Juilliard

Juilliard Information Security and Governance Policy

Table of Contents

I. **Introduction**
II. **Information Security Principles**
III. **Information Security Governance**
    A. Compliance With the Policy
    B. Information Security Controls, Standards and Testing
    C. Exceptions to the Policy
    D. Information Security Policy Enforcement
IV. **School Information Management**
    A. Introduction
    B. Information Creation and Reproduction
    C. Information Storage and Retention
    D. Information Transport and Transmission
    E. Information Disposal and Destruction
    F. Copyrighted Materials
    G. Handling Confidential/Sensitive Information and Personally Identifying Information
    H. Web Forms and Surveys
V. **School Device Administration and Governance**
    A. Approvals
    B. Electronic Access Privileges
    C. Physical Access Privileges
VI. **Information Technology Acceptable Use**
    A. The Internet
    B. E-Mail, Text/SMS Messages and Instant Messaging (IM)
    C. Facsimile Machines, Printers, Scanners and Photocopiers
    D. Remote IT Network Access
    E. Wireless Technology (WiFi)
    F. Public Cloud and File Hosting Services
    G. Mobile Devices
    H. Social Media
    I. Peer-to-Peer (P2P) Software
    J. Lila Acheson Wallace Library
    K. Technology Resource Center
VII. **Travel Security**
VIII. **Information Security Education, Training and Threat Awareness**

I. Introduction

The Juilliard School ("the School") creates and manages sensitive and confidential information that must be protected. To that end, the Information Security and Governance Policy ("the Policy") specifies permissible information management practices that align with the School's tolerance for risk.

Specifically, it governs (a) the management of confidential or sensitive information ("School information") and (b) the use of devices that store, process or provide access to School information ("School devices"). Anyone who studies at or is employed by the School ("School personnel") including third parties, and uses Juilliard information resources must abide by the Policy.

II. Information Security Principles

The Juilliard Information Security Principles are set forth below. They reflect the School's commitment to protecting confidential and sensitive information. These eight principles represent the foundation for the provisions in the Policy as well as the performance specifications in the School's technology standards. Privilege to access School information and School devices is contingent upon an unconditional acceptance of these Principles and their incorporation into day-to-day information management practices.

Every student, faculty, or staff member working at the School or using School information resources must always do the following:

1. Protect the confidentiality and integrity of School information at all times
2. Exercise professionalism, good judgment and discretion in managing School Information and when using School devices, and be cognizant of the fact that any information we create or action we take may be subject to public scrutiny
3. Comply with all School security policies and standards, and never attempt to subvert, circumvent or otherwise impede controls
4. Only use School information for School-related purposes and only use School devices in a secure manner
5. Never attempt to review, use or disseminate School information or gain access to School devices beyond what is necessary to perform required business activities
6. Only retain School information within approved information repositories
7. Accept that School information will be retained only for as long as necessary for business purposes
8. Immediately report any unauthorized disclosure of School information or the loss or potential compromise of School devices to the Information Technology (IT) Department or the Office of the General Counsel

III. Information Security Governance

A. Compliance with the Policy

The Policy represents the definitive and authoritative reference on School information management and School device usage. All individuals authorized to access School information and/or School devices including affiliated third parties must agree to comply with the Policy at all times. Furthermore, School personnel and affiliated third parties must always comply with IT Department directives. Questions or concerns about the Policy should be directed to the Chief Information Officer or the Office of the General Counsel.

Note that the Policy specifies the minimum requirements necessary to adequately protect School information. Additional requirements may be specified in an agreement between the School and a third party if, for example, the scope of the third party agreement includes potential exposure to confidential health information or other form of controlled information. School personnel must coordinate with the Office of the General Counsel prior to entering into such agreements.

B. Information Security Controls, Standards and Testing

The School utilizes numerous procedures, processes and technologies to protect School information ("Controls"). These controls are necessary to address information security threats that are constantly evolving. In some cases Control specifications have been developed by the Information Technology (IT) Department, and these specifications are reflected in technology standards that align with the Policy.

The IT Department also uses methods and technologies to monitor the IT environment for both security and technology performance. No attempt should ever be made to hide, obfuscate or otherwise defeat such monitoring.

The School also periodically conducts tests designed to assess the viability of its defenses as well as the School's security preparedness. School personnel will not necessarily be aware of these tests, and may be required to undergo additional security training based on test results.

Use of a password is a security control chosen by IT users and is critical to protecting School information. Minimum standards exist for password complexity but IT users are encouraged to exceed those standards. A password for a Juilliard device should never be shared nor publicly displayed.

