Assistance & Guidance on

CITY OF TALLAHASSEE
Sam M. McCall, CPA, CIA, CGFM
City Auditor

"Departments' Responsibility Regarding Information Exempt from Public Record"

Report #0202   **November 7, 2001**

Introduction

The purpose of this assistance and guidance report is to provide: 1) direction to departments on what information is exempt from public record; 2) examples of exempt data; and 3) assistance to departments regarding what their responsibilities are to protect that information.

In summary, departments are responsible for:

- following the appropriate City policies and procedures;
- knowing their data and the related laws, rules, and regulations regarding whether it is or is not a public record; and
- taking appropriate actions to adequately protect it on the network and within the application.

Background

Our office recently completed an audit that addressed the logical security of the City's local area network (Audit Report #0201).

There are two basic types of security controls that together can protect information resources: physical and logical. Physical security controls address restricting access to the location where computer hardware and equipment are housed. Logical security controls address restricting access into specific information systems and applications so that only authorized individuals can perform functions on the system.

The City stores information on computers in files or applications housed 1) on the user's individual hard drive; or 2) in folders on the network. Logical security controls should be in place to control access to both locations in order to protect the data from improper disclosure, or inadvertent or malicious acts that could damage or destroy the data.

User IDs, passwords, and password protected screen savers are common controls to protect data on local hard drives. For data stored on the network, departments are responsible for knowing who should have access to their data and notifying Information Systems Services (ISS) so they can set the network security appropriately. Access within the application is the

responsibility of the application security administrator in the department that "owns" the application. Typically, this department is the key business user of the application.

In non-police operations, selected personal data is stored for employees and customers, and can include (but is not limited to): home address and phone number, social security number, and bank account numbers. Such data may be considered public record or exempt from public record. In police operations, there is a great deal more information that is exempt from public record, including (but not limited to) data related to juveniles, victims, and criminal intelligence, and data defined to be exempt via court order.

As part of the logical security audit, we noted that some of the data that should be exempt from public record was not always adequately protected in the various City's information systems to prevent improper disclosure.

Chapter 119, Florida Statutes (F.S.), provides for the inspection, examination, and duplication of all public records. There are, however, many exemptions to this statute. According to Chapter 119, F.S., exemptions are "created or maintained only if the exempted record or meeting is of a sensitive, personal nature concerning individuals; the exemption is necessary for the effective and efficient administration of a governmental program; or the exemption affects confidential information concerning an entity."

During our audit, we worked with City departments to identify the types of data that were being stored in City information systems and whether the data was protected by a federal or state law, or local ordinance. In addition, we also worked with the City Attorney to obtain counsel regarding the legal interpretation of some of the exemptions and with Human Resources staff to ensure that their forms and instructions are consistent with those legal interpretations.

Examples of information the City Attorney agrees are exempt from public record (clarifications are in italics) are shown below in Table 1.

| **Table 1** |
| **Examples of City Information Exempt from Public Record** |
| ⇒ Section 119.07(3)(x) states that all employees' social security numbers are exempt. |
| ⇒ Section 119.07(3)(z) states that bank account numbers or debit, charge, or credit card numbers given to an agency for the purpose of payment of any fee or debt owing are confidential and exempt. |
| ⇒ Section 119.07(3)(i) states that specific personal information is exempt from public record (including but not limited to: home address and phone number, social security number) for individuals in certain public positions, and in some cases, their spouses and children. Such positions in the City include: active and former law enforcement personnel; revenue collection and enforcement or child support enforcement; active firefighters (certified according to F.S. 633.35); current and former code enforcement officers; current and former human resource, labor relations, or employee relations directors, assistant directors, managers, or assistant managers whose duties include hiring and firing employees, labor contract negotiation, administration, or other personnel-related duties.

