



THE NEW SCHOOL

Information Security Standard

General Controls for Handling Sensitive Information

Revision 1.0
January 18, 2012



RESTRICTED

TABLE OF CONTENTS

1	INTRODUCTION	1
1.1	Objective	1
1.2	Scope.....	1
1.3	Compliance	1
1.4	Exceptions.....	1
2	HANDLING SENSITIVE INFORMATION.....	3
2.1	General Requirements.....	3
2.2	Handling Paper Documents	5
2.3	Handling Electronic Information	6
2.4	Handling Spoken Communications	9
2.5	Disposing of Sensitive Information	9
3	DOCUMENT ADMINISTRATION.....	11
3.1	Document Owner.....	11
3.2	Document Review	11
3.3	Change history	11
3.4	Approval History.....	11

1 INTRODUCTION

This standard defines general controls for handling sensitive (Restricted and Confidential) information at The New School. These controls support the principles and objectives of *The New School Information Security Policy*, of which this standard is a component.

1.1 Objective

The objective of this standard is to describe the controls that must be implemented and practices that must be undertaken when handling sensitive information resources to ensure that the confidentiality, integrity, and availability of the information is properly safeguarded.

1.2 Scope

This standard applies to all offices and departments of the university.

1.3 Compliance

Compliance with this standard is mandatory.

1.4 Exceptions

Exceptions to this standard must be requested through the information security *Procedure for Policy Exception Requests*.

2 HANDLING SENSITIVE INFORMATION

The classification of an information resource determines the rules for accessing, processing, storing, transmitting, and disposing of that information. *The New School Information Security Policy* defines three information classifications: Unrestricted, Restricted, and Confidential.

Unrestricted information is information that can be disclosed to anyone inside or outside of the university, and does not have any special handling requirements other than routine due care to protect it against unauthorized modification, destruction, or loss. Restricted and Confidential information do have special handling requirements, however; these requirements are described in the table below.

	Restricted	Confidential
2.1 General Requirements		
Definition	Information that is generally not public, and whose disclosure, loss, or corruption may cause embarrassment or damage (financial or otherwise) to The New School. The sensitivity of this information is less than that of Confidential information.	Information whose disclosure, loss, or corruption would cause significant embarrassment or damage (financial or otherwise) to The New School or the individuals who are the subjects of the information. Confidential information includes any information that is protected under federal or state laws or regulations, personally identifiable information about faculty, staff, and students, and sensitive information about the university.
Clear Desk Policy	All papers and physical materials must be put away when not in use. Computer screens must be protected by a password-controlled screen saver when not in use.	All papers and physical materials must be put away in a locked drawer, file cabinet, or file storage room when not in use. Computer screens must be protected by a password-controlled screen saver when not in use.
Marking Requirements	Physical and electronic documents must display the word “RESTRICTED” in the header or footer of each page. Electronic data files (e.g., spreadsheets) must	Physical and electronic documents must display the word “CONFIDENTIAL” in the header or footer of each page. Electronic data files (e.g., spreadsheets) must

	Restricted	Confidential
	<p>display the word “RESTRICTED” in a similar manner.</p> <p>Removable media (USB flash drives, CDs, DVDs, etc.) must display the marking of the highest classification information stored on the media.</p>	<p>display the word “CONFIDENTIAL” in a similar manner.</p> <p>Removable media (USB flash drives, CDs, DVDs, etc.) must display the marking of the highest classification information stored on the media.</p>
Access Control Requirements	<p>Access to information must be limited to those individuals in roles with a need to know. Access may be granted on a group basis (e.g., to all employees in a particular job role or area). All access requests must be approved by the Information Owner.</p> <p>All personnel with access must receive the <i>Information Resource Acceptable Use Policy</i>.</p> <p>Strong passwords must be used. Passwords must be changed regularly.</p> <p>The Information Owner must regularly review the list of individuals with access and remove those individuals who have been terminated, transferred, or no longer have a need to know.</p>	<p>Access to information must be limited to those individuals with a need to know, and must be authorized on an individual basis. Groups may be used to manage access, but membership in the group must then be authorized on an individual basis. All access requests must be approved by the Information Owner.</p> <p>All personnel with access must agree, through their signature, to abide by the <i>Information Resource Acceptable Use Policy</i>.</p> <p>Strong passwords must be used. Passwords must be changed regularly. Two-factor authentication (e.g., tokens) should be used where feasible.</p> <p>Access rights for terminated and transferred individuals must be removed immediately. The Information Owner must regularly review the list of individuals with access and remove those individuals who no longer have a need to know.</p>
Distribution to Third Parties (not individuals; see below)	<p>May only be provided to third parties where a clear business purpose exists and there is a written confidentiality agreement in effect between the third party and The New School.</p>	<p>May only be provided to third parties where a clear business purpose exists, there is a written confidentiality agreement in effect between the third party and The New School, and there is a written agreement of security controls to be implemented by the third party.</p>

