GENERAL ORDER

DURHAM POLICE DEPARTMENT
DURHAM, NC

NUMBER:
2031

SECURITY OF SENSITIVE & CONFIDENTIAL INFORMATION

Effective Date: **11/10/2010**	Revision Dates:

INTRODUCTION

The Durham Police Department will maintain procedures for the protection of sensitive and confidential information. Sensitive data is privileged or proprietary information which if compromised through alteration, corruption, loss, misuse or unauthorized disclosure could cause serious harm to the organization or person owning it. Sensitive data maintained by the Department includes, but is not limited to, social security numbers, drivers' license numbers, personal medical information protected by HIPAA, law enforcement intelligence information, notes and files related to on-going investigations, employee personnel files, credit card information, and the home phone numbers and addresses of police personnel.

This General Order and the Standard Operating Procedures developed by each Unit and Division within the Police Department will supplement and not supersede City policy FP 706.03, Security of Sensitive and Confidential Information and Breach Response Plan.

REGULATIONS

Employees who have access to sensitive and confidential information will create, handle, maintain and dispose of such information with prudent care to avoid unauthorized access through a technology or physical breach. The following regulations must be followed to maintain confidentiality:

- Access to sensitive and confidential information will be limited to authorized employees.
- If sensitive information is written on paper for reference, it must be shredded upon recording the information in the final destination unless this information is considered criminal discovery and must be maintained in the case file as described in GO 4070.
- Sensitive information will not be included on printed reports except as needed for the performance of essential tasks.
- Upon leaving your work area, log off or lock the workstation.
- Documents that contain sensitive information will be stored in a locked file cabinet or secured room and access to the area will be limited to appropriate personnel.

- Sensitive and confidential information will be released in accordance with State Statute and staff will consult the City Attorneys as appropriate before releasing sensitive and confidential information to third parties.

- Any employee who becomes aware of an unauthorized access of sensitive and confidential information must report the incident immediately to their supervisor, who in turn, will report the incident through their chain of command to the Chief of Police.

- Persons authorized to handle sensitive and confidential information will be required to read this General Order, their unit's Standard Operating Procedures, City Policy #FP 706.03 and sign the City's "Sensitive Information User Agreement" (Attachment 1) which will be maintained in the employee's personnel file.

PURGING SENSITIVE DOCUMENTS

Documents ready for destruction according to the Municipal Records and Retention Schedule that contain sensitive and confidential information will be disposed of by shredding. Documents will never be disposed of in a trash can or recycle bin if the documents have not been shredded. Employees authorized to handle sensitive and confidential information must have supervisory approval before destroying such documents.

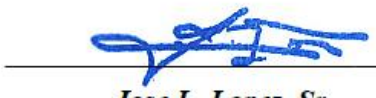
Documents with sensitive and confidential information will be shredded by the individual who has authorized access to the data or by another employee who is in the presence of the authorized employee.

The Department may enter into a contract with a third party in the business of record destruction to destroy sensitive and confidential information in a manner consistent with City policy #FP 706.03.

STANDARD OPERATING PROCEDURES

Each Division and Unit in the Police Department that handles sensitive information will develop Standard Operating Procedures which detail the following information:

- Specific types of sensitive information maintained and the reasons why it is maintained.
- Specific position titles within the Division/Unit that have access to the information.
- To whom the information may be released to and under what conditions.
- The location and method for secure storage of the information when not in use.
- The retention period for the sensitive information.
- The disposal method at the end of the retention period.



Jose L. Lopez, Sr.
Chief of Police