Rule XI-6 Information Security

A. PURPOSE

This policy assigns responsibility for the security of City-wide, departmental, administrative and other critical ~~City of Hammond~~ information. Components of security include confidentiality, availability, and integrity.

B. DEFINITIONS

Information technology resources:
Specific items such as telecommunications devices, computer systems, media, and other equipment, goods, services, and personnel related to the collection, storage or transport of electronic information.

Critical data:
Data that is so important to the City of Hammond that the loss or unavailability is unacceptable.

Federal Information System:
A federal information system is a system used or operated to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of information, in any form, by or for the federal government.

Personally Identifiable Information (PII):
Personally identifiable information is 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. Some information that is considered to be PII is available in public sources such as telephone books, public websites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and 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.

C. APPLICABILITY

This policy applies to all information ~~collected, and/or processed~~ created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of using the City's information technology resources. In the case of PII, applicability also extends to information in any federal information system used or operated by the City.

D. POLICY

~~City~~ Information and information technology resources must be recognized as sensitive and valuable and be protected. Depending on the scope and nature of the information, integrity constraints and special procedures for access and handling may be required.

One of the fundamental requirements and goals of ~~City~~ information processing, whether manual or automated is to manage a single resource: information. This goal drives all others as the City works to define, manage, guard the integrity of, bring access to, and mobilize this resource. The individual data elements and their interface to the larger process must be protected and managed.

E. PROCEDURES

Departments shall develop, manage and review their own operating policies and procedures and include information security as part of their department's processes. Integrity constraints, procedures that ensure correct processing of correct data, shall be written as departmental procedure. Such procedures should be reviewed as required, at least once a year.

Actual or Imminent Breach of PII

In the event of an actual breach or the detection of an imminent breach of PII, the IT Director shall be immediately notified. The IT Director shall then immediately notify the Mayor or, in his/her absence, the Director of Administration of the actual or imminent breach and take action to limit further exposure of PII and to protect the City's information technology resources.

No later than 24 hours after an occurrence of an actual breach or the detection of an imminent breach of PII 1) associated with an Office of Justice Programs (OJP)-funded program or activity or 2) in any federal information system used or operated by the City, the IT Director and/or the Grants Director shall notify an OJP Program Manager of the actual or imminent breach.

F. RESPONSIBILITIES

The IT department is responsible for:

- Ensuring the security, confidentiality, and availability of data and software stored on individual computers and on centrally-managed computer systems.
- Ensuring the backup of critical data and software
- Providing account management
- Establishing and maintaining the physical security of the central computing facilities.
- Establishing and maintaining the physical security of the communications network.
- Establishing and maintaining the physical security of data for which the Information Technology Department (IT) is the custodian.

This policy also places responsibility on TEAM Leaders to:

- Encourage appropriate computer use as specified in the Appropriate Use of Information Technology Resources policy
- Ensure compliance with information technology policies and standards by people and services under their control
- Implement and monitor additional procedures as necessary to provide appropriate security of information and technology resources within their area of responsibility.

G. SANCTIONS

Sanctions will be commensurate with the severity and/or frequency of the offense and may include termination of employment; however, termination of employment does not fall under the realm of the IT department.

H. EXCLUSIONS

None.

I. INTERPRETATION

Authority to interpret this policy rests with the Mayor and Director of Administration, and is generally delegated to the Director of the IT department.