	Restricted	Confidential
		The Office of General Counsel and the Office of Information Technology must review and approve the confidentiality and security controls agreements to ensure they meet relevant legal and technical security standards.
Distribution to Individuals	May only be provided to the individual who is the subject of the information or an authorized representative.	May only be provided to the individual who is the subject of the information. Express written consent must be given by a student if he or she wishes to authorize his or her parents or legal guardians to discuss Confidential information with The New School.
2.2 Handling Paper Documents		
Storage	Store in folders or binders when not in use to prevent casual disclosure.	Store in locked desk or file cabinet drawers or other secure containers, or in secure file or storage rooms. Key/combination access limited to authorized individuals.
Copying	No restrictions on copying for business purposes. Copies must be collected from copy machine / facility promptly. Copies must retain classification markings or be applied manually.	Copying must be performed or supervised by an individual with authorized access to the information. Copy machine must not be left unattended while making copies. Copies must retain classification markings or be applied manually. Extra copies must be securely destroyed.
Facsimile	Recipient must be notified before sending, and must retrieve transmission promptly. Cover sheet must be used, and must indicate sender's name, contact information, and that the information is RESTRICTED.	Recipient must be notified before sending, and must be present to receive transmission immediately. Receiving telephone number must be confirmed

	Restricted	Confidential
		<p>before sending.</p> <p>Cover sheet must be used, and must indicate sender's name, contact information, and that the information is CONFIDENTIAL.</p> <p>Receipt of transmission must be verified by sender.</p>
Mailing & Courier Services	No restrictions on sending for business purposes.	<p>Documents must be placed in an internal envelope marked "CONFIDENTIAL" and labeled with sender's name and contact information.</p> <p>External envelope must not display information classification.</p> <p>Sending method must include signature-on-receipt and tracking capability.</p>
2.3 Handling Electronic Information		
Hard Drive/Network Storage	<p>File system access control features must be used to limit access (see "Access Control Requirements," above).</p> <p>May not be copied onto Internet-based hosting, storage, or backup sites unless an approved contract has been established between the provider and the university.</p>	<p>File system access control features must be used to limit access (see "Access Control Requirements," above).</p> <p>May not be copied onto Internet-based hosting, storage, or backup sites unless an approved contract has been established between the provider and the university.</p> <p>Must be encrypted, using university-approved encryption methods, when stored outside university premises.</p>
Copying	<p>No restrictions on copying for business purposes.</p> <p>Copies must be protected in the same way as the original.</p>	<p>Copying must be performed or supervised by an individual with authorized access to the information.</p> <p>Copies must be protected in the same way as the original.</p>

	Restricted	Confidential
Printing	<p>No restrictions on printing for business purposes.</p> <p>Printouts must be collected from printer / printing facility promptly.</p> <p>Printouts must retain classification markings or be applied manually.</p>	<p>Printing must be performed or supervised by an individual with authorized access to the information.</p> <p>Printer must not be left unattended while making printouts.</p> <p>Printouts must retain classification markings or be applied manually.</p> <p>Extra printouts must be securely destroyed.</p>
Electronic Mail	<p>May not be sent outside the university without a business purpose. No restrictions on sending within the university (“@newschool.edu”).</p> <p>Attachments must be labeled (see “Marking Requirements,” above). If the message text sent with the attachments is RESTRICTED, it must also be marked.</p> <p>Use of the New School Secure File Transfer service is recommended, but not required.</p>	<p>Use of the New School Secure File Transfer service is required when sending, both within the university and to outside addresses.</p> <p>Recipient’s electronic mail address must be confirmed before sending.</p> <p>May not be sent via “regular” electronic mail under any circumstances.</p> <p>Special exception for Student N-numbers: N-numbers may be sent via electronic mail when operationally necessary, but only to <i>newschool.edu</i> addresses. They may not be sent to non-university addresses; they may not be sent to students in aggregate form (e.g., a list of N-numbers and grades); and they should not be associated with student names unless operationally necessary.</p> <p>Attachments must be labeled (see “Marking Requirements,” above). If the message text sent with the attachments is CONFIDENTIAL, it must be sent as an attachment, not in the message body.</p> <p>CONFIDENTIAL information must never be <i>requested</i> via electronic mail by the university; such information must be collected using a</p>

