TianjinJuilliard
天津茱莉亚学院

Title:	Tianjin Juilliard School Information Security and Governance Policy ("Policy")
文件名：	天津茱莉亚学院信息安全及治理政策（"政策"）
Policy Owner:	Office of Information Technology ("IT" or "IT Department")
政策所有者：	信息技术办公室（"IT部门"）
Contact Information:	Gary Ma 2964 Xinhua Road Central Binhai New Area, Tianjin 300452, China 022 6633 8819 ALLIT@tianjinjuilliard.edu.cn
联系方式：	马志强 中国天津滨海新区 新华路2946号 300452 022 6633 8819 ALLIT@tianjinjuilliard.edu.cn
Applies to:	All members of the Tianjin Juilliard School community (includes all faculty; staff; and students)
适用于：	天津茱莉亚学院全体成员（包括所有教师、行政人员及学生）
Effective Date:	August 3, 2020
生效日期：	2020年8月3日

TianjinJuilliard
天津茱莉亚学院

Tianjin Juilliard School Information Security and Governance Policy

天津茱莉亚学院
信息安全及治理政策

2946 Xinhua Road Binhai New Area, Tianjin, China
中国天津滨海新区新华路2946号300450
tianjinjuilliard.edu.cn

Table of Contents
目录

A. Approvals
批准
B. Electronic Access Privileges
在线访问特权
C. Physical Access Privileges
实际访问特权

VI. Information Technology Acceptable Use
可接受信息技术使用

A. The Internet
互联网
B. E-Mail, Text/SMS Messages and Instant Messaging (IM)
邮件、手机短信及即时消息
C. Facsimile Machines, Printers, Scanners and Photocopiers
传真机、打印机、扫描仪及复印机
D. Remote IT Network Access
远程访问IT网络
E. Wireless Technology (Wi-Fi)
无线技术（Wi-Fi）
F. Public Cloud and File Hosting Services
公共云及及文件存储服务
G. Mobile Devices
移动设备
H. Social Media
社交媒体
I. Peer-to-Peer (P2P) Software
点对点（P2P）软件
J. Lila Acheson Wallace Library
莱拉·艾奇逊·华莱士图书馆
K. Technology Resource Center
技术资源中心

VII. Travel Security
出行安全

VIII. Information Security Education, Training and Threat Awareness
信息安全教育、培训及威胁意识培养

IX. Applicable Laws
适用法律

X. Amendment to the Policy
政策附加条款

I. Introduction
信息

The Tianjin 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.
天津茱莉亚学院（以下称“学院”）创建和管理必须受到保护的敏感及机密信息。为此，信息安全及治理政策（以下称“政策”）规定了与学院风险承受能力相一致的受许可信息管理实践。

Specifically, it governs (a) the management of confidential or sensitive information, including any information, whatever its forms, that is not in the public domain and that must be protected from any inappropriate or unauthorized disclosure or use which could potentially adversely affect the operation and reputation of the School (“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 Tianjin Juilliard School information resources must abide by the Policy.
具体而言，本政策管理（a）机密或敏感信息，包括任何形式、不属于公共领域以及一旦被不当或未经授权披露或使用将对学院运营及名誉造成负面影响，因此必须加以保护的信息（以下称“学院信息“）。（b）对存储、处理或提供学院信息访问的设备的使用（“学院设备”）。任何在学院学习或受雇于学院（统称为“学院人员”，包括第三方在内）并使用天津茱莉亚学院信息资源的人员必须遵守本政策。

II. Information Security Principles
信息安全原则

The Tianjin Juilliard School Information Security Principles are set forth below. They reflect the School’s commitment to protecting School 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.
天津茱莉亚学院信息安全原则如下。它们反映了学院对保护学院信息的承诺。这八项原则是政策规定的基础，也是学院技术标准的表现规范。是否享有访问学院信息和设备特权取决于无条件接受这些原则并将其纳入日常信息管理实践。

Every School personnel, including student, faculty, or staff member and any third parties working at the School or using School information resources must always do the following:
全体学院人员，包括学生、教师或行政人员以及在学院工作或使用学院信息资源的任何第三方必须始终执行以下操作：

1. Protect the confidentiality and integrity of School information at all times
   始终保护学院信息机密性及完整性

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
   在管理学院信息和使用学院设备时，应具有专业精神、良好的判断力和谨慎意识，并认识到我们所创建的任何信息或采取的任何行动都可能受到公众监督

3. Comply with all School security policies and standards, and never attempt to subvert, circumvent or otherwise impede controls
   遵守学院所有安全政策和标准，不得试图颠覆、规避或以其他方式阻碍控制

4. Only use School information for School-related purposes and only use School devices in a secure manner
   仅将学院信息用于与学院相关目的，并且仅以安全方式使用学院设备

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
   切勿在超出执行所需业务活动必要的情况下，试图审查、使用或传播学院信息及取得学校设备的访问

6. Only retain School information within approved information repositories
   仅在批准的信息存储库中保留学院信息

7. Accept that School information will be retained only for as long as necessary for business purposes
   认同学院信息将只在业务需要时保留