C. Exceptions to the Policy

The Office of the General Counsel in partnership with the Chief Information Officer oversees information security governance at the School. Their mandate is to facilitate the School's mission and objectives while ensuring School information is protected.

In addition, these entities are responsible for developing, communicating and updating the Policy based on the assessed information security risks to The School. They also adjudicate information management issues with security implications. Exceptions to the Policy may be granted for compelling business reasons and with due consideration for the broader risks to the School. The Office of the General Counsel or its proxy is the only entity at Juilliard that is authorized to grant such exceptions.

D. Information Security Policy Enforcement

School personnel or anyone operating under the direction of the School who willfully disobey the Policy or intentionally subvert and/or repeatedly disregard Controls are subject to discipline to include suspension or dismissal.

IV. School Information Management

A. Introduction

All individuals with privilege to access physical or electronic documents containing confidential or sensitive School information ("School documents") must ensure that all electronic or physical copies of such documents in their possession are securely managed from creation to destruction. Sections B-E below specify the security requirements for managing School Documents across the information lifecycle.

B. Information Creation and Reproduction

The creation or reproduction of a School Document immediately triggers security requirements that persist throughout the life of that document. An omnipresent security requirement is that a School Document may only be viewed by those individuals with a legitimate business requirement to access the information contained therein.

Every reasonable effort should be made to minimize the creation and reproduction of School Documents and thereby reduce the potential for information loss. Note that forwarding an electronic document via e-mail or other information transfer mechanism creates additional copies of that document. Therefore it is incumbent upon individuals sending or forwarding electronic documents containing School information to ensure that every recipient is authorized to review the information contained therein.

Copies of School documents such as PowerPoint presentations disseminated at

meetings should be collected immediately after the meeting and stored securely or destroyed. School Information written on white boards should be erased immediately following the conclusion of the meeting and prior to vacating conference rooms in which that information is displayed. School Documents should be expeditiously removed from printer trays and copier platens, and printing privileges for specific printers should be segregated according to business function and a specific individual's access privileges.

C. Information Storage and Retention

Once a School document is created or reproduced all copies must be stored in an approved information repository. School documents that are stored in electronic repositories must be appropriately segregated or obfuscated (i.e., encrypted) or otherwise managed using appropriate physical and/or electronic security controls so that individuals are only allowed to view those documents for which they have permission.

All School documents and electronic media containing School information should be physically secured. Specifically, and whenever possible and practical, School documents and electronic media containing School information should be stored in locked environments, and strict control of keys and lock combinations maintained. Ideally access to rooms or areas storing documents containing School information should be managed via the School's electronic access control system. As always, deployment of Controls should be based on the assessed risk.

School documents should not be left unattended for extended periods of time. School personnel are encouraged to maintain a neat workspace and thereby assist in maintaining a secure environment. School documents should only be retained for as long as necessary to facilitate School business.

D. Information Transport and Transmission

A School representative must control School documents when these are transported outside of Juilliard. School documents that are hand carried must never be made visible to the public, and should be transported inside a secure container whenever possible and practical.

School documents sent by courier should be tracked and signed for by the intended recipient. Tamper-proof containers should be considered when such documents are physically transported. School documents that are transmitted via the Internet should only be sent to individuals authorized to view that document. School documents should be password-protected and/or file encryption implemented if possible and practical.

The Office of the General Counsel must be notified immediately if a School document is

lost or mistakenly sent to an individual or entity not authorized to view that document.

E. Information Disposal and Destruction

School documents must be disposed of in an effective manner. School documents destroyed on-site (i.e., within Juilliard premises) ideally should be shredded using a cross-cut shredder. School documents should never be disposed of in ordinary trash containers. School personnel should understand how a School Document will be destroyed before discarding that document.

Computer hard drives, portable hard drives and portable memory devices should be electronically wiped or otherwise rendered permanently disabled by the IT Department prior to disposal.

F. Copyrighted Material

IT users must abide by all applicable copyright laws and licensing. Juilliard reserves the right to decline to legally defend any member of faculty, staff or student named in a lawsuit arising out of an alleged copyright infringement, and the School may refuse to pay any damages awarded by a court of law against such persons.

G. Handling Confidential/Sensitive Information or Personally Identifying Information

Confidential/sensitive information or personally identifying information (PII) must be handled differently than other forms of information. PII is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used to de-anonymize anonymous data can be considered PII.