	Restricted	Confidential
		<p>secure web site.</p> <p>Unsolicited CONFIDENTIAL information received via electronic mail must be deleted immediately from mail servers.</p>
Internet File Transfer	<p>Use of a secure channel (VPN, SSL) or the New School Secure File Transfer service is recommended, but not required.</p> <p>Access to the file transfer site must be limited to authorized users; information may not be left on “public” or “anonymous” FTP sites.</p>	<p>Use of a secure channel (VPN, SSL), or the New School Secure File Transfer service is required when feasible.</p> <p>If the above cannot be used, the information must be encrypted, using university-approved encryption methods, before sending.</p> <p>Access to the file transfer site must be limited to authorized users; information may not be left on “public” or “anonymous” FTP sites.</p> <p>Information must not be stored in unencrypted form at the receiving site until it has been moved to the internal network.</p>
Portable Computers	<p>Portable computers must require a valid user name and password to access their contents.</p> <p>Portable computers must not be left unattended, must be secured with a locking cable when in use, and must be stored in a secure area when not in use.</p>	<p>Portable computer hard drives must be encrypted (full-disk encryption).</p> <p>Portable computers must require a valid user name and password to access their contents.</p> <p>Portable computers must not be left unattended, must be secured with a locking cable when in use, and must be stored in a secure area when not in use.</p>
Smart Phones, Blackberries, etc.	<p>Access to the device must be password- or PIN-protected (password preferred).</p> <p>Information must be deleted from the device when no longer needed.</p>	<p>Device storage must be encrypted.</p> <p>Access to the device must be password- or PIN-protected (password preferred).</p> <p>Information must be deleted from the device when no longer needed.</p>

	Restricted	Confidential
Removable Storage Media (USB flash drives, CDs, DVDs, etc.)	<p>Must not be copied or transferred electronically to non-university USB flash drives, memory cards, etc.</p> <p>Media must be marked “RESTRICTED.”</p> <p>Media must be stored in a manner to prevent casual access when not in use.</p>	<p>Must not be copied or transferred electronically to non-university USB flash drives, memory cards, etc.</p> <p>Must be encrypted, using university-approved encryption methods, on media that will be sent/taken off university premises.</p> <p>Media must be marked “CONFIDENTIAL.”</p> <p>Media must be stored in locked desk or file cabinet drawers or other secure containers, or in secure file or storage rooms when not in use.</p> <p>Key/combination access limited to authorized individuals.</p>
2.4 Handling Spoken Communications		
Conversation (including telephone)	<p>Take due care to minimize the risk of being overheard, especially in public areas or on conference calls.</p>	<p>Must not be discussed when third parties are present, unless a non-disclosure agreement is in place.</p> <p>Take due care to minimize the risk of being overheard, especially in public areas or on conference calls.</p>
Voice Mail	<p>Information must not be left on non-university voice mail systems.</p>	<p>Information must not be left on voice mail systems.</p>
2.5 Disposing of Sensitive Information		
Paper Documents	<p>Documents must be disposed of by placing them in secure, locked recycling bins designed for sensitive information or shredding them in a cross-cut shredder.</p> <p>Documents must not be placed in normal office trash cans or non-secure waste paper / recycling bins.</p>	<p>Documents must be disposed of by placing them in secure, locked recycling bins designed for sensitive information or shredding them in a cross-cut shredder.</p> <p>Documents must not be placed in normal office trash cans or non-secure waste paper / recycling bins.</p>

	Restricted	Confidential
Electronic Information	<p>Magnetic hard drives and USB flash drives must be wiped using an approved secure wiping program before being re-deployed or sent off-site for maintenance or repair. Magnetic hard drives and USB flash drives must be securely wiped or degaussed using an approved degaussing tool prior to being discarded or disposed.</p> <p>CDs and DVDs must be disposed of by shredding, chipping, or manually breaking the disc into multiple pieces.</p> <p>Magnetic tape and diskettes (“floppies”) must be disposed of by degaussing, incineration, or shredding.</p>	<p>Magnetic hard drives and USB flash drives must be wiped using an approved secure wiping program before being re-deployed or sent off-site for maintenance or repair. Magnetic hard drives and USB flash drives must be securely wiped or degaussed using an approved degaussing tool prior to being discarded or disposed.</p> <p>CDs and DVDs must be disposed of by shredding, chipping, or manually breaking the disc into multiple pieces.</p> <p>Magnetic tape and diskettes (“floppies”) must be disposed of by degaussing, incineration, or shredding.</p>

3 DOCUMENT ADMINISTRATION

3.1 Document Owner

This document is owned by the Information Security Office, which is responsible for its content and maintenance.

3.2 Document Review

This document is subject to review on an annual (or more frequent, if necessary) basis to validate that its content remains relevant and up-to-date.

3.3 Change history

Version	Description	Author	Date
1.0	Initial publication	D. Curry	18 Jan 2012

3.4 Approval History

Version	Name	Title	Date
1.0	Information Security Steering Committee Marla Appelbaum Jacob Campbell Alex Carnes Tara Creagh David Curry Robert Lutomski Robin Lynn Paula Maas Natalie Pressey Donna Puchalski Shelley Reed Elizabeth Ross Paul Shosho Keila Tennent	Sr. Director, Design & Construction Asst. Director, Advancement Information Services Asst. University Registrar Sr. Benefits Specialist, Human Resources Director, Information Security Director, Student Housing Assoc. Director, Online Media Assoc. Provost, Institutional Research & Effectiveness Asst. Vice President & Comptroller AVP, Payroll & Tax Compliance Sr. Vice President, Information Technology Vice Provost Director, Financial Systems & Analysis Assoc. General Counsel	18 Jan 2012