Information Security Policy

Revision 2.0
Effective July 1, 2016
# Table of Contents

1 Introduction ........................................................................................................... 1

2 Delegation of Administrative Authority and Responsibility ...................... 3

3 The New School Information Security Program ........................................... 5
   3.1 Objective ........................................................................................................ 5
   3.2 Scope ............................................................................................................ 5
   3.3 Compliance, Monitoring, and Enforcement .................................................. 5
      3.3.1 Monitoring ............................................................................................ 6
      3.3.2 Enforcement ......................................................................................... 6
   3.4 Exceptions ..................................................................................................... 7

4 Roles and Responsibilities .................................................................................. 9
   4.1 Information Trustees .................................................................................. 9
   4.2 Information Owners ................................................................................... 9
   4.3 Information Custodians ............................................................................. 10
   4.4 Information Users ..................................................................................... 10
   4.5 Information Security Advisory Committee ............................................. 11

5 Information Classification ............................................................................... 13
   5.1 Classification Levels ................................................................................ 13
      5.1.1 Unrestricted Information ..................................................................... 13
         5.1.1.1 Security considerations ................................................................. 13
         5.1.1.2 Examples .................................................................................... 13
      5.1.2 Restricted Information ....................................................................... 13
         5.1.2.1 Security considerations ................................................................. 14
         5.1.2.2 Examples .................................................................................... 14
      5.1.3 Confidential Information .................................................................. 14
         5.1.3.1 Security considerations ................................................................. 14
         5.1.3.2 Examples .................................................................................... 14
   5.2 Assigning Classification Levels ................................................................. 15
   5.3 Handling Classified Information ............................................................... 15
   5.4 Non-Disclosure Agreements and Confidentiality Terms .......................... 15

6 Document Administration ................................................................................. 17
   6.1 Document Owner ........................................................................................ 17
6.2 Document Review ........................................................................................................................................... 17
6.3 Change history ............................................................................................................................................... 17
6.4 Approval History .......................................................................................................................................... 17
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 policy establishes the New School Information Security Program, grants the authority and responsibility for operating the program, establishes categories of information and their protection requirements, and assigns roles and responsibilities for implementing and complying with those requirements.
2 Delegation of Administrative Authority and Responsibility

The following specific assignments of administrative authority and responsibility are hereby delegated to the Senior Vice President for Information Technology to assist and act for the President.

The Senior Vice President for Information Technology shall:

1. Have responsibility for:
   a. development of practical and effective university policies, standards, guidelines, procedures, and best practices for information security;
   b. development and implementation of an information security awareness program to be offered periodically to all university faculty and staff;
   c. development of a risk assessment process to be used for identifying, analyzing, and mitigating risks to university information and systems;
   d. development of a response plan for information security incidents and personal information data breaches;
   e. implementation of practical and effective technologies and services to ensure the security of university information, networks, and computing infrastructure; and
   f. establishment of an information security function (the “Information Security Office”), led by a senior staff member dedicated full-time to information security, to develop, implement, and operate the New School Information Security Program.

2. Have authority to disconnect any device or disable any account if it is believed that either is involved in compromising the security of university information or systems until such time as it is demonstrated that the device or account no longer poses a threat. Devices will not be disconnected without consultation with relevant departmental officials, unless a critical situation exists (e.g., active compromise, serious vulnerability, denial of service, worm or virus attack) and organization officials cannot be contacted quickly. The New School Technology Advisory Committee shall be notified promptly of any device(s) disconnected or account(s) disabled pursuant to this paragraph. The individual or department responsible for the device(s) or account(s) in question may appeal any such disconnection or disablement to the Technology Advisory Committee.

3. Have authority to stop application development or deployment efforts if it is found during a risk assessment that the impact of a particular threat will compromise the security of university information or systems until a remedy is implemented to reduce or eliminate the impact of that threat.

In all instances, administration and approvals shall be in accordance with existing federal and state laws and regulations and the policies of the university. Deviation from these policies will require advance written permission of the President.
3 The New School Information Security Program

The New School Information Security Program comprises

- information security policies, standards, and guidelines
- information security best practices and procedures
- information security technologies and services.

