Juilliard

Juilliard Information Security and Governance Policy

Table of Contents

I. Introduction

A. Applicability: The Juilliard School (the "School") Information Security and Governance Policy (the "Policy") applies to anyone who studies (including Pre-College, Extension) at or is employed by the School ("School Personnel"), affiliated third parties, such as independent contractors, board and trustee members, volunteers, and any individual who uses Juilliard information resources (each, a "Covered Person").

B. Scope: The Policy governs (a) the management of confidential or sensitive information, which includes, but is not limited to, information that is confidential, including personally identifiable information ("PII"), student education records, School financial records, School alumni records ("Sensitive School Information"); and (b) the use of School technical resources, which include, but are not limited to, School networks, servers, devices, software, applications and any technical resource used in the course of your employment or studies, that store, process or provide access to Sensitive School Information. School technical resources may include employee personal devices or contracted platforms.

II. Information Security Standards

Each Covered Person is required to adhere to the following Information Security Standards (the "Standards"):

1. Protect the confidentiality and integrity of Sensitive School Information at all times;
2. Exercise professionalism, good judgment, and discretion in managing Sensitive School Information and when using School technology resources, 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 Sensitive School Information for School-related purposes and only use all devices in a secure manner;
5. Never attempt to review, use or disseminate Sensitive School Information or gain access to School technology resources beyond what is necessary to perform required business activities;
6. Always handle Sensitive School Information using good judgment and in accordance with this Policy. For more details, see Section VI; and
7. Immediately report any unauthorized disclosure of School information or the loss or potential compromise of School technology resources to the Office of Information Technology (IT), the IT Service Desk at servicedesk@juilliard.edu, and the Office of General Counsel (legal@juilliard.edu). Anonymous reports may be made via the school's EthicsPoint hotline.

III. Information Security Governance

A. Compliance with the Policy

Covered Persons must comply with this Policy at all times. Furthermore, School Personnel and affiliated third parties must always comply with IT Department directives. Questions or concerns about this Policy should be directed to the Chief Technology 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 IT Department and 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 this Policy.

The IT Department also uses methods and technologies to monitor the IT environment for both security and technology performance. Users shall not attempt to hide from, 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 single-sign-on provider and complex passwords 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.
Where possible, any technological service must be incorporated using the School’s single-sign on provider as this provides, at a minimum, multi-factor authentication. If an approved service cannot be incorporated in such a manner, the IT Department will provide the appropriate guidance and controls that must be followed.

C. Exceptions to the Policy

Exceptions to this 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, in consultation with the Chief Technology Officer, are the only entities at Juilliard that are authorized to grant such exceptions.

D. Information Security Policy Enforcement

School Personnel or anyone operating under the direction of the School who violate this Policy are subject to discipline up to, and including, suspension or dismissal.

IV. School Information Management

A. Introduction

Covered Persons accessing 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, including when those documents are on their personal devices. Sections B-E below specify the security requirements for managing School Documents across the information lifecycle.

B. Information Creation and Reproduction

School Documents 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 Sensitive School Information to ensure that every recipient is authorized to review the information contained therein.

Hard copies of School Documents with Sensitive School Information that are shared with non-Covered Persons should be collected immediately after use and stored securely or destroyed. Sensitive School Information written on whiteboards should be erased immediately following the conclusion of the meeting and prior to vacating conference rooms in which that information is displayed.

C. Information Storage and Retention

Once a School Document is created or reproduced, all copies must be stored in a Schoolprovided and approved information repository, such as the internal network share or OneDrive. 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. This includes documents on School Personnel's and Trustee's personal devices.

All School Documents and electronic media containing School information must 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.

School Documents should not be left unattended for extended periods of time. School Documents should only be retained for as long as necessary to facilitate School business, and otherwise in accordance with the School's document retention policy.

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 containing privileged information should be password-protected and/or file encryption implemented if possible and practical using the resources approved by the IT Department.

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. Hard copies of School Documents destroyed on-site (i.e., within Juilliard premises) ideally should be shredded. School Documents should never be disposed of in ordinary trash containers.

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 re-assignment within the organization or disposal.

F. Copyrighted Material

All School Personnel must abide by all applicable copyright laws and licensing. Juilliard shall not be responsible for defending or indemnifying Covered Persons against copyright infringement arising from uses of intellectual property in violation of this Policy or other School policies.

G. Handling Confidential/Sensitive Information or Personally Identifying Information

Confidential/sensitive information or personally identifying 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.

PII includes, but is 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 and/or home number

Confidential/sensitive information includes, but is not limited to the following:

- Health records (e.g., medical history, prescriptions)
- Financial information (e.g., credit card numbers, bank account details)
- Biometric data (e.g., fingerprints, facial recognition)
- Login credentials (e.g., usernames and passwords)
- Racial or ethnic origin
- Political opinions
- Sexual orientation
- Institutional data that distinguishes yourself from someone else
- Employment data (termination, promotion, salary, etc.)

