Data Management Group Policy
Data Access Control

Policy Identification Number: DMG-2009-005-SE
Policy Name: Data Access Control
Date Approved: September 24, 2009
Approval Authority: Data Management Group (DMG)
Statutory Reference: Statewide Information Security Manual as authorized by N.C.G.S. 147-33.110, FERPA Regulations

Policy Statement: Data managers will apply data access control when providing/granting access to source systems and transmission of data in accordance with the standards for Controlling Access to Information and Systems as detailed in Chapter 2 of the Statewide Information Security Manual (see link in Related Documents section), which has jurisdiction and authority provided by N.C.G.S. 147-33.110.

Reason for Policy: The DPI manages data (information and systems) that are considered confidential in nature by NC State Board of Education and Local, State, and Federal Standards/Policies/Legislation.

Policy Details and Related Documents: The DPI is obligated to protect all personally identifiable information (PII) data. All data managers are expected to be knowledgeable of and adhere to all relevant legislation, policies, and procedures related to access control and the security of PII. Important standards detailed in the Statewide Information Security Manual include managing access control, managing user access, controlling access to systems, passwords, monitoring system access and use, and other access procedures.

Related Documents: Chapter 2: Controlling Access to Information and Systems of the Statewide Information Security Manual: http://www.scio.state.nc.us/SITPoliciesAndStandards/Statewide_Information_Security_Manual.asp and DMG Policies: DMG-2009-001-RR Sharing Data with Researchers and DMG-2009-002-RR Requests for Personally Identifiable Information.

Contacts: Questions related to this policy or exception to the policy should be directed to the Enterprise Data Manager at 919-807-3241.

Revision History:

Version #	Version Date	Source file	Description of Change	Author

This policy applies to all data used by the agency in the performance of its mission. This data includes any that is collected, stored, processed, and/or disseminated using DPI information systems.