3.1 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 the Information Security Program is to ensure that it is always properly safeguarded.

3.2 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.

The requirements of the Information Security Program apply 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, 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 the Information Security Program 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.

3.3 Compliance, Monitoring, and Enforcement

Compliance with the requirements of the Information Security Program 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 resources.

3.3.1 Monitoring
The university considers the data processed by and stored on administrative computer systems (both those operated locally and those hosted by a third party) 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 privacy is not guaranteed when using university information resources, including accessing the Internet or using New School electronic mail, telephone, or voice mail. 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. In addition, the university may use automated tools to detect, alert, and respond to improper storage, sharing, or transmission of confidential or personally identifiable information that could result in such information being disclosed to unauthorized persons. 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:

- 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 the requirements of the Information Security Program;
- 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 Chief Enrollment and Success Officer, 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.

3.3.2 Enforcement
Failure to comply with the requirements of the Information Security Program, 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, Office of Human Resources, or Office of Student Success, as appropriate. Upon determination of misuse, individuals who are found to be in violation of the requirements of the Information Security Program may be subject to any or all of 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.

3.4 Exceptions
Organizations within the university that cannot comply with the requirements of the Information Security Program must submit a written exception request to the Information Security Office for review and disposition. Depending on the level of risk posed by granting the exception, the request may be referred to relevant members of the senior leadership team 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 Procedure for Information Security Program Exception Requests.
# 4 Roles and Responsibilities

All members of the university community share in the responsibility to protect information resources to which they have access; individuals are also accountable for their access to and use of information resources.

The following roles are defined and used throughout the policies, standards, guidelines, procedures, and best practices that comprise the Information Security Program. The same individual may hold more than one of these roles simultaneously.

## 4.1 Information Trustees

Information Trustees are the senior executive officers of the university and the Deans and Directors of the individual academic faculties (i.e., the president, provost, and other members of the senior leadership team). 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 requirements of the Information Security Program are communicated to and followed by office or department personnel.

## 4.2 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. Information Owners are typically the senior-level executives or managers of university organizational units who have responsibility for the information used by that unit. For example, the University Registrar is the Information Owner for student registration information. When information crosses multiple business processes, each business process owner is deemed an Information Owner. Information Owners are responsible for:

- assigning information classification categories (see Section 5, 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.

4.3 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. Information Custodians are typically system administrators or application administrators in Information Technology or a university organizational unit. When information crosses multiple systems, each system manager is deemed an Information Custodian. Information Custodians are responsible for:

• implementing and applying the information protection levels specified by the Information Owner by using the information security controls required by, and the information security technologies and services provided by, the Information Security Program;
• 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.

4.4 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 requirements of the Information Security Program relevant to their use of university information resources, including the Acceptable Use Policy;
• agree to perform their work according to such requirements;
• 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 roles;
• notify the IT Service Desk or the Information Security Office of any known or suspected information security incident or issue; and
• conduct themselves in a manner consistent with the requirements of the Information Security Program.

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.

4.5 Information Security Advisory Committee

The Information Security Advisory Committee represents the senior leadership of the major academic, 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 should be resolved effectively. This includes:

• facilitating the adoption and implementation of prescribed information security processes or process steps within the office or department, and ensuring compliance with the requirements of the Information Security Program;

• maintaining awareness of 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, guidelines, or other components of the Information Security Program to address new information security and privacy issues as they arise.

The New School Technology Advisory Committee shall fulfill the role of the Information Security Advisory Committee.
5 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.

5.1 Classification Levels

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

5.1.1 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.

5.1.1.1 Security considerations

• Integrity
• Availability

5.1.1.2 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
  - Publications, blog entries, and message board postings
  - Student policies and handbooks
  - School calendars
  - Donor names, amounts, designations
  - Any item The New School has published in the past

5.1.2 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.
5.1.2.1 Security considerations
- Confidentiality
- Integrity
- Availability
- Access Control

5.1.2.2 Examples
- 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
- Internal operating procedures of the university 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

5.1.3 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.