Covered Persons possessing or retaining documents containing PII must store the document in a folder or location that has the appropriate security controls, e.g., password protected and restricted. Covered Persons must use encrypted email or similar protective measures in transmitting confidential/sensitive information and PII via email.

If the document contains PII and retention is not required for business purposes, the document must be permanently deleted as soon as possible. Please note that permanent deletion requires the user to empty the recycle bin.

H. Web Forms, App Forms, and Surveys

Web forms, app 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). Online forms / apps also create an interaction point between the public internet and private systems, which carries inherent security risks. 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, app 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 if:

- 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 website.
- The form is disseminated from a Juilliard email address or app.
- The form does not conform to Juilliard branding standards as determined by the Juilliard Office of Communications and Marketing.

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 or app form using a Juilliard-approved application. In addition, IT will determine the appropriate hosting solution.

V. School Technology Resources Administration and Governance

A. Approvals

IT Department approval is required prior to installing software/applications on School technical resources or when connecting any device to the School IT network. Only School technical resources and methods may be used to create, store, process and/or transmit School information.

School technical resources may never be lent to individuals other than those explicitly authorized to possess and operate such devices. Upon ending employment, consultation or any relationship with Juilliard, individuals 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 their designated business functions. Electronic access to School technical resources is contingent upon the successful completion of all required School or School-equivalent background investigation(s). 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 technical resource(s) being accessed.

Electronic access to School technical resources always requires authentication of identity, including two-factor identification, in accordance with IT instructions.

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 technology resources. Furthermore, no one is ever permitted to access School technical resources or information for which they do not have authorization and no attempt should be made to circumvent or reduce the effectiveness of security controls used to protect resources or information. Knowingly accepting information that has been harvested or accessed illegally is not permitted.

C. Physical Access Privileges

Individuals should only request, accept and/or be granted physical access privileges that are necessary to perform their designated business function, as determined by the IT Department. 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 all required Juilliard or Juilliard-equivalent background investigation(s). 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 software/network/hardware. School Personnel are prohibited from connecting School devices/software/network/hardware other than those specified for that device as determined by the IT Department.

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

VI. Information Technology Acceptable Use

The Internet, Apps, and other Online Resources

School Personnel are always expected to exercise good judgment and proper decorum when accessing internet sites, apps, and other online resources ("the Internet") via School resources. For example, without limitation, accessing sites that publish objectionable and/or explicit content is not permitted. School Personnel are prohibited from using School resources to engage in activities such as (but not limited to): 1) accessing, downloading, or disseminating any content or services that contains any material that is defamatory, obscene, indecent, abusive, offensive, harassing, retaliatory, violent, hateful, inflammatory, or otherwise objectionable; 2) promoting violence of any kind, or discrimination based on legally impermissible characteristics such as race, sex, religion, nationality, disability, sexual orientation, age, or other protected status; 3) infringing any patent, trademark, trade secret, copyright, or other intellectual property rights of any other person; 4) violating the legal rights (including the rights of publicity and privacy) of others or contains any material that could give rise to any civil or criminal liability under applicable laws or regulations; 5) advocates, promotes, or assists with any illegal activity; 6) impersonating any person, or misrepresents identity or affiliation with any person or organization; or 7) giving the impression that you are endorsed by the School or any other person or entity, if this is not the case.

A. School Monitoring

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 as determined by the IT Department.

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.

B. Communications platforms

Communications platforms are any messaging services implemented as a web application running on a web server, including email and messenger apps. Examples of such platforms include but are not limited to: G-mail, Messenger, WhatsApp, and other messaging services integrated into social media apps, such as Teams, Asana, and Airtable.

Accessing personal accounts is allowed, but as always students, faculty and staff must demonstrate appropriate behavior and exercise good judgment when accessing from the Juilliard network or device.

Clicking on embedded links that connect to malicious web sites is a common mode of attack used by malware.

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 or phone numbers.
- Always check the “To”, “Carbon Copy (CC)” and “Blind Carbon Copy (BCC)” 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 authorized to view that information.
- Ensure that you intend to send a message outside of the Juilliard network before you send it. Once it leaves the Juilliard network, it is no longer under

Juilliard's control.

- Approved file sharing solutions, such as OneDrive, should be used to transfer confidential or Sensitive School Information whenever possible and practical. Dropbox, Google Sheets, and other non-Juilliard hosted services are less secure than Juilliard-hosted secure file sharing solutions. 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. Printers, Scanners, Photocopiers, and Fax Machines

Printers, scanners, photocopiers, and fax machines ("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 and/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 Juilliard owned equipment and network.

D. Remote IT Network Access

IT users connecting to the School network who are remote 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 or you may be working on an unsecured WiFi network which may put your machine or data at risk. Using Juilliard remote access tools will help keep you and Juilliard's data safe.

Users connecting to the School network must log off at the end of a session and should not leave their machine unattended for extended periods while connected.

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: Parallels 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 Parallels 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 Parallels 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. Individuals must use Juilliard-supplied IT equipment to access the Juilliard network via VPN. The Juilliard VPN is limited to a Juilliard-issued machine, and any request for VPN access is 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. Please lock your device when not in use.