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 General Counsel

如出现任何未经授权泄露学院信息或学院设备丢失或潜在受损情况，应立即向信息技术（IT）部门或法务总监报告。

III. Information Security Governance
信息安全治理

A. Compliance with the Policy
遵守政策

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 Information Technology (IT) Department or the General Counsel.
本政策对学院信息管理和设备使用具有权威性。所有被授权访问学院信息和/或学院设备的个人（包括附属第三方）必须同意始终遵守本政策。此外，学院人员和附属第三方必须始终遵守IT部门的指令。如有关于政策方面的问题或疑虑，应直接联系信息技术（IT）部门或法务总监。

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 General Counsel prior to entering into such agreements.
请注意，本政策规定了充分保护学院信息所需的最低要求。例如，如果第三方协议范围包括潜在机密健康信息或其他形式受控信息，则可在学院与第三方之间协议中规定附加要求。在签订此类协议之前，学院人员必须与法务总监进行协调。

B. Information Security Controls, Standards and Testing
信息安全控制、标准及测试

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.
学院利用多种流程、程序和技术来着保护学院信息（“控制措施”）。这些控制措施对于应对不断演变的信息安全威胁是必要的。在某些情况下，控制规范由信息技术（IT）部门制定，并被纳入与政策一致的技术标准中。

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.
IT部门还使用方法和技术监控IT环境的安全性和技术性能。不得试图隐藏、混淆或以其他方式干扰此类监控。

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.
此外，学院还定期进行测试，以评估其防御措施可行性以及学院安全准备情况。学院人员不一定清楚相关测试，可能需要根据测试结果接受额外安全培训。

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 Tianjin Juilliard School device should never be shared nor publicly displayed.
使用密码是IT使用者选择的安全控制，对于保护学院信息安全的至关重要。针对密码复杂性设有最低标准，但鼓励IT用户超过相关标准。天津茱莉亚学院设备密码不得共享或公开显示。

c. Exceptions to the Policy
例外情况

The Legal Counsel in partnership with the IT Department oversees information security governance at the School. Their mandate is to facilitate the School’s mission and objectives while ensuring School information is protected.
法务总监与信息技术部合作，监管学院信息安全。他们的任务是促进学院的使命和目标达成，同时确保学院信息得到保护。

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 General Counsel or its proxy is the only entity at Tianjin Juilliard School that is authorized to grant such exceptions.
此外，上述人员及部门负责根据所评估学院信息安全风险制定、传达和更新政策。他们还就涉及安全问题的信息管理事宜进行判断。如有令人信服的业务原因，并适当考虑到学院面临的更为广泛的风险，可能会批准该政策的例外情况。法务总监或其代理人为天津茱莉亚学院唯一有权批准此类例外的实体。

D. Information Security Policy Enforcement
信息安全政策实施

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.
学院工作人员或在学院指导下执行工作的任何人员，如有故意违反政策或故意破坏和/或多次无视控制行为，将受到纪律处分，包括停职或开除。

IV. School Information Management
学院信息管理

A. Introduction
介绍

All individuals with privilege to access physical or electronic documents containing 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.
有权访问包含学院信息纸质或电子文件（"学院文件"）的所有个人必须确保其所拥有的此类文件的所有电子或纸质副本从创建到销毁都得到安全管理。下文B-E部分详细说明了跨信息生命周期管理学院文档的安全要求。

B. Information Creation and Reproduction
信息创建及复制

The creation or reproduction of a School documents immediately triggers security requirements that persist throughout the life of that document. An omnipresent security requirement is that a School documents may only be viewed by those individuals with a legitimate business requirement to access the information contained therein.
创建或复制学院文档将立即触发贯穿该文档整个生命周期的安全要求。始终存在的安全要求是，学院文件只能由有合法业务要求的个人查看，以访问其中包含的信息。

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.
应尽一切合理努力尽量减少创建和复制学院文件，从而降低信息丢失可能性。请注意，通过电子邮件或其他信息传输机制转发电子文件将创建该文档的额外副本。因此，发送或转发包含学院信息电子文件的个人有责任确保每个接收者都被授权查看其中包含的信息。

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.
会议结束后，应立即收集学院文件副本，如在会议上分发的PowerPoint演示文稿等，并妥善保存或销毁。在会议结束后且腾出会议室之前，应立即抹去写在白板上的学院信息。应迅速从打印机托盘和复印机印版上取下学院文件，特定打印机的打印权限应根据业务功能和特定个人的访问权限进行区分。

C. Information Storage and Retention
信息存储及保留

Once a School document is created or reproduced all copies must be stored in an IT 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.
一旦创建或复制学院文件，所有副本必须存储在IT批准的信息存储库中。必须对存储在电子存储库中的学院文件进行适当分隔或模糊处理（即加密），或使用适当实体和/或电子安全控制进行管理，以保证个人只能查看他们有权查看的文件。

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.
所有包含学院信息的文件和电子媒体都应受到保护。具体而言，在可能和可行的情况下，学院文件和包含学院信息的电子媒体应存放在上锁环境中，并严格控制钥匙和密码锁。理想情况下，应通过学院电子访问控制系统管理存储包含学院信息文件的房间或区域。同以往一样，应基于所评估风险进行控制。

