

CITY OF NEW ORLEANS
CHIEF ADMINISTRATIVE OFFICE

POLICY MEMORANDUM NO. 100

June 11, 1996

TO: All Departments, Boards, Agencies, and Commissions

FROM: Marlin N. Gusman, Chief Administrative Officer

SUBJECT: GFS SECURITY

I. PURPOSE.

This memorandum establishes security policies for GFS, the City's computerized financial management system.

II. POLICY.

Computer data is a valuable asset of city government. All data has an assigned owner or agency that has responsibility for the accuracy and integrity of that data and authorization of access to it.

The Management Information Systems Division of the Chief Administrative Office assists in the maintenance, backup, and technical support of all departmental data. MIS provides control of access to all data and capability for timely recovery from disaster.

Individual may view and work with the data only with the approvals of their appointing authorities, the owner agency, and MIS.

The MIS Security Administrator is responsible for insuring that information is protected in accordance with this policy.

Any violation of this policy may result in disciplinary action, including termination.

III. PROCEDURE.

A. To Gain Access.

1. Anyone who needs access to GFS for data or transactions must complete a GFS User Request Form. Information on the form should include the user's name, the user's department, bureau, telephone number, and the profiles desired. A list of profiles and a User Request Form can be obtained from the MIS Security Administrator.
2. The appropriate appointing authority must sign the form to indicate approval of access.

3. If access is requested to data or transactions that have a different assigned owner, the appointing authority for the assigned owner agency must also sign approval on the User Request Form.
4. The appointing authorities of the Chief Administrative Office and the Department of Finance may authorize multi-departmental access for those under their supervision who need wider access.
5. The completed User Request Form shall be submitted to the MIS Division of the Chief Administrative Office.
6. The approved user will be notified that the two levels of security tables have been adjusted to allow access.

B. To Remove Access.

1. If an approved user terminated employment, immediate written notification shall be sent to the MIS Security Administrator to delete that user from the security tables.
2. If a user transfers from one agency to another, the MIS Security Administrator shall be notified so the user can be suspended from access until a new GFS User Request Form is received.
3. If a user does not sign on to GFS for six (6) months, that user will be deleted or deactivated automatically.

C. Records.

The MIS Security Administrator will maintain records of all approved users. The record for each user will include the user name, agency, telephone number, and capabilities along with a list of profiles that the person is allowed to use.

D. Security Logs.

The MIS Security Administrator may choose to activate any of the three security logs in the computer system.

1. The **Security Violation Log** keeps a record of failed attempts to access the system or perform actions. Through this system administrators can monitor attempts by users to perform unauthorized actions.
2. The **Approval Log** records all approvals applied or removed from documents and batches.

3. The **Override Log** records user overrides of error in documents and batches.

E. User Approval Protocol

When requesting approval for a user to look at data or execute transactions, agencies should remember the separation of powers developed to maintain the integrity of the City's financial systems, as required by the independent auditor. The following protocols should be followed.

1. A user with authorization to **approve** transactions in a profile group **may not** enter data in the same group.
2. Approval capability should be requested only for the senior employee of a group or an employee with supervisory responsibility in the agency.
3. To be issued a GFS User ID, an employee must be authorized for mainframe computer access.
4. A User ID is issued to an individual and is not transferrable and not to be used by anyone else. Violation of this protocol may result in disciplinary action against both parties.
5. Each user is responsible for protection of the personal password. If a user thinks the personal password has been compromised, it is the user's responsibility to change the password.

IV. INQUIRIES.

Questions regarding this memorandum should be referred to the MIS security Administrator.

MNG/LRF/itb