Notable examples of such information include but are not limited to the following:

- Social Security Account Number
- Personal address
- Date of birth
- Passport number
- Tax ID number
- Financial account number
- Credit card number
- Cell/mobile number

Such information needs to be protected so that only individuals authorized to view that information are able to access it. Therefore, anyone who is in possession of documents containing PII and such documents must be retained for business purposes should store the document in a folder or location that has the appropriate security controls, e.g., password protected and restricted. Note that for transmitting confidential/sensitive

information and PII via email users should use the email encryption feature that is available in Office 365.

If the document contains PII and retention is not required for business purposes the document must be permanently deleted as soon as possible and practical. Please note that permanent deletion requires the user to empty the recycle bin. Any questions regarding creating such folders or deleting PII should be directed to the Service Desk at servicedesk@juilliard.edu.

Please see the Juilliard Security Policy for requirements in handling physical documents containing confidential/sensitive information or PII.

H. Web Forms and Surveys

Web forms and surveys are on-line forms that allow recipients to fill in information per the request of the sender. Such forms are powerful information gathering tools but also carry enhanced risk if the information being entered is confidential, sensitive and/or contains personally identifying information (see Section G above). In addition, the School maintains standards to protect its brand, so forms that originate from Juilliard but deviate from established standards can cause reputational harm.

Therefore, individuals wishing to create and send customized Web forms or surveys that meet one or more of the following criteria must submit a ticket to the Juilliard Service Desk (servicedesk@juilliard.edu) prior to creating and disseminating such forms:

- The form contains confidential, sensitive or personally identifying information as noted in Section G above.
- The form contains Juilliard-affiliated personnel names, email addresses, phone numbers or any personal information specific to such individuals.
- The form is posted to a Juilliard web site.
- The form is disseminated from a Juilliard email address.
- The form does not conform to Juilliard branding standards as determined by the Juilliard Communications Department.

Once the Service Desk ticket has been opened an IT Department representative will contact the requestor to obtain more information and coordinate the form development effort. In cases where one or more of the above criteria are met, only the IT Department is allowed to create the customized Web form using a Juilliard-approved application. In addition, IT will determine the appropriate hosting solution.

V. School Device Administration and Governance

A. Approvals

IT Department approval is required prior to installing software/applications on School

devices or when connecting any device to the School IT network. Only IT Department-approved equipment and methods may be used to create, store, process and/or transmit School information.

School devices may never be lent to individuals other than those explicitly authorized to possess and operate such devices. Upon ending employment at Juilliard, School personnel must promptly return all non-personally-owned IT equipment to a Human Resources or IT Department representative.

B. Electronic Access Privileges

An individual should only request, accept and/or be granted electronic access privileges that are necessary to perform his or her designated business function. Electronic access to a School device is contingent upon the successful completion of a School or School-equivalent background investigation. Thereafter, School personnel and third parties must remain in good standing, comply with all School policies and standards and demonstrate a legitimate and ongoing business need to access the information contained within the specific School device(s) being accessed.

Electronic access to School devices always requires authentication of identity using a password or passphrase. Rules on password complexity must comply with applicable Juilliard standards. Note that password complexity can vary depending on the device type or user access privileges (e.g., domain administrator, local administrator, and user). For specific School devices enhanced authentication may be required in the form of two-factors (i.e., “something you know and something you possess”) based on the assessed likelihood, vulnerability or impact of information loss.

Passwords must be protected at all times, and should never be shared or shown to another individual. Passwords and passphrases must be changed periodically in accordance with stated requirements.

No attempt should ever be made to bypass, disrupt or otherwise subvert the use of passwords or any other authentication method used to access School devices. Furthermore, no one is ever permitted to access devices or information for which they do not have authorization and no attempt should ever be made to circumvent or reduce the effectiveness of security controls used to protect a device or information. Knowingly accepting information that has been harvested or accessed illegally is not permitted and is subject to discipline.

C. Physical Access Privileges

Individuals should only request, accept and/or be granted physical access privileges that are necessary to perform his or her designated business function. As with electronic

access privileges, physical access to School devices or areas that house enterprise IT equipment (e.g., server rooms, technology closets) is contingent upon the successful completion of a Juilliard or Juilliard-equivalent background investigation. Thereafter, School personnel and third parties must remain in good standing, comply with School Policies and standards, and demonstrate a legitimate and ongoing business need to access the information contained within the specific School device(s) being accessed.