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.
学院文件不应长期无人看管。鼓励学院工作人员保持整洁的工作环境，从而帮助维持安全的环境。应仅在业务所需时间内保留学院文件。

D. Information Transport and Transmission
信息传输及传播

A School representative must control School documents when these are transported outside of the School. 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.
将学院文件运输至校外时，学院代表必须予以控制。随身携带的学院文件决不能被公众看到，应在可能和可行时将其放入安全容器中进行运输。

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.
应对由快递寄送的学院文件进行跟踪并由指定收件人签字。在实际运输此类文件时，应考虑使用防损毁容器。通过互联网传输的学院文件应仅发送给有权查看该文件的个人。应对学院文件采用密码保护和/或文件加密（如果可能和可行时）。

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.
如果学院文件丢失或错误将其发送给未被授权查看该文件的个人或实体，则必须立即通知法务总监。

E. Information Disposal and Destruction
信息处理及销毁

School documents must be disposed of in an effective manner. School documents destroyed on-site (i.e., within Tianjin Juilliard School 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. When deleting a School document in an electronic form, make sure the document has been deleted in hard drive permanently; in particular, dropping a document into the recycle bin of devices (e.g., laptops) does not delete the document permanently but only remove the file from desktop or delete the virtual pathway to it.
必须对有效学院文件进行处理。现场销毁的学院文件（即在天津茱莉亚大楼内）最好使用横切式碎纸机粉碎。决不能使用普通垃圾桶处理学院文件。学院工作人员在丢弃学院文件之前应了解如何销毁该文件。删除电子形式的学院文档时，请确保该文档已在硬盘中被永久删除；尤其需要注意的是，将文档放入设备（如笔记本电脑）的回收站中并不会永久删除该文档，而只会从桌面上删除该文件或删除指向该文件的虚拟路径。

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.

计算机硬盘、便携式硬盘和便携式存储设备应在处理前由IT部门进行电子抹除或以其他方式使其永久失效。

F. Copyrighted Material
版权保护材料

IT users must abide by all applicable copyright laws and licensing. Tianjin Juilliard School 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.
IT用户必须遵守所有适用版权法和许可。天津茱莉亚学院有权拒绝为因涉嫌侵犯著作权而被提起诉讼的教师、行政人员或学生进行法律辩护，并可拒绝支付法院要求相关人员支付的任何损害赔偿。

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 or reflect the individual's activities. 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.
处理机密/敏感信息或个人身份识别信息机密/敏感信息或个人识别信息（PII）必须与处理其他形式的信息不同。PII为能够识别特定个体或反映个体活动的任何数据。任何可以用来区分一个人和另一个人，并可用于给匿名数据去匿名化的信息都可以被看做是PII。

Notable examples of such information include but are not limited to the following:
此类信息的典型示例包括但不限于以下各项：

- Social Security Account Number
  社保账户号码
- Personal address
  个人地址
- Date of birth
  出生日期
- Passport number
  护照号码
- Chinese National ID number
  中国居民身份证号码

- Financial account number
  财务账户号码
- Credit card number
  银行卡号码
- Cell/mobile number
  手机号码

H. Such information needs to be protected so that only individuals authorized to view that information can 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.
应对此类信息进行保护，以保证只有被授权查看相关信息的个人才能访问。因此，出于安全考虑，任何人都应将文件保存在适当文件夹中，以保护文件安全。请注意，邮件用户应使用Office365邮件加密功能传输机密/敏感信息及PII。

If the document contains PII and retention is not required for business purposes or compliance with mandatory legal requirements 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 helpdesk-it@TianjinJuilliard.onmicrosoft.com

Please see the Tianjin Juilliard School Security Policy for requirements in handling physical documents containing confidential or sensitive information or PII.
如文件包含PII，且无需出于业务目的或遵守强制性法律要求进行保留，则必须尽快永久删除该文件。请注意，永久删除需要用户清空回收站。任何有关创建此类文件夹或删除PII的问题，请直接联系服务台：helpdesk-it@TianjinJuilliard.onmicrosoft.com
有关处理包含机密或敏感信息或PII纸质文件的要求，请参阅《天津茱莉亚学院安全政策》。

I. Web Forms and Surveys
Web表单和调查

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.
Web表单和调查为在线表单，允许接收者根据发送者请求填写信息。此类表单为功能强大的信息收集工具，但如果输入的信息机密、敏感和/或包含个人识别信息（见上文G部门），则风险也会增加。此外，学院维持相应标准以保护其品牌，因此源自茱莉亚但偏离既定标准的表单可能会造成声誉损害。

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 (helpdesk-it@TianjinJuilliard.onmicrosoft.com) prior to creating and disseminating such forms:
因此，想要创建和发送满足以下一个或多个标准定制Web表单或调查的个人必须在创建和传播此类表单之前，向茱莉亚服务台提交一张票据(helpdesk-it@TianjinJuilliard.onmicrosoft.com)：

