



# THE NEW SCHOOL

## Information Security Policy

Revision 1.0  
November 18, 2011





**TABLE OF CONTENTS**

**1 INTRODUCTION ..... 1**

1.1 Objective ..... 1

1.2 Scope..... 2

1.3 Compliance, Monitoring, and Enforcement ..... 2

    1.3.1 Monitoring ..... 2

    1.3.2 Enforcement..... 3

1.4 Exceptions..... 3

**2 PRINCIPLES OF INFORMATION SECURITY..... 5**

**3 ROLES AND RESPONSIBILITIES ..... 9**

3.1 Information Trustees ..... 9

3.2 Information Owners ..... 10

3.3 Information Custodians ..... 10

3.4 Information Users..... 11

3.5 Office of Information Technology..... 11

3.6 Business Partners and Vendors..... 12

3.7 Information Security Steering Committee..... 12

3.8 Information Security Office ..... 12

**4 INFORMATION CLASSIFICATION..... 15**

4.1 Classification Levels..... 15

    4.1.1 Unrestricted Information ..... 15

        4.1.1.1 Security considerations ..... 15

        4.1.1.2 Examples ..... 15

    4.1.2 Restricted Information..... 16

        4.1.2.1 Security considerations ..... 16

        4.1.2.2 Examples ..... 16

    4.1.3 Confidential Information..... 16

        4.1.3.1 Security considerations ..... 16

        4.1.3.2 Examples ..... 17

4.2 Assigning Classification Levels ..... 17

4.3 Handling Classified Information ..... 17

4.4 Non-Disclosure Agreements and Confidentiality Terms..... 18

<b>5</b>	<b>ORGANIZATION OF THE INFORMATION SECURITY POLICY .....</b>	<b>19</b>
5.1	Policies .....	19
5.2	Standards .....	19
5.3	Procedures.....	20
<b>6</b>	<b>MAPPING TO ISO 27002:2005 .....</b>	<b>21</b>
<b>7</b>	<b>DOCUMENT ADMINISTRATION.....</b>	<b>23</b>
7.1	Document Owner .....	23
7.2	Document Review .....	23
7.3	Change history.....	23
7.4	Approval History.....	23

# 1 INTRODUCTION

Information, and the supporting processes, systems, and networks used to process, store, retrieve, and transmit that information, play a vital role in the conduct and success of The New School's academic, research, and public service mission. As more information is used and shared by students, faculty, and staff, both within and outside the university, a concerted effort must be made to protect that information. Confidentiality, integrity, and availability of information are essential to maintaining the university's reputation, legal position, and ability to conduct its operations.

The senior leadership of the university is committed to:

- achieving high standards of university information security governance;
- treating information security as a critical business issue and creating a security-conscious environment;
- demonstrating to third parties that the university deals with information security in a proactive manner; and
- applying fundamental principles such as assuming ultimate responsibility for information security, implementing controls that are proportionate to risk, and achieving individual accountability.

This document defines the fundamental principles of the New School information security program, establishes categories of information and their protection requirements, and assigns roles and responsibilities for implementing and complying with those requirements.

*The New School Information Security Policy* (the "Policy") comprises this document and additional policies, standards, and procedures. Section 5, *Organization of the Information Security Policy*, describes each of these components in more detail.

## 1.1 Objective

The information that The New School uses to conduct its operations—whether owned or created by the university, received from business partners and vendors, entrusted to us by our students, or maintained by us about our employees—is a valuable asset that must be protected at all times.

Information security is defined as the protection (or preservation) of:

- *Confidentiality*—ensuring that information is accessible only to those persons authorized to have access
- *Integrity*—safeguarding the accuracy and completeness of information and information processing methods
- *Availability*—ensuring that authorized users have access to information and information systems in a timely manner, when they are needed

Information can exist in many forms. It can be written or printed on paper, stored electronically or optically, transmitted by courier or using electronic means, recorded on magnetic disk or tape, or spoken in conversation. Whatever form information takes, or means by which it is shared or stored, the objective of this Policy is to ensure that it is always properly safeguarded.

## 1.2 Scope

Maintaining the security of information, whether it belongs to the university, its business partners, its students, or its employees, is a primary business objective that requires the attention of all faculty, staff, and students.