5.1.3.1 Security considerations
- Confidentiality
- Integrity
- Availability
- Access Control
- Non-repudiation

5.1.3.2 Examples
- N-number*
- Social Security number
- Driver's license number
- Other government-issued ID number
- SEVIS number
- Immigration status
- Employee date of birth
- Employee payroll information
- Employee disciplinary information
- Bank account numbers
- Credit/debit card numbers
- Wire transfer information

* Prior to July 1, 2016, N-numbers belonging to employees were classified as Restricted and N-numbers belonging to students were classified as Confidential. To eliminate confusion, especially in cases where an individual is both a student (or former student) and an employee (or former employee), the classification of N-numbers belonging to employees has been changed so that, as of July 1, 2016, all N-numbers are classified as Confidential.
• 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
• Directory information for students who have opted-out of public disclosure
• Information disclosed to or created by the University Ombuds
• 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

5.2 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.

5.3 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 Standard 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

5.4 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.
6  Document Administration

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

6.2 Document Review
This document is subject to periodic review to validate that its content remains relevant and up-to-date. Significant or material changes to this document must be submitted to the Information Security Advisory Committee for review and comment prior to adoption.

6.3 Change history

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial publication</td>
<td>D. Curry</td>
<td>18 Nov 2011</td>
</tr>
<tr>
<td>2.0</td>
<td>Substantial changes to reflect new Information Security Program structure:</td>
<td>D. Curry</td>
<td>April, 2016</td>
</tr>
<tr>
<td></td>
<td>• Split Section 1, “Overview,” into two sections—a shorter overview and Section 3, “The New School Information Security Program”</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Added new Section 2, “Delegation of Administrative Authority and Responsibility”</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Renamed the Information Security Steering Committee to the Information Security Advisory Committee, which better reflects its role</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6.4 Approval History

<table>
<thead>
<tr>
<th>Version</th>
<th>Name</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Information Security Steering Committee</td>
<td>Sr. Director, Design &amp; Construction</td>
<td>18 Nov 2011</td>
</tr>
<tr>
<td></td>
<td>Marla Appelbaum</td>
<td>Asst. Director, Advancement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Jacob Campbell</td>
<td>Information Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alex Carnes</td>
<td>Asst. University Registrar</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tara Creagh</td>
<td>Sr. Benefits Specialist, Human</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Resources</td>
<td></td>
</tr>
<tr>
<td>Version</td>
<td>Name</td>
<td>Title</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>David Curry</td>
<td>Director, Information Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Robert Lutomski</td>
<td>Director, Student Housing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Robin Lynn</td>
<td>Assoc. Director, Online Media</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Charis Ng</td>
<td>Assoc. Director, Institutional Research</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Natalie Pressey</td>
<td>Asst. Vice President &amp; Comptroller</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Donna Puchalski</td>
<td>AVP, Payroll &amp; Tax Compliance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shelley Reed</td>
<td>Sr. Vice President, Information Technology</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Elizabeth Ross</td>
<td>Vice Provost</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Paul Shosho</td>
<td>Director, Financial Systems &amp; Analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Keila Tennent</td>
<td>Assoc. General Counsel</td>
<td></td>
</tr>
</tbody>
</table>
| 2.0     | **Technology Advisory Committee /**  
|         | **Information Security Advisory Committee**            |                | June 2016     |
|         | Anand Padmanabhan (chair) | Senior Vice President and Chief Information Officer       |               |
|         | Andy Atzert               | Vice President for Distributed and Global Education       |               |
|         | Alec Gershberg            | Chair of Urban Policy and Associate Professor of Urban Policy, Milano School of International Affairs, Management, and Urban Policy |               |
|         | Donald Resnick            | Chief Enrollment and Success Officer                      |               |
|         | Barry Salmon              | Associate Professor of Media Studies, School of Media Studies |               |
|         | Bryna Sanger              | Deputy Provost and Senior Vice President for Academic Affairs |               |
|         | Ed Scarcelle              | University Librarian                                       |               |
|         | Tokumbo Shobowale         | Chief Operating Officer                                   |               |
|         | Steve Stabile             | Vice President for Finance and Business and Treasurer     |               |
|         | Joel Towers               | Executive Dean, Parsons School of Design                  |               |