- The form contains confidential, sensitive or personally identifying information as
  noted in Section G above.
  该表单包含机密、敏感或个人识别信息，如上文G部分所述。
- The form contains Tianjin Juilliard School-affiliated personnel names, email addresses, phone numbers or any personal information specific to such individuals.
  该表单包含天津茱莉亚学院所属人员姓名、电子邮件地址、电话号码或任何与此类人员相关的个人信息。
- The form is posted to a Tianjin Juilliard School website, applications or other platforms.
  该表单可在天津茱莉亚学院网站、申请页面或其他平台找到。
- The form is disseminated from a Tianjin Juilliard School email address.
  该表单通过天津茱莉亚学院邮件地址发送。
- The form does not conform to Tianjin Juilliard School branding standards as
  determined by the Tianjin Juilliard School Communications Department.
  该表单不符合天津茱莉亚学院品牌标准，该品牌由天津茱莉亚学院市场部决定。

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 Tianjin Juilliard School-approved application. In addition, IT will determine the appropriate hosting solution.
一旦服务台票据被查收，IT部门代表将联系请求者获取更多信息并协调表单开发工作。如果满足上述一个或多个条件，则只有IT部门可以使用天津茱莉亚学院批准的应用程序创建自定义Web表单。此外，IT部门还将确定合适的托管解决方案。

V. School Device Administration and Governance
学院设备管理

A. Approvals
批准

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. (Also reference to our laptop agreement for TJS document for specific details)
在学院设备上安装软件/应用程序或将任何设备连接到学院IT网络时，需要获得IT部门批准。仅经IT部门批准的设备和方法方可被用于创建、存储、处理和/或传输学院信息。（具体细节请参考天津茱莉亚学院笔记本电脑协议文件）

School devices may never be lent to individuals other than those explicitly authorized to possess and operate such devices. Upon ending employment at or otherwise leaving from (e.g., graduation) The Tianjin Juilliard School, personnel must promptly return all non-personally owned IT equipment to a Human Resources or IT Department representative.
不得将学院借给未经明确授权拥有和操作此类设备的个人。与天津茱莉亚学院结束雇佣关系或以其他方式离开（例如，毕业）后，相关人员必须立即将所有非个人拥有的IT设备归还给人力资源部或IT部门代表。

B. Electronic Access Privileges
在线访问特权

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.
个人只应请求、接受和/或被授予履行其指定业务职能所需的在线访问特权。在线访问学院设备取决于成功完成学院或学院同等背景调查。此后，学院人员和第三方必须保持良好信誉，遵守学院所有政策和标准，并证明出于合法和持续业务需要访问特定学院设备中所包含信息。

Electronic access to School devices always requires authentication of identity using a password or passphrase. Rules on password complexity must comply with applicable Tianjin 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).
访问学院设备始终需要使用密码或口令进行身份验证。密码复杂性规则必须符合适用的天津茱莉亚标准。请注意，密码复杂性可能因设备类型或用户访问权限（例如域管理员、本地管理员和用户）而异。

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.
对于特定的学院设备，根据所评估信息丢失可能性、脆弱性或影响，可能需要通过两个因素（即“您知道的东西和您拥有的东西”）进行增强认证。

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.
密码必须始终受到保护，不得与他人共享或展示给他人。必须根据规定的要求定期更改密码和口令。

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.
不得试图绕过、中断或以其他方式破坏使用密码或任何其他用于访问学院设备的身份验证方法。此外，任何人都不得访问未经授权的设备或信息，也不得试图规避或降低用于保护设备或信息的安全控制的效力。禁止故意接受非法获取的信息，如有违反则将受到处分。

c. Physical Access Privileges
实际访问特权

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 Tianjin Juilliard or TJS-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.
个人只应请求、接受和/或被授予执行其指定业务职能所需的实际访问权限。与在线访问特权一样，对学院设备或企业IT设备所在区域（如服务器室、技术柜）的实际访问取决于是否成功完成天津茱莉亚调查或天津茱莉亚同等背景调查。此后，学院人员和第三方必须保持良好信誉，遵守学院政策和标准，并证明出于合法和持续业务需要访问特定学院设备中包含的信息。

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.
仅经IT部门授权个人可以实际访问包含IT网络设备（如交换机、路由器和/或中央存储/内存）的空间。

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.
未成功通过学院或学院同等背景调查的学院工作人员或附属第三方必须受到密切监控，在有IT网络设备的空间内或在电话间内时，最好由学院员工陪同。

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.
学院设备有时可能被限制在链接到特定物理端口的特定子网中。学院人员不得将学院设备链接到IT部门确定的设备指定端口以外的端口。

Questions about physical security controls applied to School devices or other information assets should be directed to the IT Department.
如有应用于学院设备或其他信息资产的实际安全控制相关问题，应联系IT部门。

VI. Information Technology Acceptable Use
可接受信息技术使用

A. The Internet
互联网

School personnel and third parties are always expected to exercise good judgment and proper decorum on the aspects of law, culture and humanism when accessing web sites via School devices. Any user's behavior via School IT network must abide by the RPC law at least. 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. Anyone using the School-supplied devices or School IT network shall have no expectation of privacy.
学院人员和第三方在通过学院设备访问网站时，应始终在法律、文化和人文主义方面保持良好判断力和适当礼仪。任何通过学院IT网络发生的用户行为，必须至少遵守远程过程调用法。例如，不允许访问发布色情内容的网站。请注意，学院对所有使用IT网络进行的通信采取监控。使用学院提供的设备或学院IT网络的任何人都不应期望保护隐私。

