GOVERNMENT OF THE DISTRICT OF COLUMBIA
DEPARTMENT ON DISABILITY SERVICES

PROCEDURE	
Subject: MCIS Utilization	Procedure No.: 2013-DDA-POL-021
Responsible Program or Office: Developmental Disabilities Administration	Effective Date: October 21, 2013
Date Approved: September 20, 2013	Number of Pages: 2
Cross References, Related Policies and Procedures, and Related Documents: MCIS Utilization policy; Individual Support Plan Distribution procedure; Behavior Support Plan Oversight and Safeguards procedure; Incident Reporting procedure	

1. PURPOSE

The purpose of this procedure is to establish the standards and guidelines by which DDA's providers will enter, update, maintain and protect the confidentiality of data through DDA's information system, MCIS.

2. APPLICABILITY

This policy applies to all DDS providers and vendors that provide services and supports to people with disabilities as part of the DDA service delivery system, funded by DDS or the Department of Health Care Finance ("DHCF").

3. PROCEDURES

A. Providers are responsible for requesting access to MCIS for their staff and for terminating access as soon as the employment relationship ceases, by sending an MCIS Access Request form signed by the provider agency's Executive Director, or his or her designee, to the DDA IT Specialist. Providers must send a request to terminate access to the DDA IT Specialist by email within 24 hours from the time the employment relationship has ended.

1. The DDA IT Specialist shall respond to all initial requests for access within five (5) business days. Providers should only request MCIS access for staff whose job functions would include using MCIS, such as residential managers and Qualified Developmental Disability Professionals.

2. Provider MCIS accounts automatically terminate if they are not used for 30 consecutive days. If an account automatically terminates, the provider must send

the MCIS Access Request form to the DDA IT Specialist with a request to re-establish the account. These requests will be responded to within five (5) business days.

3. The DDA IT Specialist will terminate access for provider employees within one (1) business day of receiving the request from the provider.

4. MCIS account passwords may not be shared while access for a new employee is pending, or at any other time.

B. Providers are responsible for ensuring that their employees, consultants, contractors, and volunteers who have access to MCIS reset their password every 30 days, using the "change password" function within MCIS.

C. Providers are responsible for regularly using MCIS, including but not limited to:

1. Accessing copies of a person's Individual Support Plan ("ISP") in accordance with DDS's ISP Distribution procedure;

2. Entering all reportable and serious reportable incidents, in accordance with DDS's Incident Reporting procedure;

3. Uploading a person's Behavior Support Plan ("BSP") and all supporting documents, in accordance with DDS's BSP Oversight and Safeguards procedure;

4. Tracking all adaptive equipment repair and replacement needs; and

5. Entering or uploading any other information, as requested by DDS.

D. Providers are required to have a quality assurance and improvement system that ensures that all required information is entered or uploaded into MCIS in a timely manner, and that the information is up-to-date, accurate, and complete.

E. Providers shall train all of their employees, consultants, contractors, and volunteers who have access to MCIS on how to safeguard the confidentiality of people's records, specifically including training on D.C. statutory requirements regarding confidentiality of people's records and the Health Insurance Portability and Accountability Act's ("HIPAA") requirements on confidentiality of protected health information. Each person accessing MCIS is responsible for using it such a way as to protect people's private information.

F. DDS may sanction providers who do not comply with the requirements of the MCIS Utilization policy and/ or this procedure.