FOREST PRESERVES of Cook County	POLICY PROCEDURE GUIDELINES	POLICY NUMBER: 02.30.00.	PAGE NUMBER: 1 of 3
		SUBJECT: Identity Protection Policy	Adopted: **12/8/2015** Latest Revision: **04/15/2016** Next Review:

02.30.00. POLICY STATEMENT

The Forest Preserve District of Cook County (the "District") recognizes that it is important to safeguard Social Security Numbers ("SSNs") and other personal information ("PI") against unauthorized access. By the end of 2016, the District will assess its personal information collection practices, and make necessary changes to those practices to promote confidentiality and to comply with this policy.

02.30.01. PURPOSE

The Illinois Identity Protection Act (the "IPA") requires each local and state government agency to draft, approve, and implement an Identity Protection Policy that references the IPA and includes restrictions regarding the access and use of SSNs and PI as well as training for those employees who hold such data. The purpose of this policy is to comply with the IPA and all other applicable laws and statutes.

02.30.02. REFERENCES

Identity Protection Act: (5 ILCS 179/)
http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3174&ChapterID=2

Personal Information Protection Act (815 ILCS 530)
http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67

Cook County Personnel Rules
Rule 8: Conduct and Discipline of Personnel

Forest Preserve District of Cook County: Employee Handbook
Rules of Conduct

02.30.03. DEFINITIONS

Personal Information ("PI"): PI means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: **(1)** Social Security number; **(2)** Driver's license number or State identification card number; and/or **(3)** Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

* PI does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.

02.30.04. SCOPE

This policy applies to all District employees. District employees who violate this policy may be subject to discipline up to and including termination, as well criminal prosecution of a Class B Misdemeanor pursuant to the IPA.

02.30.05. RESPONSIBILITY

Legal Department: The Legal Department shall: **(1)** review Department Head/Senior Staff requests to collect and/or disclose SSNs; and **(2)** provide a response to Department Head/Senior Staff requests within three **(3)** business days.

Finance & Administration: The Finance & Administration Department shall: **(1)** direct efforts to assess the District's collection of personal information practices by the end 2016; and **(2)** make necessary changes to those practices to ensure compliance with the intent of this policy by the end of 2016.

Department Heads: Department Heads/Senior Staff shall eliminate the need for their Departments/Offices to request, store, and/or distribute SSNs or PI, if such action is not necessary to carry out District business and/or aligned with this policy (as described below).

District Employees: All District employees shall comply with this policy.

02.30.06. PROCEDURES

A. Approval Process to Collect SSNs: Generally, before a District Department Head, or other senior staff member, collects any individual's SSNs, the Department must submit a request in writing to the Legal Department for approval and an explanation as to why the SSN collected is relevant to the documented need and purpose.

B. Approved SSN Collection/Disclosure Purposes: The District may only collect or disclose SSNs for one or more of the following reasons: **(1)** Human Resources Purposes (ex. On-Boarding, Off-Boarding, etc.); **(2)** Financial, Administrative, Legal Purposes (ex. Payroll Processing, Verifications, Investigations, etc.); **(3)** Law Enforcement Purposes; **(4)** Compliance with Federal, State, Local Law and Regulation Requirements and/or requests; and/or, **(5)** Vendor Services, such as Executing Contracts and/or Billing as required by law, ordinance, policy, and/or other agreement.

C. Prohibited Disclosure Activities: As per the mandates set forth in the IPA the District may not do the following, unless otherwise allowed by law or mandated through order of the court: **(1)** Publicly post or publicly display in any manner an individual's full social security number; **(2)** Print an individual's SSN on any card required for the individual to access products or services provided; **(3)** Require an individual to transmit his or her SSN over the Internet, unless the District's connection is secure or the SSN is encrypted; **(4)** Print an individual's SSN on any materials that are mailed to the individual, through the U.S. Postal Service, any private mail service, electronic mail, or any similar method of delivery, unless State or federal law requires the SSN to be on the document to be mailed; **(5)** Require a person to use his or her SSN to access an internet website; and **(6)** Use the SSN for any purpose other than the purpose for which it was collected.

D. Personal Information (PI) Policy:

1. Only employees who are required to use or handle information or documents that contain SSNs or PI should have access to such information or documents.

2. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his/her supervisor.

3. All records containing SSNs, or other PI, whether on- or off-line, in electronic or physical format, are considered confidential information and should be maintained appropriately.

4. Any documents containing SSNs must be redacted if required to be released as part of a public records request. Therefore, any SSNs requested from individuals should be placed on the document in a manner that makes it easily redacted. If and when these records are no longer needed, disposal of the records must be handled in a secure fashion and follow the Record Retention laws and policies.

E. Electronic Distribution Policy: Any PI sent externally should include the following statement in the e-mail or letter: *"This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."*

02.30.07. TRAINING REQUIREMENTS

1. All District employees identified as having access to SSNs and other PI in the course of performing their duties shall be trained on this policy.

02.30.08. ACTION PLAN TO COMMUNICATE/DISSEMINATE

1. This policy should be distributed to all applicable employees.

2. This policy should be added to the District shared drive, intranet, and website.

3. Department Heads should work to ensure that their staff are knowledgeable about this policy.

If you have questions, comments, or suggestions concerning District policies, please contact:

Forest Preserve District of Cook County
Office of the General Superintendent
Attn: Anthony D. Tindall, Policy Director
69 W. Washington St., Suite 2040, Chicago, IL 60602
Office: (312) 603-8351; Email: Anthony.Tindall@cookcountyil.gov