This Policy applies to:

- all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers, and other members of the university community, including those affiliated with third parties, who access or in any way make use of university information or information systems;
- all university information resources, including those used by the university under license or contract. “Information resources” include information in any form and recorded on any media, and all computer hardware, computer software, and communications networks owned or operated by the university or on the university’s behalf; and
- any device, regardless of ownership and including equipment privately owned by faculty, staff, and students (e.g., laptop computers, tablet computers, smart phones, MP3 players, USB storage devices, etc.), but only with respect to the ways in which they connect to or access university information resources and the activities they perform with those resources.

The intent of this Policy is to protect against intentional and unintentional acts that could compromise the confidentiality, integrity, or availability of the university’s information resources, or interfere with access control mechanisms. It is intended to address both internal and external threats.

## 1.3 Compliance, Monitoring, and Enforcement

Compliance with this Policy is mandatory for all students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers, and other members of the university community, including those affiliated with third parties, who access or in any way make use of university information or information systems.

### 1.3.1 Monitoring

The university considers the data processed by and stored on administrative computer systems to be the property of the university. The contents of user accounts are considered to be the property of the authorized user, subject to applicable university copyright and intellectual property policies and applicable federal and state laws.

Individuals should be aware that their use of university information resources, including accessing the Internet or using electronic mail, social media, instant messaging, telephone, or voice mail, are not completely private. While the university does not routinely monitor individual usage of its information resources, the normal operation and maintenance of these resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the provision of service. The university may also specifically monitor the activity and accounts of individual users of university information resources, including individual login sessions, the content of individual communications, and the contents of stored information, with or without notice, when:

- the individual has voluntarily made the information accessible to the public, as by posting to a blog or a Web page;

- it reasonably appears necessary to do so to protect the integrity, security, or functionality of university information resources or to protect the university from liability;
- a written complaint has been received, or there is reasonable cause to believe, that the individual has violated or is violating this Policy;
- an account appears to be engaged in unusual or unusually excessive activity; or
- it is otherwise required or permitted by law.

Any such monitoring of communications or stored information, other than what is made accessible by the individual, required by law, or necessary to respond to perceived emergency situations, must be authorized in advance by the Provost and Chief Academic Officer, the Senior Vice President for Human Resources and Labor Relations, the Senior Vice President for Student Services, or the Senior Vice President for Information Technology, as appropriate, in consultation with the Office of the General Counsel. The university, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of individual communications or stored information, to appropriate university personnel or law enforcement agencies and may use those results in appropriate university disciplinary proceedings.

### **1.3.2 Enforcement**

Failure to comply with this Policy, whether deliberate or due to careless disregard, will be treated as serious misconduct and may result in actions including (but not limited to) disciplinary action, dismissal, and civil and/or criminal proceedings.

In the case of a written complaint of serious misuse, or evidence indicating that malicious software may be present in certain material on the system, the university reserves the right to temporarily remove material from the system for its review. In some situations, it may also be necessary to restrict or suspend access or account privileges to prevent ongoing misuse while the situation is under investigation.

Alleged infractions of this policy are handled via formal procedures and investigation by the Office of the Provost, Department of Human Resources, or Office of Student Services, as appropriate. Upon determination of misuse, individuals who are found to be in violation of this Policy may be subject to the following:

- restriction or suspension of computer access privileges;
- disciplinary action by their academic division and/or the university up to and including termination;
- referral to law enforcement authorities for criminal prosecution; and
- other legal action, including action to recover civil damages and penalties.

## **1.4 Exceptions**

Any department or unit of the university that cannot comply with any portion of this Policy must submit a written exception request to the Director of Information Security for review and disposition. Depending on the level of risk posed by granting the exception, the request may be referred to the Information Security Steering Committee for resolution.

Exception requests must include the scope and duration of the exception, the business reason for the exception, and a committed remediation plan and time frame to achieve compliance. Exception

requests must be reviewed and signed off by the Information Owner or Information Trustee of each information resource affected by the exception before they are submitted.

Exceptions will be granted on a time-limited basis, and must be managed according to the university's established information risk management process.

Detailed requirements, steps, and forms for making and tracking exception requests are described in the information security ***Procedure for Policy Exception Requests.***

## 2 PRINCIPLES OF INFORMATION SECURITY

The New School information security program is built on a foundation of 21 principles that reflect the information security goals and intent of the university's senior leadership and underpin the development of the policies, standards, and procedures that constitute the Policy. The principles provide a basis for:

- safeguarding critical and sensitive university information in all formats, such as databases, electronic mail, and paper documents;
- protecting critical university business applications, both those under development and those in live production environments;
- securing all types of computing devices, ranging from server farms and storage systems, through desktop and laptop computers and hand-held computing devices such as tablets and smart phones, to portable storage devices;
- protecting university communications networks, including wireless, Voice over IP (VoIP), and Internet connectivity; and
- facilitating discussions with third parties when establishing contracts or service level agreements governing information security arrangements.

