

Data Management Group Policy

Security of Confidential Data on Desktops and Laptops

Policy Identification Number: DMG-2009-001-SE

Policy Name: Security of Confidential Data in electronic form

Effective Date: April 9, 2009

Approval Authority: Data Management Group

Statutory Reference: N.C.G.S. [Chapter 132. Public records law.](#)

Policy Statement: All NCDPI full- and part-time, permanent and temporary employees, and contractors are responsible for the security of confidential data in electronic form.

Reason for Policy: To ensure security of confidential data in electronic form and to ensure compliance with state standards and federal requirements.

Policy Details: This policy ensures that electronic equipment is physically secure and that confidential data are backed up and protected through encryption only. (simple password protection without encryption is not appropriate) DPI will adhere to the State Security Standards on encryption to ensure the protection of confidential data from unauthorized users. Confidential data shall not be included in email unless the data has been encrypted according to NC Statewide Security requirements, prior to transmission. Passwords for encrypted data shall not be included in email. Additionally, all desktops and laptops will be secured based on the Desktop and Laptop Security Policy in the DPI Procedures Manual, Section 13.

Related Documents: Desktop and Laptop Security Policy in the DPI Procedures Manual, Section 13
<https://intranet.ncpublicschools.gov/divisions/technology-services/policies/DPI%20Desktop%20and%20Laptop%20Security%20Policy.pdf/view>

Statewide Information Security Manual – Chapter 1 section 1 Storing and Handling Information
<https://it.nc.gov/document/statewide-information-security-manual-2015>

Statewide Information Security Manual – Chapter 3 section 5 Securing Data
<https://it.nc.gov/document/statewide-information-security-manual-2015>

Contacts: The Division of Data, Research and Federal Policy is the proponent for this policy. Questions related to this policy or exception to the policy should be directed the Enterprise Data Manager at 919-807-3241.

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.

Revision History:

Version #	Version Date	Source file	Description of Change	Author
002	7/31/09	N/A	Subtitle Addition	Lauren Furer
003	6/17/13	N/A	Updated Related Documents and Division Name	Diane Dulaney
004	9/10/15	O:\PSP\DMG\Current Policy Drafts\Security Policies	Updated Statutory Reference and Related Documents	Diane Dulaney

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.