompliance and alerting Human Resources when a violation has occurred.

5.4. Employees

- 5.4.1. The employee is responsible for being familiar with and fully complying with this policy, including protecting electronic and paper copies of PII. Employees are responsible for maintaining the confidentiality of PII to which they are given access privileges.
- 5.4.2. Reporting all suspected security and/or policy violations to the appropriate authority (e.g. Team Lead, Division Director or Department Manager, and/or Human Resources).

6. POLICY

6.1. Handling of Confidential Information

- 6.1.1. Customer and personal employee information will be considered confidential and as such will be shared only as required and with those who need to have access to such information. All hard copy records will be maintained in locked, secure areas with access limited to those who have a need for such access. Personal employee information used in system applications will be safeguarded under DWSD information security policy and security systems. Participants in DWSD benefit plans should be aware that personal information will be shared with plan providers as required for their claims handling or record keeping needs.
- 6.1.2. DWSD human resources information, which may include organizational charts, department titles, staff charts, job titles, department budgets, company coding and recording systems, telephone directories, email lists, company facility or location information and addresses may be subject to the Freedom of Information Act. DWSD maintains the statutory right to withhold from disclosure any information that is exempt from disclosure under the Freedom of Information Act.

6.2. Reasonable and Necessary Accommodations

- 6.2.1. Management may take reasonable and necessary actions to accomplish the intent of this policy.

7. PROCEDURE

7.1. External requests

- 7.1.1. External requests for records (subpoenas, court orders or FOIA requests) are managed through the DWSD's Office of General Counsel for appropriate distribution. Any response to outside requests for employee or customer information will be responded to in conjunction with the Office of General Counsel.

7.2. Reporting Failure to Maintain Confidentiality of Personal Identifiable Information

- 7.2.1. If an employee becomes aware of a material breach in maintaining the confidentiality of his or her personal information, a fellow employee's information, or a customer's information, the employee should report the incident to a representative of the Human Resources Division. The Human Resources Division has the responsibility to investigate the incident and take corrective action. A standard of reasonableness will apply in these circumstances.
- 7.2.2. Examples of the release of personal employee information that will not be considered a breach include the following:
 - 7.2.2.1. Release of partial employee birth dates, i.e., day and month is not considered confidential and will be shared with supervisors who elect to recognize employees on such dates.
 - 7.2.2.2. Personal telephone numbers or e-mail addresses may be distributed to supervisors or designees in order to facilitate company work schedules or business operations.
 - 7.2.2.3. Employee identifier information used in salary or budget planning, review processes and for timekeeping purposes will be shared with appropriate individuals.
 - 7.2.2.4. Employee's work anniversary or service recognition information may be distributed to appropriate individuals periodically.
- 7.2.3. Examples of the release of personal customer information that will not be considered a breach include the following:
 - 7.2.3.1. Confirmation of account holder's name when corresponding to confirm information for landlord-tenant account transfers.
 - 7.2.3.2. Internal usage of account information when used in the course of conducting normal business operations.