The principles also facilitate mapping the Policy to security-related standards such as *ISO/IEC 27002:2005 Code of practice for information security management* (see Section 6).

Governance and Compliance		
1 Information Security Governance	Principle	Establish, maintain, and monitor an information security governance framework
	Purpose	To provide assurance that required security management activities are performed consistently and correctly by designated individuals
2 Information Security Policy	Principle	Develop and distribute a comprehensive, approved information security policy to all individuals with access to the New School's information resources
	Purpose	To communicate the university leadership's direction on and commitment to information security, provide guidance for undertaking security activities, and set expectations for individual behavior
3 Accountability and Ownership	Principle	Assign ownership and responsibility for particular information resources to designated individuals who have the skills, tools, and authority to secure them
	Purpose	To ensure that individuals are accountable for protecting designated information resources
4 Security Education and Awareness	Principle	Establish an information security awareness program, supported by a range of education and training activities
	Purpose	To create a security-positive environment and provide individuals with the knowledge and skills required to use security controls effectively
5 Legal and Regulatory Compliance	Principle	Apply an approved method for identifying, maintaining, and protecting regulated information
	Purpose	To ensure that information is used in compliance with legal and regulatory requirements for information security and privacy

<b>Risk Management</b>		
<b>6</b> Information Risk Management	Principle	Undertake an information risk analysis of each critical system, on a regular basis, in a rigorous and consistent manner, using a structured methodology
	Purpose	To enable individuals who are responsible for critical information systems to identify the potential business impact and likelihood of potential threats materializing, and determine the controls required to keep risk within acceptable limits
<b>7</b> Asset Management	Principle	Acquire hardware and software from approved vendors, ensure that it meets security requirements before purchase, and record it in an inventory
	Purpose	To maximize the availability of information systems, help ensure the confidentiality and integrity of information, and meet licensing requirements
<b>8</b> Third Party Management	Principle	Restrict access to university information resources to third parties who have been authorized and are subject to security requirements that have been documented in an approved agreement
	Purpose	To prevent unauthorized third party access and ensure that required security controls are implemented by authorized third parties
<b>Infrastructure</b>		
<b>9</b> Physical and Environmental Security	Principle	Protect IT facilities and services against malicious attack, accidental damage, natural hazards, and unauthorized physical access
	Purpose	To ensure that important IT facilities and services are available when required and prevent unauthorized disclosure of information
<b>10</b> System Configuration	Principle	Configure systems and networks in a consistent, accurate manner and apply approved security settings
	Purpose	To ensure that systems and networks function as intended, are available when required, and do not reveal unnecessary configuration details
<b>11</b> System Monitoring	Principle	Perform continuous monitoring of designated systems and networks, employ intrusion detection and/or prevention systems, and record security events
	Purpose	To highlight system and network errors, detect potential and actual attacks, and support investigations
<b>12</b> Network Security	Principle	Design and operate robust, resilient networks that can cope with current and predicted levels of traffic, are supported by alternative facilities, incorporate firewalls, and restrict network access to authorized individuals
	Purpose	To protect network traffic against interception or interference, ensure that networks function as intended, and are available as required
<b>13</b> Electronic Communication	Principle	Protect electronic communications systems (e.g., electronic mail, instant messaging, social media, and VoIP) by setting policy for their use, configuring security settings, performing capacity planning, and hardening the supporting infrastructure
	Purpose	To preserve the integrity of important business messages, prevent unauthorized disclosure of sensitive information, and maximize availability
<b>14</b> Business Continuity and Disaster Recovery	Principle	Develop business continuity and disaster recovery plans that are supported by alternative processing facilities and tested regularly using simulations of the live environment
	Purpose	To ensure that the university can continue to operate effectively in the event of prolonged unavailability of primary services or facilities
<b>Applications</b>		
<b>15</b> Application Security	Principle	Validate information entered into, processed by, and output from business applications and verify that it has not been subject to unauthorized change
	Purpose	To ensure the accuracy and completeness of information stored or processed by business applications