Physical entry into space containing IT network equipment (e.g., switches, routers, and/or central storage/memory) is restricted to authorized individuals as determined by the IT Department.

School personnel or affiliated third parties who have not successfully passed a School or School- equivalent background investigation must be closely monitored and ideally escorted by a School employee when physically inside space containing IT network equipment or when inside telephone closets.

A School device may sometimes be restricted to a particular sub-network which links to specific physical ports. School personnel are prohibited from connecting School devices to ports other than those specified for that device as determined by the IT Department.

Questions about physical security controls applied to School devices or other information assets should be directed to the Juilliard Department of Public Safety.

VI. Information Technology Acceptable Use

A. The Internet

School personnel and third parties are always expected to exercise good judgment and proper decorum when accessing web sites via School devices. For example, accessing sites that publish sexually explicit content is not permitted. Note that the School monitors all communications to and from the IT network.

Streaming content via devices on the School IT network can place strains on available bandwidth and thereby limit overall network performance. Access to such sites via the School IT network may be restricted based on business requirements, the time-of-day and/or local IT network conditions.

Employees are expected to focus on work-related efforts during business hours and all students, faculty and staff are always expected to exercise good judgment when accessing the Internet.

Webmail or web-based email is any e-mail client implemented as a web application running on a web server. Webmail is accessed on the Internet through a web browser, while client-based email is accessed through a desktop program (e.g., Outlook).

Examples of webmail providers include g-mail, AOL Mail, and Yahoo! Mail.

Accessing personal accounts via webmail is allowed, but as always students, faculty and staff are expected to demonstrate appropriate behavior and exercise good judgment when accessing webmail from the Juilliard network.

B. E-Mail, Text/SMS Messages and Instant Messaging (IM)

E-mail promotes communication but also carries significant risks of unauthorized disclosure of School information. For example, the "Auto Complete" function enables rapid identification of e-mail recipients but also facilitates transmissions to unintended parties. Clicking on embedded links that connect to malicious web sites is a common mode of attack used by malware.

Notwithstanding these vulnerabilities, business requirements mandate the use of e-mail and other common modes of electronic communication. These vulnerabilities mandate hyper-vigilance by IT users when creating and sending emails, text/Short Message Service (SMS) messages and Instant Messages (IMs).

The following are practices expected of Juilliard IT users to reduce the risk of information loss and information leakage:

- Never click on embedded links in communications from un-trusted sources such as unknown e-mail addresses.
- Always check the “To” and “Copy Count (CC)” lines in the communication header before sending. Best practice is to compose the body of the message and insert the recipient’s address before sending.
- Use embedded links to facilitate access to documents rather than attachments whenever possible.
- Always scrutinize communications for information that might be embarrassing or otherwise harmful to the reputation of the sender and/or Juilliard especially if taken out of context. A simple litmus test for the appropriate content is to imagine the impact of that communication being published on the front page of a major news publication.
- Never transmit a message containing sensitive or confidential School information to individuals or accounts of individuals not unauthorized to view that information.

- Ensure that you intend to send a message outside the Juilliard network before you send it. Once it leaves the Juilliard network it is no longer under Juilliard's control and the School cannot be held responsible for the consequences resulting from sending or forwarding email to intended or unintended recipients.

- Approved file sharing solutions should be used to transfer confidential or sensitive School information whenever possible and practical. Faxing is less secure than a secure file sharing solution but it is more secure than e-mail. Questions regarding the security of a particular mode of communication should be directed to the IT Department prior to its use.

- Perform routine "housecleaning" on mailboxes. The School imposes a limit on mailbox size and exceeding that limit will result in the user not being able to send or receive email.

C. Facsimile Machines, Printers, Scanners and Photocopiers

Facsimile machines, printers, scanners and photocopiers ("office machines") are networked devices just like computers. These also have vulnerabilities that are inherent to their set-up, maintenance, and usage. Office machines are increasingly sophisticated and possess enhanced storage capacity.

Therefore, office machines can be used to launch attacks, store unauthorized data, retrieve School documents, and print offensive or unauthorized material. Office machines are often shared by multiple individuals and are focal points of risk both in terms of storing significant School information in memory and creating printed material that is not under a specific individual's physical control. For all of the above reasons, only approved office machines are allowed to be connected to the Juilliard IT network.

D. Remote IT Network Access

IT users connecting to the School network who are physically located outside School space carry enhanced risk of information loss. For example, School information on a computer screen might be visible to individuals not authorized to view that information. School devices that connect to the Internet via WiFi "hot spots" are susceptible to sniffing and man-in-the-middle attacks.