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.
通过使用学院IT网络的设备传输内容会对可用带宽造成压力，从而限制整体网络性

能。根据业务要求、时间和/或本地IT网络条件，可限制通过学院IT网络访问此类网站。

Employees are expected to focus on work-related efforts during business hours.
雇员应在工作时间内专注于与工作相关的工作。

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 AOL Mail, and Yahoo! Mail etc. 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 Tianjin Juilliard School network.
网络邮件或基于网页的电子邮件是在网页服务器上运行的作为网页应用程序实现的任何电子邮件　客户端。网络邮件通过网页浏览器在因特网上访问，而基于客户端的电子邮件则通过桌面程序（如Outlook）访问。网络邮件供应商包括AOL Mail和Yahoo！等。允许通过电子邮件等方式访问个人账户，但与往常一样，学生、教师和行政人员在通过天津茱莉亚学院网络访问网络邮件时应表现出恰当行为和良好判断力。

B. E-Mail, Text/SMS Messages and Instant Messaging (IM)
邮件、手机短信及即时消息

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.
通过电子邮件可以实现通讯，但也可能带来泄露未经授权信息的重大风险。例如，“自动完成”功能可以快速识别电子邮件收件人，但也可能将邮件传输给非预期各方。点击连接到恶意网站的嵌入链接是恶意软件常用的攻击模式。

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).
尽管存在这些漏洞，但出于业务需求，仍然要求使用电子邮件和其他常见的电子通信方式。这些漏洞要求IT用户在创建和发送电子邮件、短信（SMS）

和即时消息（IMs）时高度警惕。

The following are practices expected of The Tianjin Juilliard School IT users to reduce the risk of information loss and information leakage:
以下是天津茱莉亚学院IT用户为降低信息丢失和信息泄露风险所采取的措施：

- Never connect to untrusted network or click on embedded links or attachments in communications from un-trusted sources such as unknown e-mail addresses.
  切勿连接到不受信任的网络，或单击来自未知电子邮件地址等不可信来源的通信中的嵌入链接或附件。

  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.
  发送前，请始终检查通信标头中的“收件人”和“副本计数（CC）”行。最佳做法是在发送邮件之前撰写邮件正文并插入收件人地址。
- Use embedded links to facilitate access to documents rather than attachments whenever possible.
  尽可能使用嵌入链接而非附件来帮助访问文档。
- 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.
  始终仔细检查通信中可能会给发送者和/或茱莉亚造成尴尬或损害其声誉的信息，尤其是在被断章取义的情况下。如要确认内容是否恰当，可以想象其在某主要新闻出版物首页被发表后可能给通信带来的影响。
- Never transmit a message containing sensitive or confidential School information to individuals or accounts of individuals not unauthorized to view that information.
  不得将含有学院敏感或机密内容的信息发送给未经授权查看该信息的个人或个人账户。
- Ensure that you intend to send a message outside the Tianjin Juilliard School network before you send it. Once it leaves the Tianjin Juilliard School network it is no longer under Tianjin Juilliard’s control and the School cannot be held responsible for the consequences resulting from sending or forwarding email to intended or unintended recipients.

在发送之前，请确保您准备向天津茱莉亚学院网络外发送消息。一旦离开天津茱莉亚学院网络，该信息就不再受天津茱莉亚控制，学院不对向预期或非预期收件人发送或转发电子邮件所造成的后果承担任何责任。

- 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.
  在可能和可行情况下，应使用经批准的文件共享解决方案传输机密或敏感学院信息。传真的安全程度不如安全的文件共享解决方案，但比电子邮件更安全。有关特定通信方式安全性的问题，应在使用前咨询IT部门。

- 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.
  对邮箱进行例行"大扫除"。学院限制了邮箱大小，超过这个限制将导致用户无法发送或接收电子邮件。

- Be aware of your surroundings when sharing, sending or faxing School information.
  分享、发送或传真学院信息时，请注意周围环境。

c. Facsimile Machines, Printers, Scanners and Photocopiers
传真机、打印机、扫描仪及复印机

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.
传真机、打印机、扫描仪和复印机（"办公机器"）与计算机一样都是联网设备。它们的设置、维护和使用也存在固有漏洞。办公机器越来越复杂，存储容量也越来越大。

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 the above reasons, only approved office machines are allowed to be connected to the Juilliard IT network. When using office machines, School personnel must ensure information is picked up from the office machines by using their ID card. 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 Wi-Fi "hot spots" are susceptible to sniffing and man-in-the-middle attacks.
因此，办公机器可以用来发动攻击，存储未经授权的数据，检索学院文件，以及打印攻击性或未经授权材料。办公机器通常由多人共享，无论是在内存中存储重要学院信息还是制作不受特定个人实际控制的打印材料，都是风险焦点。基于上述所有原因，只有被批准的办公机器才可连接到茱莉亚 IT网络。使用办公机器时，学院工作人员必须确保使用身份证从办公机器上提取信息。远程IT网络访问连接到学院网络的IT用户，实际位于学院空间之外，增加了信息丢失风险。例如，计算机屏幕上的学院信息可能对未经授权查看该信息的个人可见。通过Wi-Fi"热点"连接到互联网的学院设备容易受到嗅探和中间人攻击。