<b>16</b> <b>System Development</b>	<b>Principle</b>	Develop systems using a structured and approved system development methodology that ensures that information security requirements are defined, documented, and met
	<b>Purpose</b>	To build required information security functionality into systems during development
<b>17</b> <b>Change Management</b>	<b>Principle</b>	Implement a comprehensive and approved change management process for information and systems that includes testing and accepting authorized changes and evaluating security implications
	<b>Purpose</b>	To ensure that changes are authorized, applied correctly, and do not compromise information security
<b>Security Services</b>		
<b>18</b> <b>Identity and Access Management</b>	<b>Principle</b>	Implement a consistent identity and access management approach that provides effective user administration, identification, authentication, and authorization mechanisms
	<b>Purpose</b>	To effectively administer users, restrict access to information resources to authorized individuals, and provide them with approved levels of access
<b>19</b> <b>Malware Protection</b>	<b>Principle</b>	Deploy comprehensive, up-to-date malware protection software, supported by a user awareness campaign and a procedure for handling malware infections
	<b>Purpose</b>	To protect against all types of malware attacks, respond to infections within defined timescales, and minimize their business impact
<b>20</b> <b>Cryptography</b>	<b>Principle</b>	Apply approved, documented cryptographic solutions, supported by effective cryptographic key management
	<b>Purpose</b>	To confirm the identity of the originator of information, preserve the integrity of important information, and prevent unauthorized disclosure of sensitive information
<b>21</b> <b>Incident Management</b>	<b>Principle</b>	Implement a comprehensive and approved incident management process for information resources that includes identification, response, recovery, and post-incident review of information security and privacy incidents
	<b>Purpose</b>	To resolve information security and privacy incidents in a consistent and effective manner, minimize their business impact, and reduce the risk of similar incidents occurring

The security requirements for individual information resources are determined by a methodical assessment of risk—not all information resources require the same level of security or protection mechanisms. The controls specified by the policies, standards, and procedures that constitute the Policy have been formulated with the intent that application of security measures should be commensurate with the sensitivity and value of the information resources to be protected, and the actual threats to those resources.



### 3 ROLES AND RESPONSIBILITIES

Implementation of this Policy requires a clear definition of security roles and responsibilities for all individuals with access to university information resources. All members of the university community share in the responsibility to protect information resources to which they have access; this Policy also intends that individuals are accountable for their access to and use of information resources.

The following roles are defined and used throughout the policies, standards, and procedures that constitute the Policy. The same individual may hold more than one of these roles simultaneously.

#### 3.1 Information Trustees

Information Trustees are the senior executive officers of the university and the Deans and Directors of the individual academic faculties:

- President
- Provost and Chief Academic Officer
- Deputy Provost and Senior Vice President for Academic Affairs
- Senior Vice President for Finance and Business
- Senior Vice President for Distributed and Global Learning
- Senior Vice President for Human Resources and Labor Relations
- Senior Vice President for Information Technology
- Senior Vice President for Student Services
- Vice President and Treasurer
- Vice President for Communications and External Affairs
- Vice President for Design, Construction, and Facilities Management
- Vice President for Development and Alumni Relations
- Vice President for Enrollment Management
- General Counsel and Vice President for Legal Affairs
- Executive Dean – The New School for Public Engagement
- Executive Dean – Parsons The New School for Design
- Dean – Eugene Lang College The New School for Liberal Arts
- Dean – Mannes College The New School for Music
- Dean – The New School for Social Research
- Executive Director – The New School for Jazz and Contemporary Music
- Director – The New School for Drama

Information Trustees are accountable to ensure the exercise of due diligence in protecting all university information resources that fall within their respective offices or departments by:

- maintaining an appreciation of the risks associated with the loss of confidentiality, integrity, or availability of business information resources used in the office or department;
- determining, in coordination with responsible staff functions (e.g., General Counsel, Information Security, etc.) and through participation in risk assessment activities, the proper levels of protection for office or department business information resources and/or

information resources under office/department control and ensuring that necessary safeguards are implemented;

- ensuring that every information resource used by the office or department is assigned an Information Owner (see below);
- taking the lead in promoting information security awareness in the office or department and ensuring that all personnel participate in relevant security and privacy training;
- ensuring office or department personnel know what is expected of them and that they act in a reasonable manner to protect university information resources;
- making reasonable efforts to ensure that all personal and business information maintained by the office or department is accurate, timely, relevant, and complete;
- ensuring that end users' access to information resources is in accordance with their job function, and that such access is current, regularly reviewed, and administered securely; and
- ensuring that the information security policies, standards, and procedures that constitute this Policy are communicated to and followed by office or department personnel.