Users connecting to the School network can inadvertently forget to log off or leave their machine unattended for extended periods thereby enabling unauthorized individuals to access the School network if they have physical access to the computer.

Remote network access solutions facilitate secure access to internal Juilliard IT resources from computers external to the network. The School utilizes two solutions to

implement remote access: Virtual Desktop Infrastructure (Citrix) and a Virtual Private Network (VPN). One of these secure remote access solutions is required whenever remotely accessing the Juilliard network.

IT users should be aware that the School monitors Internet access during Citrix and VPN sessions, and on-line behavior must always comply with the Policy. Access to computer resources and/or information available through or displayed via the Citrix solution or VPN is restricted to School personnel and appropriate third parties.

Note that a VPN session is electronically equivalent to being inside the School network. If the computer connecting to the network is compromised, the entire Juilliard network is at risk. Therefore, whenever possible and practical, individuals should use Juilliard-supplied IT equipment to access the Juilliard network via VPN since these devices are managed by the IT Department.

The following are security requirements when remotely accessing the School's IT network:

- Never leave a computer or School device unattended for extended periods while logged into the School network.
- Never allow unauthorized individuals to use a computer or School device while logged into the School network.
- Never allow unauthorized individuals to view School information that appears on a computer monitor screen.
- Ensure remotely printed material containing School information is protected at all times.
- Log off immediately after concluding a remote session.

E. Wireless Technology (WiFi)

1. Juilliard WiFi Domains

   WiFi technology enables wireless access to the Internet. There are four wireless domains at Juilliard:

   a. JUILLIARDwifi is the principal WiFi domain used by students, faculty and staff. It enables a wireless connection to the same IT resources that are accessible via a Juilliard desktop computer. In other words, connecting to the network via JUILLIARDwifi is the wireless equivalent of logging into the School's desktop computers so a Juilliard username and password are

required for authentication.

b. JUILLIARDconsole is used to connect devices (e.g., AppleTV, gaming consoles) to the Internet where a user name and password is not required. Advance permission is required to use JUILLIARDconsole, which can be requested via the Service Desk (helpdesk@juilliard.edu).

c. JUILLIARDsummer is available only during the summer for Juilliard-affiliated residents of the Rose Building.

d. JUILLIARDguest enables wireless access to the Internet by visitors and guests. It does not facilitate access to Juilliard internal IT resources. Note there is a 60-minute time limit when accessing WiFi via JUILLIARDguest, and email can only be sent via Web-based applications. School personnel are not permitted to connect to the Internet via the Guest network using School devices while simultaneously connected to the School network.

2. Wireless Network Access from Public Facilities

Public venues allowing unrestricted Wi-Fi access carry enhanced risk of information loss as they are prime locations for "sniffing" wireless network traffic as well as other attacks. Whenever possible users should access the Internet using Wi-Fi providers that require authentication.

3. Wireless Network Access from Home

As noted above, users may access the IT network remotely via VPN or Citrix remote access solutions using a wireless router and modem. However, users must utilize a wireless protocol that uses strong encryption such as WPA2, the current industry standard. Questions regarding the type of encryption used in a specific home environment should be directed to the IT Department.

F. Public Cloud and File Hosting Services

Cloud-based applications that store information are ubiquitous and their use is sometimes not an option if a particular capability or software is required. However, hosting Juilliard data off-premises carries information security risks. Therefore, coordination with the IT Department is required prior to establishing a contract with a cloud-hosted solution where Juilliard information will be stored.

At a minimum, any public cloud-based service or application used by the School to store and/or process School information should employ the following security controls, noting additional controls may be warranted depending on the assessed risk to the School as

determined by the IT Department:

- Strong encryption to store and transmit information
- Appropriately segregated School information from information belonging to other public cloud clients
- Multi-factor authentication to access School information
- Appropriate password complexity

File hosting services that are pre-approved for Juilliard-related information include One Drive (Office 365) and Dropbox. Users should query the IT Department regarding the appropriate use of these services.

G. Mobile Devices

Mobile devices such as smart phones and tablets are highly portable computers. These devices pose enhanced risk precisely because of their ease of use, portability, processing power and the information they can store and/or access.

Juilliard staff who utilize mobile phones that are configured to receive Juilliard email should coordinate with the IT Department regarding the information security risks. Such devices must be password protected, and any such device that is lost or stolen should be reported to the IT Department immediately.

