PROCEDURES FOR VISIONS USERS

Access to the District’s financial management system (Infinite Visions) can be granted or modified at any time. To request access to the system or to change an employee’s access profile, complete the Visions User Account Request Form.

Access to the District’s financial data carries with it important responsibility. Supervisors who approve Infinite Visions access for employees must have authority over the budget for which access is requested. Information made available through system access should only be shared when appropriate. Employees with access to payroll and/or vendor information in the District’s financial management system (Infinite Visions) must sign the Visions User Confidentiality Agreement Form.

If your Visions user role changes, you move to another department, or if you manage someone whose role changes, you must request a change in the user’s access profile immediately.

Requests for access to the District’s financial management system should come from the employee’s direct supervisor. The Visions User Account Request Form should be completed and submitted to the Business Manager in District’s Finance Office for review and approval. Once approved by the Finance Office, the IT department will implement your request. The employee’s direct supervisor will need to validate the following information:

(1) Employee information,
(2) Access authorization,
(3) Intended system usage,
(4) Employee’s employment status (employee transfers or termination must be reported immediately)

The District’s IT department will establish the employee’s username and system access and communicate it back to the employee’s supervisor. The username and password will allow employee’s access to the District's financial management system. Employees should reset their password immediately and not share their passwords with anyone. The District will hold employees accountable for all activities associated with their user accounts.

At least once a year the District’s Business Manager and the IT Director shall review the list of Visions users to certify that:

(1) Visions users have the minimum access privileges required to perform their job responsibilities
(2) Only pre-identified personnel have access rights for administration or security functions of the system.
(3) Access or changes in user access was granted only when initiated via written request from the user’s direct supervisor.
(4) Inactive user accounts are disabled.
(5) Employee terminations are disabled.