### 3.2 Information Owners

Information Owners are those personnel who have primary responsibility for business processes through which information is received, created, stored, handled, or discarded, whether in physical or electronic form. When information crosses multiple business processes, each business process owner is deemed an Information Owner under this Policy. Information Owners are responsible for:

- assigning information classification categories (see Section 4, *Information Classification*);
- maintaining records of classified information resources, their locations, and who has access to them;
- specifying the level of protection that should be applied to information resources;
- verifying that specified levels of protection have been implemented;
- reviewing and authorizing user access to information resources based on business need;
- reviewing and authorizing privileged user access to information systems;
- controlling changes to information;
- defining recovery time objectives and recovery point objectives for information resources and ensuring that backup and recovery processes can meet those objectives;
- ensuring compliance with applicable record retention policies and schedules;
- ensuring that information resources that are no longer needed are disposed of securely; and
- ensuring that essential business functions and applications are recoverable in the event the existing environment is unavailable.

The term "Owner" as used here does not imply ownership in any legal sense.

### 3.3 Information Custodians

Information custodians are those personnel who have primary operational responsibility for physical and electronic systems that receive, create, store, handle, or discard information. When information

crosses multiple systems, each system manager is deemed an Information Custodian under this Policy. Information Custodians are responsible for:

- implementing and applying the information protection levels specified by the Information Owner by using the information security controls specified by the policies, standards, and procedures that constitute this Policy;
- providing documentation to the Information Owner demonstrating that the specified levels of protection have been implemented;
- granting and revoking user rights to information and privileged user access to information systems as specified by the Information Owner;
- providing documentation to the Information Owner showing who has access to information and systems, and the level of access that they have; and
- implementing appropriate arrangements to recover information, applications, and systems in the manner and timeframes specified by the Information Owner.

### 3.4 Information Users

Information Users are individuals who have been granted access to specific information resources in the performance of their assigned duties. All members of the university community are Information Users of some part of the New School's information resources, even if they do not have responsibility for managing those resources. Information Users include students, faculty, staff, contractors, consultants, temporary employees, guests, volunteers, and other affiliates of The New School. Information Users have a responsibility to:

- review, understand, and comply with the policies, standards, and procedures that comprise this Policy, including the *Information Resource Acceptable Use Policy*;
- agree, in writing, on an annual basis, to perform their work according to such policies, standards, and procedures;
- comply with software licenses and with other legal and regulatory obligations that apply to them including, but not limited to, the Family Educational Rights and Privacy Act (FERPA) and United States copyright law;
- participate in security awareness, training, and education sessions as appropriate to their job functions and as directed by their supervisors and/or management;
- notify the University Help Desk or the Information Security Office of any known or suspected information security incident or issue; and
- conduct themselves in a manner consistent with this Policy.

These responsibilities cover both computerized and non-computerized information and information technology devices (paper, computers, smart phones, external memory devices, printers, fax machines, etc.) that are in the Users' care or possession.

### 3.5 Office of Information Technology

The Office of Information Technology is responsible for:

- ensuring that information technology architecture components are designed and implemented to protect the information they process in accordance with the policies, standards, and procedures that constitute this Policy;
- defining, implementing, and testing disaster recovery plans and making contingency arrangements to manage the prolonged unavailability of critical computer facilities, equipment, or communications services;
- maintaining an accurate and up-to-date inventory of information system hardware and software in use; and
- ensuring that all implementations, maintenance, enhancements, and other project activities within its purview are conducted in accordance with the policies, standards, and procedures that constitute this Policy.

### **3.6 Business Partners and Vendors**

Business partners and vendors must:

- comply with the information security and data protection requirements of the contracts, service agreements, and non-disclosure agreements that govern their relationship with the university;
- exercise due care and caution when accessing university information and information systems; and
- ensure that the confidentiality and integrity of university data is adequately safeguarded.