- 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.

- When completed accessing materials remotely, please ensure you log off or disconnect your remote session.

E. Wireless Technology (Wi-Fi)

1. Juilliard Wi-Fi Domains

Wi-Fi technology enables wireless access to the Internet. There are three (3) wireless domains at Juilliard:

a. JUILLIARD Wi-Fi is the primary Wi-Fi network 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 JUILLIARD Wi-Fi is the wireless equivalent of logging into the School's desktop computers, so a Juilliard username and password are required for authentication.

b. JUILLIARD console 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 JUILLIARD console, which can be requested via the Service Desk (servicedesk@juilliard.edu).

c. JUILLIARD guests enable 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 Wi-Fi via JUILLIARD guest, 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 may not be as secure as Juilliard's network or your home network. 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 Parallels 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, approval from the IT Department is required prior to establishing a contract with a cloud-hosted solution where Juilliard information will be stored.

OneDrive (Office 365) is the only preapproved file hosting service for Juilliard-related information. Dropbox use is limited to a few departments in consultation with the CTO. Google Drive is not approved for business use.

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

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 permits School Personnel to use their personal mobile devices to perform work for Juilliard, during working and nonworking hours, on and off Juilliard premises. All materials, data, communications, and information (including but not limited to e-mail, telephone conversations and voicemail recordings, instant messages, and internet and social media postings and activities) created on, transmitted to, received or printed from, or stored or recorded on the device for purposes of conducting Juilliard business or on behalf of Juilliard, are Juilliard property, regardless of who owns the device at issue.

School Personnel who utilize mobile devices that are configured to receive Juilliard email must coordinate with the IT Department regarding the information security risks. Such devices must be password protected, and any such device that is lost, stolen, or potentially compromised, must be reported to the IT Department immediately. School Personnel who utilize such mobile devices must also promptly provide Juilliard IT access to the devices when requested or required for Juilliard's legitimate business purposes, including in the event of any security event or investigation. Any use by School Personnel of a personal mobile device for Juilliard business purposes must conform to this policy, and each user is responsible for using such a device in a productive, ethical, and lawful manner. This includes complying with Juilliard's policies.

H. Social Media

Social media offers tremendous opportunities to network and engage in social interaction. They also pose significant risks to users of School technology resources and the school. School Personnel and third-party contractors are required to limit their non-School business social media activity when using School technology resources so that their work is not impacted.

As always, School Personnel must behave professionally and exercise good judgment whenever using an on-line resource including social media. Importantly, School Personnel must never post Sensitive 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 IT department via service desk to servicedesk@juilliard.edu or the Office of the General Counsel to legal@juilliard.edu.

School Personnel are strongly encouraged to employ basic security precautions when using social media, utilizing a password and activating two factor authentication, implementing the highest level of social media platforms' privacy and security settings, and being attuned to social engineering attempts such as phishing. School Personnel are 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 as needed. Requests for file sharing must specify in writing that the resource is required to support specific academic or administrative activities of the School. Such requests must be submitted to the IT Department, which will review and contact the requestor to discuss the request and determine whether to approve.

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. Technology Resource Center (TRC)

The Technology Resource Center 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 this 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 or terminated 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 provides numerous opportunities for devices and/or documents to be lost, seized, or stolen. The following are information security procedures that must 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.
- Do not take any external storage whenever possible.
- 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 Sensitive School Information immediately to the Office of the General Counsel and the IT Department.
- If you are traveling outside of the United States, please reach out to the IT Department to determine whether any additional measures are needed.

VIII. Information Security Education, Training and Threat Awareness

Compliance with this Policy is the responsibility of all School Personnel with access to School information or School technology resources. 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 posts information on security best practices and security alerts and updates on immediate threats as well as other security information on MyJuilliard and sent via e-mail. We encourage school personnel to review and follow such alerts.

The IT Department periodically disseminates security training as needed via various tools, which training must be completed in order to keep access to Juilliard accounts and School technology resources. The Department also offers talks on security-related issues. Everyone in the Juilliard community is strongly encouraged to attend, participate, and inform colleagues who are not in attendance. The IT Departments welcomes suggestions on future security topics. Security awareness campaigns are also conducted throughout the year.

If you do notice any unusual and/or suspicious activity while using any Juilliard technology resource, please report these issues immediately to the Service Desk to servicedesk@juilliard.edu or to another IT Department representative.

IX. Generative Artificial Intelligence

The use of Generative Artificial Intelligence ("AI") is an emerging technology with tremendous potential in the Information and Data space. This type of AI allows learning through the use of data, images and videos and is based on natural language prompts in an effort to achieve a specific result. With respect to information security, all School Personnel are required to maintain the same standards when using AI as outlined in the policy. As a whole, School Personnel should not use Sensitive School Information when using Generative AI tools.

Juilliard has AI policies for faculty/students and staff that provides guidance on its use. Please refer to the Generative AI Use policies and resources.