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.
连接到学院网络的用户可能会无意中忘记注销或使其计算机长时间处于无人看管状态，从而使未经授权的个人能够访问学院网络（如后者可以实际访问计算机）。

Remote network access solution facilitates secure access to internal Tianjin Juilliard IT resources from computers external to the network. The School utilizes a solution to implement remote access: Cisco AnyConnect.
远程网络接入解决方案有助于通过网络外部计算机安全访问天津茱莉亚内部IT资源。学院利用一个解决方案来实现远程访问：Cisco AnyConnect。

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

IT用户应清楚，在使用Cisco AnyConnect召开会议期间，学院会监控互联网的访问，而且在线行为必须始终遵守政策和适用法律。仅限学院人员和恰当第三方通过Cisco AnyConnect访问可用或被展示的计算机资源和/或信息。

Note that a Cisco AnyConnect session is electronically equivalent to being inside the School network. If the computer connecting to the network is compromised, the entire Tianjin Juilliard School network is at risk. Therefore, whenever possible and practical, individuals should use School supplied IT equipment to access the internal network via Cisco AnyConnect since these devices are managed by the IT Department.
请注意，使用Cisco AnyConnect召开会议在等同于使用学院网络。如果连接到网络的计算机遭到破坏，整个天津茱莉亚学院网络都将处于危险之中。因此，在可能和可行情况下，个人应使用学院提供的IT设备通过Cisco AnyConnect访问内部网络，后者由IT部门负责管理。

The following are security requirements when remotely accessing the School's IT
network:
以下为远程访问学院IT网络时的安全要求：

- Never leave a computer or School device unattended for extended periods while logged into the School network.
  登录学院网络时，切勿让计算机或学院设备长时间无人看管。
- Never allow unauthorized individuals to use a computer or School device while logged into the School network.
  学院或个人在未经授权情况下，不得使用未经授权设备登入网络。
- Never allow unauthorized individuals to view School information that appears on a computer monitor screen.
  绝不允许未经授权个人查看出现在计算机显示器屏幕上的学院信息。
- Ensure remotely printed material containing School information is protected at all times.
  确保包含学院信息的远程打印材料始终受到保护。
- Log off immediately after concluding a remote session.
  结束远程会话后立即注销。

D. Wireless Technology (Wi-Fi)
无线技术（Wi-Fi）

1. The Tianjin Juilliard School Wi-Fi Domains
   天津茱莉亚学院无线局域网
   Wi-Fi technology enables wireless access to the Internet. There are four wireless domains at School:
   Wi-Fi技术使无线访问互联网成为可能。学院有四个无线域：
   a. TJS is the principal Wi-Fi domain used by students, faculty and staff. It enables a wireless connection to the same IT resources that are accessible via a School desktop computer. In other words, connecting to the network via TJS is the wireless equivalent of logging into the School's desktop computers so a network username and password are required for authentication.
      TJS为学生、教师和行政人员使用的主要Wi-Fi域。通过它可以无线连接到相同的信息技术资源，可以通过学院的台式计算机访问这些资源。换言之，通过TJS连接到网络相当于登录学院的台式计算机，因此需要网络用户名和密码进行验证。

   b. TJS-console is used to connect devices (e.g., AppleTV, gaming consoles) to the Internet where a username and password is not required. Advance permission is required to use TJS-console, which can be requested via the Service Desk (helpdesk-it@tianjinjuilliard.onmicrosoft.com).
      TJS控制台被用于将设备（如AppleTV、游戏机）连接到不需要用户名和密码的网络。使用TJS控制台需要事先批准，可通过服务台请求(helpdesk-it@tianjinjuilliard.onmicrosoft.com).

   c. TJS-Guest enables wireless access to the Internet by visitors and guests. It does not facilitate access to Tianjin Juilliard School internal IT resources. Note there is a 60-minute time limit when accessing Wi-Fi via TJS-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.
      通过TJS-Guest，访客可无线访问互联网，但不可获取天津茱莉亚学院内部IT资源。请注意，通过TJS-Guest访问Wi-Fi时有60分钟的时长限制，电子邮件只能通过基于Web的应用程序发送。学院人员在连接到学院网络时，不得同时使用学院设备通过访客网络连接到互联网。

2. Wireless Network Access from Public Facilities
在公共场所访问无线网络

Public venues allowing unrestricted Wi-Fi access to 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.
允许不受限制的Wi-Fi接入的公共场所增加了信息丢失的风险，因为后者为“嗅探”无线网络流量和其他攻击的主要地点。只要可能，用户应通过需要验证身份的Wi-Fi提供商访问互联网。

3. Wireless Network Access from Home
在家访问无线网络

As noted above, users may access the IT network remotely via remote access solution using a wireless router and modem. However, users' 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.
如上所述，用户可以通过使用无线路由器和调制解调器的远程访问解决方案远程访问IT网络。然而，用户无线协议使用了强加密技术，如目前的行业标准WPA2。
有关在特定家庭环境中所使用加密类型的问题，请咨询IT部门。