### **3.7 Information Security Steering Committee**

The Information Security Steering Committee represents the senior leadership of the major administrative and operational areas of the university. Members of the Committee are responsible for championing, within their respective offices or departments, the ideas that information security activities should be carried out in a timely and accurate manner and that security issues are resolved effectively. This includes:

- facilitating the adoption and implementation of prescribed information security methodologies and processes within the office or department, and ensuring compliance with university information security policies and standards;
- monitoring and reporting on the state of information security, privacy, and statutory/regulatory compliance within the office or department, both generally and with regard to specific issues that have been previously identified; and
- identifying the need for development of new or changes to existing policies, standards, methodologies, and processes to address new information security and privacy issues as they arise.

### **3.8 Information Security Office**

The New School Information Security Office is responsible for developing The New School's university-wide information security vision, strategy, and program. The Information Security Office is responsible for:

- performing independent oversight and governance functions for information assurance and protection, information risk management, security incident investigations, business continuity, and disaster recovery across the entire university;
- working in cooperation with the Office of the General Counsel to interpret laws and regulations governing information security and privacy and provide appropriate compliance oversight;
- producing and maintaining university-wide information security policies and standards that specify required and recommended information security measures and controls;
- developing methodologies and processes to help The New School offices and departments comply with information security policies and standards in a consistent and effective manner;
- providing expertise and knowledge of current higher education trends in information security and business continuity to ensure parity with peer organizations and improve control processes across the university; and
- responding to, investigating, and reporting on information security incidents.

The Information Security Office is led by the Director of Information Security.



## 4 INFORMATION CLASSIFICATION

Information resources are some of the most valuable assets The New School owns, and, as is the case with all valuable assets, they need to be protected accordingly. The meaning of “accordingly” is mostly driven by legal, academic, financial, and operational requirements and is based on the criticality and risk level of the information. To help protect information resources appropriately while supporting the academic, research, and public service mission of the university, each information resource produced or handled by The New School is assigned one of three classifications based on the level of protection required for that resource.

### 4.1 Classification Levels

In increasing order of protection level, the classifications used by The New School are Unrestricted, Restricted, and Confidential.

#### 4.1.1 Unrestricted Information

Unrestricted information is information that can be disclosed to any person inside or outside the university. Although security controls are not needed to prevent disclosure and dissemination of this information, they are still necessary to protect against unauthorized modification, destruction, or loss of the information.

##### 4.1.1.1 Security considerations

- Integrity
- Availability

##### 4.1.1.2 Examples

- Student information designated as public or directory information by The New School under the Family Educational Rights and Privacy Act (FERPA):
  - Student name
  - Major field of study
  - Dates of attendance
  - Full- or part-time enrollment status
  - Year level
  - Degrees and awards, including dean’s list
  - Addresses
  - Telephone numbers
  - Photographs
  - E-mail addresses
  - Date and place of birth
  - Most recent previous educational agency or institution attended
- Faculty and staff directory information and any general biographical information already published by the faculty or staff member:
  - Employee name
  - Job/position title
  - Office mailing address
  - Office telephone number
  - Office e-mail address
  - Curriculum vitae
- General information about The New School:
  - Campus maps
  - Course catalogs and schedules
  - Campus brochures
  - Student policies and handbooks
  - School calendars
  - Donor names, amounts, designations

- Publications, blog entries, and message board postings
- Any item The New School has published in the past

#### **4.1.2 Restricted Information**

Restricted information is information that is generally not public, and whose disclosure, loss, or corruption may cause embarrassment or damage (financial or otherwise) to The New School. This information requires protection against unauthorized access and disclosure, modification, destruction, and use. However, the sensitivity of this information is less than that of Confidential information.

##### **4.1.2.1 Security considerations**

- Confidentiality
- Integrity
- Availability
- Access Control

##### **4.1.2.2 Examples**

- Employee N-number
- Employee place of birth
- Employee home address
- Employee evaluations
- Employee resumes
- Individual employee salary data
- Individual employee benefit data
- Gender
- Individual student tuition payment information
- Internal correspondence and minutes from committee meetings that do not include Confidential information
- Class rosters
- Student grades
- Student resumes
- Student academic records
- Library transactions
- Vendor contracts
- Invoices and internal billing
- Detailed annual budget information
- Financial transactions that do not include Confidential data
- Internal operating procedures of the university that do not include Confidential information

#### **4.1.3 Confidential Information**

Confidential information is 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. This information requires a high level of protection against unauthorized access and disclosure, modification, destruction, and use.