Additional clarifications and recommendations by the City Attorney include:
o *The statutes specifically do not include "former" firefighters, however, the City Attorney* |

> *recommends including former firefighters in the "exempt from public records" category for safety purposes.*
>
> o *The statutes specifically identify certified firefighters. Although other fire department personnel are involved in fire department operations, the City should include only those that are certified in the "exempt" category. Also, there was a question about former certified firefighters that are now employed in non-firefighting positions in the City. If they were firefighters at one time, the City Attorney recommends continuing keeping their personal information exempt from public record.*
>
> o *The City has employees in Accounting/Payroll that are responsible for garnishing employees' pay for child support. The Florida Statutes are unclear as to exactly which persons in local government that collect child support revenue should be exempt from public records. The City Attorney recommends that the persons in payroll responsible for the garnishment (about 3-4) should be included in the "exempt" category.*
>
> o *Regarding the human resource positions and those **whose "duties include hiring and firing employees, labor contract negotiation, administration, or other personnel-related duties,"** this can be interpreted in many ways. The City Attorney recommends that the human resource positions that should be protected here include only those persons who make the ultimate decisions regarding hiring and firing employees.*

⇒ Section 119.07(3)(i)(1,2) states that personal information for persons <u>not</u> employed at the City may also be exempt from public records, such as law enforcement officers from other municipalities, supreme court justices, appeal judges, circuit court judges, and county court judges, current or former state attorneys, assistant state attorneys, statewide prosecutors, or assistant statewide prosecutors, or other persons identified in Section 119, F.S. The City will maintain the confidentiality of the personal information only if the officer, employee, justice, judge, other person, or employing agency of the designated employee submits a written request for confidentiality to the City. <u>It is that person's responsibility to make the request.</u>

⇒ Section 119.07(3)(b-h) addresses police-related information that is exempt, including (but not limited to) criminal intelligence, criminal investigations, identity of selected victims and surveillance techniques. (Note: There are other statutes that address police operations and information. Police Department Standard Operating Procedure RCD-4 can provide more detailed information.)

⇒ Section 119.07(3)(o) states that data processing software that is sensitive is exempt from public record. This includes: software applications that store data exempt from public record; software that collects, processes, stores, and retrieves agency payroll and accounting records; and control and access authorizations and security measures for automated systems.

⇒ Section 119.07(3)(cc) states that medical history records, bank account numbers, credit card numbers, telephone numbers and information related to health or property insurance furnished by an individual to any agency pursuant to federal, state, or local housing assistance programs are confidential and exempt from public record.

⇒ Section 119.07(3)(r) states that all records supplied by a telecommunications company (as defined by Section 364.02, F.S.) to a local governmental agency that contain the name, address, and telephone number of subscribers are confidential and exempt from public record.

> ⇒ The City receives funding from federal grants that require that specified information be protected from disclosure (<u>OMB Circular A-130</u>, Transmittal Memorandum #4, dated 11/28/00, Management of Federal Information Resources, web site: http://www.whitehouse.gov/omb/circulars/a133/a133.html). Examples of such information include drug testing of transportation workers, medical information of passengers utilizing special transportation services, and testing results for hepatitis B. To comply with these grants, the City must take measures to adequately protect this data.

The City Attorney was of the opinion that any City actions should focus on providing the highest protections to current and former employees in classifications shown above.

Additional information and forms can be found by accessing the Human Resource Intranet web site. This site provides information regarding what information is exempt from public record, City forms, and a link to Chapter 119, F.S. (*http://ntapps8/human_resources/ City_Forms/public_records.htm - list*)

Departments' Responsibility

All City processes, including information systems, should protect the personal information of those employees that are exempt from public records as well as other non-employee persons (citizens served by the City) that meet the criteria <u>and have requested</u> the City to keep their information confidential.

City departments are responsible for:

♦ following Administrative Procedures #206, "Public Records Policy," and processing appropriate public records requests through the Treasurer-Clerk's Office;

♦ knowing what types of data is stored in their application systems and network folders;

♦ notifying ISS regarding who should have access into their departmental folders on the City network;

♦ specifying the level of application security required for their operations and supporting information systems;

♦ determining who is given access to their application system and what transactions they can perform, such as inquire only, add, change, and/or delete; and

♦ notifying the application security administrator regarding what access capabilities are appropriate for their department users.

The above information should assist you in determining what information (if any) is exempt from public record by federal or state law, or local ordinance.

The above examples obtained from Chapter 119, F.S., may not cover all information exempt from public record that is maintained by the City. Department management should request assistance from the City Attorney if they need help in making that determination.