E. Public Cloud and File Hosting Services
公共云及文件储存服务

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 Tianjin 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.
基于云的信息储存应用程序无处不在，如果需要特定的功能或软件，则有时不能选择使用这些应用程序。然而，在异地托管天津茱莉亚数据会带来信息安全风险。因此，在与存储茱莉亚信息的云托管解决方案建立合同之前，需要与IT部门进行协调。

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:
学院用于存储和/或处理学院信息的任何基于云的公共服务或应用程序至少应采用以下安全控制措施。请注意，根据IT部门确定的对学院的评估风险，可能需要采取额外控制措施：

- Strong encryption to store and transmit information
  强加密以存储和传输信息
- Appropriately segregated School information from information belonging to other public cloud clients
  适当地将学院信息与属于其他公共云客户端的信息分开
- Multi-factor authentication to access School information
  采用多因素验证以访问学院信息
- Appropriate password complexity
  采用恰当复杂程度的密码

File hosting services that are pre-approved for Tianjin Juilliard School-related information include One Drive (Office 365). Users should query the IT Department regarding the appropriate use of these services.
预先批准用于天津茱莉亚学院相关信息的文件托管服务包括One Drive（Office 365）。用户应向IT部门询问相关服务的恰当使用情况。

F. Mobile Devices
移动设备

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 Multi-factor authentication access.
The Tianjin Juilliard School staff who utilizes mobile phones that are configured to receive School email should coordinate with the IT Department regarding the information security risks. Such devices must be password protected, and any such device that is believed to be lost or stolen should be reported to the IT Department immediately. To the extent practically possible, in the event a mobile device is believed to be lost, stolen or wrongfully accessed, the IT Department may decide to wipe the mobile device in full or in part. The wiping of mobile devices may delete any personal identifiable information on the device. The users of the mobile device shall be responsible for backing up data on the device on data hosting solution approved by The Tianjin Juilliard School.

智能手机和平板电脑等移动设备都属于高度便携计算机。这些设备正是由于其易用性、便携性、处理能力及可以存储的信息和/或多因素身份验证访问带来了更大风险。

使用被配置为可以接收学院电子邮件的手机的天津茱莉亚学院行政人员应与IT部门就信息安全风险进行协调。此类设备必须设有密码保护，如被认为丢失或被盗，应立即向IT部门报告。在实际可行的范围内，如果移动设备被认为丢失、被盗或错误访问，IT部门可决定全部或部分抹除移动设备。抹除移动设备可删除设备上的任何个人识别信息。移动设备用户应负责通过天津茱莉亚学院批准的数据托管解决方案对设备上的数据进行备份。

G. Social Media
社交媒体

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.

社交媒体为建立网络和参与社会互动提供了无限机会，同时也给IT用户和学院带来了巨大风险。虽然工作时间内允许在社交媒体网站上活动，但学院员工应限制其相关活动以免影响工作，同时应明智地使用相关资源。

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 member of the Juilliard community discovers malicious content and/or inappropriate postings regarding the School or School personnel, they should report such activity immediately to the General Counsel.

和往常一样，学院人员在使用包括社交媒体在内的在线资源时，应该表现出专业行为和良好判断力。重要的是，学院人员不得在社交媒体网站上发布学院信息，也不得对与工作相关的非公共事务发表评论。如果茱莉亚成员发现关于学院或学院人员的恶意内容和/或不恰当帖子，应立即向法务总监报告此类活动。

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.

学院鼓励学生在使用社交媒体时采取诸如密码保护等基本安全防范措施，避免社交媒体平台的默认隐私和安全设置，并适应网络钓鱼等企图进行社会工程诈骗的行为。

School personnel are also encouraged to contact the IT Department with questions or concerns about the risks associated with social media.
学院也鼓励学生就社交媒体相关风险的问题和顾虑与IT部门进行联系。

H. Peer-to-Peer (P2P) Software
点对点（P2P）软件

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 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.
未经IT部事先与法务总监协商批准，不得使用学院电脑及通讯资源进行任何类型的P2P资料分享。一般来说，只有当请求者以书面形式明确要求需要软件支持学院特定学术或行政活动时，才会被授予此类批准。

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.
使用P2P软件的许可可能会被IT部门基于服务滥用、网络性能下降或用于支持上述特定学术或行政活动等原因而撤销。

I. Library ("the Library")
图书馆（"图书馆"）

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 computers at 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 apart from laptops.
通过图书馆计算机网络可以访问JUILCAT、茱莉亚学院在线图书馆目录，以及许多电子资源。图书馆内的大多数计算机都为参考和研究目的而设。图书

馆资料室里有专门用来浏览网页的电脑。使用此种电脑每次限时20分钟。笔记本电脑外，图书馆中的其他联网计算机不得被用于浏览网页或收发电子邮件。

J. Technology Resource Lab (TRL)
技术资源实验室（TRL）

The Technology Resource Lab is a School resource that is managed by the IT Department and provides academic computing resources. The TRL maintains Windows and Apple machines for general use as well as specialized applications to support academic and performance-related programs. Only current Tianjin Juilliard School faculty, staff and students are permitted to use the computing resources in the TRL.
技术资源实验室由IT部门管理，提供学术计算资源。TRL维护微软和苹果的通用设备及专业应用程序，以支持学术和演出相关项目。目前只有天津茱莉亚学院教师、行政人员和学生可以使用TRL中的计算资源。