##### **4.1.3.1 Security considerations**

- Confidentiality
- Integrity
- Availability

- Access Control
- Non-repudiation

#### 4.1.3.2 Examples

- Student N-number
- Social Security number
- Driver's license number
- Other government-issued ID number
- SEVIS number
- Immigration status
- Disability or veteran status
- Protected Health Information (HIPAA)
- Ethnic, religious, racial, or national affiliation
- Human Resources information on individual applicants
- Donor information (except name, amount, designation)
- All anonymous donor information
- Employee date of birth
- Employee payroll information
- Employee disciplinary information
- Bank account numbers
- Credit/debit card numbers
- Wire transfer information
- Payment history information
- Individual taxation records
- Individual student counseling information
- Individual student disciplinary information
- Federal individual financial aid / grant information
- Privileged data in the Office of the General Counsel
- Information security data, including passwords and sensitive information related to the university's information technology infrastructure and operations
- Directory information for students who have opted-out of public disclosure

## 4.2 Assigning Classification Levels

Information Owners are responsible for assigning the appropriate classification to each information resource for which they are responsible, and ensuring that the resource is protected in accordance with that classification.

Many information resources will not be explicitly classified, particularly if they are not in the form of a printed or electronic document. Information that is not explicitly classified is classified implicitly as follows: Any information that contains confidential elements as defined above is classified as Confidential. Other information is classified as Restricted unless it is published (made publicly available in any medium) by the Information Owner, in which case it is classified as Unrestricted.

## 4.3 Handling Classified Information

The classification level determines the information security controls that must be applied to protect an information resource, and the procedures that must be followed when acquiring, storing, using, transmitting, archiving, and destroying that resource.

The information security standard document entitled *General Controls for Handling Sensitive Information* describes the techniques and tools that should be used when:

- Providing (restricting) access to information

- Labeling information
- Storing electronic information
- Storing printed information
- Printing information
- Transmitting information
- Using classified information
- Archiving information (record retention)
- Disposing of (destroying) information

#### **4.4 Non-Disclosure Agreements and Confidentiality Terms**

Before Restricted or Confidential information may be disclosed to individuals or organizations outside The New School, including business partners, suppliers, and vendors, the Office of the General Counsel must be consulted to ensure that appropriate non-disclosure agreements or confidentiality contract terms are in place.

## 5 ORGANIZATION OF THE INFORMATION SECURITY POLICY

*The New School Information Security Policy* (the “Policy”) is organized as a collection of separate documents, including this one, to provide an extensible framework that can be updated easily. The document set includes detail appropriate for various audiences, and allows document ownership and approval to match authority and knowledge. The Policy comprises three types of documents:

- Policies
- Standards
- Procedures

References to “The New School Information Security Policy” are inclusive of all the policies, standards, and procedures published by the Information Security Office.

### 5.1 Policies

*Policies* specify the information security intentions of the university’s senior leadership, grant authority, define roles and responsibilities, and establish high-level requirements for protecting the university’s information resources.

Policies are strategic in nature, specifying the desired security state of the university, but not how to achieve it. There are three major types of policies contained in the Policy:

- *Regulatory policies* discuss the laws and regulations with which The New School must comply, and outline the procedures that must be followed to ensure compliance. This policy type may also be used to establish “pseudo-regulatory” requirements, such as the implementation of “best practices.”
- *Advisory policies* discuss acceptable and unacceptable behaviors and activities and define consequences of violations. They communicate the senior leadership’s desires for security and compliance throughout the university.
- *Informative policies* provide support, research, or background information relevant to specific elements of the overall Policy. They discuss such things as goals, mission statements, or how The New School interacts with business partners and the community. Informative policies are generally not enforceable.

The policies contained in the Policy represent baseline, or minimum, requirements that must be met by all offices and departments of the university. As appropriate and necessary, additional policies may be established at the office or department level to codify office-specific or department-specific requirements. These additional policies may supplement, but never reduce, the level of security required by the Policy.

### 5.2 Standards

*Standards* define the mandatory settings, controls, and requirements that must be implemented to achieve policy objectives. Compliance with standards is measurable, allowing risks to be identified, quantified, and managed at various organizational levels within the university.

There are two types of standards in the Policy:

- *General control standards* describe the tasks that must be accomplished and controls that must be put in place to comply with information security policies. They apply broadly to all software and hardware implementations, and are therefore written in platform-neutral, or generic, language. General control standards are derived from a combination of university policies, the laws and regulations that apply to the university, and generally-accepted information security practices in the higher education sector.
- *Technical control standards* describe the specific steps (procedures, configuration settings, etc.) that should be used to implement the tasks and controls specified by one or more general control standards with a particular software or hardware product(s). Technical control standards are usually derived from general control standards; they are rarely derived directly from policy.