H. Social Media

Social media offer tremendous opportunities to network and engage in social interaction. They also pose significant risks to IT users and the School. Although activity is allowed on social media sites during work hours, School employees are expected to limit their activity on these sites so that their work is not impacted and to use such resources judiciously.

As always, School personnel should behave professionally and exercise good judgment whenever using an on-line resource including social media. Importantly, School personnel must never post School information on a social media site nor comment on non-public work-related matters. If anyone discovers malicious content and/or inappropriate postings regarding the School or School personnel they should report such activity immediately to the Office of the General Counsel.

School personnel are encouraged to employ basic security precautions when using social media such as password protection, avoiding social media platforms' default privacy and security settings and being attuned to social engineering attempts such as phishing. School personnel are also encouraged to contact the IT Department with

questions or concerns about the risks associated with social media.

I. Peer-to-Peer (P2P) Software

The School's computing and telecommunications resources may not be used for any type of P2P file sharing without pre-approval by the IT Department in consultation with the Office of the General Counsel. In general, such approvals will only be granted if the requestor specifies in writing that the software is required to support specific academic or administrative activities of the School.

Permission to use P2P software may be revoked by the IT Department based on service abuse, network performance degradation, or use in support of the specific academic or administrative activities noted above.

J. Lila Acheson Wallace Library ("the Library")

The Library computer network proves access to JUILCAT, The Juilliard School online library catalogue, as well as to numerous electronic resources. The majority of the computers in the Library are reserved for reference and research purposes only.

There are three computers at the far end of the Library reference room designated for web browsing. There is a twenty-minute per-session time limit on these machines. Other networked computers in the Library may not be used for web browsing or email with the exception of laptops.

K. Technology Resource Center (TRC)

The Technology Resource Center (formerly the "Student Laboratory") is a School resource that is managed by the IT Department, and provides academic computing resources. The TRC maintains Windows and Apple machines for general use as well as specialized applications to support academic and performance-related programs. Only current Juilliard faculty, staff and students are permitted to use the computing resources in the TRC.

All terms specified in the Policy apply to the computing resources in the TRC. In particular, installation of software on TRC machines is not allowed. TRC computer usage may be restricted if a user's conduct on-line is considered inappropriate. Juilliard may in its sole discretion terminate a TRC account if a user has violated the Policy.

Printing resources are also available through a Print Accounting system where each student is granted an initial allowance. Students who exhaust their initial printing allocation are charged for additional pages.

VII. Travel Security

Protecting School information while traveling has specific challenges depending on the destination, business purpose and the traveler. Since travelers are not located in environments controlled by the School, physical vulnerabilities contribute to the risk of information loss. In addition, traveling providing numerous opportunities for devices and/or documents to be lost or stolen. The following are information security procedures that should be followed when traveling:

- Physically secure all documents and portable electronic devices that contain School information at all times. If these are not under your personal control they should be secured in a locked container and/or within a locked room if it is possible and practical to do so.
- Encrypt portable flash memory drives and School devices whenever possible.
- Password-protect all mobile devices containing School information.
- Ensure conversations about sensitive matters cannot be unintentionally overheard in public places, and pay particular attention to the loudness of your voice while speaking on a mobile phone in public.
- Report lost or stolen documents or electronic devices containing School information immediately to the Office of the General Counsel and the IT Department.

VIII. Information Security Education, Training and Threat Awareness

Compliance with the Policy is the responsibility of every School employee or third party with access to School information or School devices. Comprehensive security controls are essential to an effective information security strategy and information security training, education and threat awareness is a significant security control.

To that end, the IT Department leverages a number of methods to ensure IT users are aware of current information security threats and are able to learn about information security best practices. For example, security alerts and updates on immediate threats or other information security-related issues are posted on MyJuilliard, electronic bulletin boards and/or are sent via e-mail. School personnel and IT users should pay close attention to such alerts.

The IT Department periodically provides training or gives talks on security-related issues. Everyone in the Juilliard community is encouraged to attend, participate, and inform colleagues who are not in attendance. In addition, suggestions on future topics are always welcome. Security awareness campaigns are also conducted throughout the year.

In addition, the IT Department posts relevant security information on MyJuilliard, which covers topics related to information security at work and at home. Links to helpful information related

to information security are also posted on this site.

Finally, School personnel who notice unusual and/or suspicious activity while logged into the School network, click on a suspicious link, and/or suspect a machine is compromised, should report these issues immediately to the Service Desk (servicedesk@juilliard.edu) or another IT Department representative.