All terms specified in the Policy apply to the computing resources in the TRL. In particular, installation of software on TRL machines is not allowed. TRL computer usage may be restricted if a user's conduct on-line is considered inappropriate. Tianjin Juilliard School may in its sole discretion terminate a TRL account if a user has violated the Policy.
本政策中所述的所有术语都适用于TRL中的计算资源。特别需要注意的是，不允许在TRL设备上安装软件。如果用户的在线行为被认为是不适当的，则其TRL计算机的使用可能会受到限制。如果用户违反本政策，天津茱莉亚学院可自行决定终止TRL帐户。

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.
打印资源也可以通过打印会计系统访问，每个学生都将获得初始津贴。使用完初始打印配额的学生将按额外页数被收取费用。

VII. Travel Security
旅行安全

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:
因目的地、业务需求和旅行者不同，在旅行时保护学院信息面临特殊挑战。由于旅行者不在学院控制的环境中，物理上的脆弱性会增加信息丢失的风险。此外，旅行为设备和/或文件丢失或被盗提供了大量机会。以下是旅行时应遵守的信息安全流程：

- 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.
  对包含学院信息的所有文件和便携式电子设备进行实际保护。如果这些物品不在您的个人控制之下，则应将其妥善存放在上锁容器中和/或锁好的房间内（如果可能且可行）。
- Encrypt portable flash memory drives and School devices whenever possible.
  尽可能对便携式闪存驱动器和学院设备进行加密。
- Password-protect all mobile devices containing School information.
  对所有包含学院信息的移动设备进行密码保护。
- Never leave mobile devices containing School information unattended for extended periods. Always lock such mobile devices when not in use.
  不要让包含学院信息的移动设备长时间处于无人看守状态。在不使用此类移动设备时，请始终进行锁闭。
- Avoid using public Wi-Fi hotspots that are from unknown sources. When the use is must, use the School provided Cisco AnyConnect software to protect the date and device, if applicable.
  避免使用来源不明的公共Wi-Fi热点。当必须使用时，使用学院提供的Cisco AnyConnect软件以保护日期和设备（如适用）。
- 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.
  确保不会在公共场所无意中听到有关敏感事项的谈话，且在公共场所使用移动电话时特别注意声音大小。
- Report lost or stolen documents or electronic devices containing School information immediately to the General Counsel and the IT Department.
  如有包含学院信息的电子设备丢失或被盗，则应立即向法务总监和IT部门报告。

VIII. Information Security Education, Training and Threat Awareness
信息安全教育、培训及威胁意识培养

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.
遵守本政策是每个学校雇员或访问学院信息或设备第三方应承担的责任。全面的安全控制对有效的信息安全战略至关重要，信息安全培训、教育和威胁意识培养是一项重要的安全控制措施。

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 MyHub Tianjin Juilliard, electronic bulletin boards and/or are sent via e-mail. School personnel and IT users should pay close attention to such alerts.
为此，IT部门利用多种方法确保IT用户了解当前存在的信息安全威胁，并能够了解信息安全最佳做法。例如，关于即时威胁或其他信息安全相关问题的安全警报和更新被发布在MyHub Tianjin Juilliard上，电子公告板上和/通过电子邮件发送。学院人员和IT用户应密切关注此类警报。

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.
IT部门定期提供培训或就安全相关问题举行讲座。我们鼓励茱莉亚所有成员参加、参与并通知未出席的同事。此外，我们欢迎所有人就未来的议题提出建议。

Security awareness campaigns are also conducted throughout the year.
学院全年还开展安全意识宣传活动。

In addition, the IT Department posts relevant security information on Hub.tianjinjuilliard.edu.cn, 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.
此外，IT部门在Hub.tianjinjuilliard.edu.cn上发布相关安全信息，内容涉及工作和家庭中的信息安全。与信息安全相关有用信息的链接也发布在上述网站上。

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 (helpdesk-it@TianjinJuilliard.onmicrosoft.com) or another IT Department representative.
最后，如果学院人员在登录学校网络时发现异常和/或可疑活动，点击了可疑链接，和/或怀疑设备受到破坏，应立即向服务台(helpdesk-it@TianjinJuilliard.onmicrosoft.com)或者其他IT部门代表报告这些问题。

IX. Applicable Laws
适用法律

PRC laws, regulations and other normative documents shall be strictly observed at all times. In the event of a conflict between the Policy and the applicable PRC laws, regulations or other normative documents, the law, regulation or normative documents will prevail, such as China Cyber Security Law.
始终严格遵守中华人民共和国法律、法规和其他规范性文件。如本政策与适用中国法律、法规或其他规范性文件发生冲突，则以后者为准，如《中国网络安全法》。

X. Amendment to the Policy
政策附加条款

The Tianjin Juilliard School reserves the right to amend these policies from time to time as may be necessary. The updated version of the Policy would be posted on website. All School personnel shall visit the link from time to time to ensure he or she understands the most updated School policies in terms of information security and governance.
天津茱莉亚学院保留根据需要不时修改相关政策的权利。本政策的最新版本将被公布在网站上。所有学院人员应不时访问该链接，以确保他或她了解学院在信息安全和治理方面的最新政策。