The standards contained in the Policy represent baseline, or minimum, requirements that must be met by all offices and departments of the university. As appropriate and necessary, additional standards may be established at the office or department level to codify office-specific or department-specific requirements. These additional standards may supplement, but never reduce, the level of security required by the Policy.

### **5.3 Procedures**

*Procedures* help to ensure that security policies and standards are applied in a consistent and repeatable manner. A procedure is a systematic set of interrelated steps, tasks, or activities to be accomplished in order to implement a policy or standard.

The procedures contained in the Policy will be enacted at the university-wide level and apply to all offices and departments of the university. As appropriate and necessary, additional procedures may be established at the office or department level to codify office-specific or department-specific requirements. These additional procedures may supplement, but never reduce, the level of security required by the Policy.

## 6 MAPPING TO ISO 27002:2005

The table in this section shows the relationship between the *New School Information Security Policy* guiding principles (see Section 2) and the *ISO/IEC 27002:2005 Code of practice for information security management*.

Information Security Principle	ISO 27002:2005											
	4. Risk Assessment and Treatment	5. Security Policy	6. Organization of Information Security	7. Asset Management	8. Human Resources Security	9. Physical and Environmental Security	10. Communications and Operations Management	11. Access Control	12. Information Systems Acquisition, Development and Maintenance	13. Information Security Incident Management	14. Business Continuity Management	15. Compliance
<b>Governance and Compliance</b>												
1. Information Security Governance			✓									✓
2. Information Security Policy		✓			✓							
3. Accountability / Ownership			✓	✓	✓		✓					
4. Security Education / Awareness					✓		✓					
5. Legal & Regulatory Compliance					✓							✓
<b>Risk Management</b>												
6. Information Risk Management	✓											
7. Asset Management				✓	✓	✓	✓		✓			
8. Third Party Management			✓				✓		✓			✓
<b>Infrastructure</b>												
9. Physical & Environmental Security						✓		✓				
10. System Configuration						✓	✓	✓	✓			
11. System Monitoring							✓	✓				
12. Network Security				✓			✓	✓				
13. Electronic Communication				✓			✓		✓			
14. Business Continuity & Disaster Recovery						✓					✓	
<b>Applications</b>												
15. Application Security						✓	✓	✓	✓			✓
16. System Development							✓		✓			✓

Information Security Principle	ISO 27002:2005												
	4. Risk Assessment and Treatment	5. Security Policy	6. Organization of Information Security	7. Asset Management	8. Human Resources Security	9. Physical and Environmental Security	10. Communications and Operations Management	11. Access Control	12. Information Systems Acquisition, Development and Maintenance	13. Information Security Incident Management	14. Business Continuity Management	15. Compliance	
17. Change Management			✓				✓	✓	✓	✓			
<b>Security Services</b>													
18. Identity & Access Management					✓			✓				✓	
19. Malware Protection							✓						
20. Cryptography									✓			✓	
21. Incident Management							✓			✓			

## 7 DOCUMENT ADMINISTRATION

### 7.1 Document Owner

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

### 7.2 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. Significant or material changes to this document must be reviewed and approved by the Information Security Steering Committee as described in Section 3, *Roles and Responsibilities*.

### 7.3 Change history

Version	Description	Author	Date
1.0	Initial publication	D. Curry	18 Nov 2011

### 7.4 Approval History

Version	Name	Title	Date
1.0	<b>Information Security Steering Committee</b>		18 Nov 2011
	Marla Appelbaum	Sr. Director, Design & Construction	
	Jacob Campbell	Asst. Director, Advancement Information Services	
	Alex Carnes	Asst. University Registrar	
	Tara Creagh	Sr. Benefits Specialist, Human Resources	
	David Curry	Director, Information Security	
	Robert Lutomski	Director, Student Housing	
	Robin Lynn	Assoc. Director, Online Media	
	Charis Ng	Assoc. Director, Institutional Research	
	Natalie Pressey	Asst. Vice President & Comptroller	
	Donna Puchalski	AVP, Payroll & Tax Compliance	
	Shelley Reed	Sr. Vice President, Information Technology	
	Elizabeth Ross	Vice Provost	
	Paul Shosho	Director, Financial Systems & Analysis	
	Keila Tennent	Assoc. General Counsel	