Computing Policy

Policy Number: **TRU - 927**

Date of Issuance: 12 Dec 2022

Responsible Department: Office of the IT Director. Questions about this policy should be directed to the Information Security Team, infosec@indycc.edu

Purpose

The purpose of this Computing policy ("Policy") is to set forth guidelines so that members of our community may use the campus network and computing facilities in ways that are responsible and respectful of privacy.

Scope

This policy applies to all users of Independence Community College's ("College") information systems, including students, faculty and staff, and any others granted the use of college information systems and data. It applies to the use of all computing facilities owned, leased, operated, or contracted by the College. As used in this policy, terms such as "computing," "computing/information systems," "information resources," "devices", etc., refer to all computers, communication systems, and peripherals, internet of things, software, telephones, and systems with similar functions, which are owned or leased by the College, or which utilize College infrastructure such as telephone lines or computer networks.

Although this policy does not attempt to deal specifically with legal issues, college members are responsible to act in compliance with the law, including any federal, state, and local laws governing computer and telecommunications use, as well as all other applicable college policies.

Privileges and Responsibilities

Every member of the Independence community who uses computing and related communications systems at the College, or systems that belong to the College or which rely on the College's infrastructure has the responsibilities described in this policy. This includes members of the Independence community who have restricted privileges, such as alumni who may have electronic mail access only. Individuals with personally owned devices, but who rely upon the college's network to connect those devices, are expected to abide by the policies set forth in this document. Personally owned devices operating independently or networked through a non-college connection are not covered under this policy.

Access to the College's information systems is contingent upon being a member of the College community and adhering to college and Information Systems policies, guidelines, and procedures, including this policy. Misuse may result in the loss of access and/or college disciplinary action. For some users and certain systems, access may be authorized by specific departments. In such cases, any department- or group-specific policies and guidelines must be adhered to when using resources provided by the department or group. This is in addition to college policies and Technology Services guidelines and procedures.

Any user who suspects a violation of the college's Information Systems use policies, or who has knowledge of potential vulnerabilities or security loopholes in a system or network at the College, should immediately notify the Information Security Team at infosec@indycc.edu.

Maintain the Security and Confidentiality of your Account

Users assume personal responsibility for the actions associated with their computer accounts. This responsibility begins with selecting a secure password and involves maintaining the confidentiality of that password and changing the password regularly and/or enabling multi-factor authentication in order to assure the continued security of your account. For guidance in selecting a secure password and/or enabling multi-factor authentication, please contact the Help Desk. If you believe that someone has made unauthorized use of your account, you should change your password immediately and report the incident to the Help Desk.

Respect for Others’ Property and Privacy Rights

Users are responsible to respect copyright agreements and intellectual property ownership. Any material that is the work of another, whether explicitly copyrighted or not, should not be distributed by any user without appropriate acknowledgement and/or permission of the creator. Unless permission has been granted by the owner of copyright protected materials, distribution of copyright protected material via the college network or information systems is prohibited.

Improper/Illegal Communications

Any communications that would be improper or illegal on any other medium are equally so on information systems: libelous material, obscene messages, harassment, forgery, threats, etc. However, this is not intended to restrict the free expression of ideas. Communication conducted in accordance with the college policies with the statement on Academic Freedom and Responsibility will not be considered a violation of this policy.

Risks of Data Loss and Data Persistence

Although the college will make efforts to secure the network and college-controlled servers from abuse and damage, it cannot guarantee against data loss by a student, faculty or staff member, either on a college-operated or an individually owned device.

Personal Use

While the college makes information systems available primarily to achieve its goals of academic advancement and for administrative activities, it realizes the need to encourage the personal use of computing for the convenience of the campus community. Thus, it is reasonable to allow the use of information systems for activities that can facilitate convenience or enhance productivity, to the extent that the activity is within the limits described by Information System’s Policies. Any personal use of Information Systems related to operating a personal business or commercial enterprise is prohibited unless permission to do so has been specifically granted by the Vice President of Technology Services, Digital Transformation.

We reserve the right to restrict personal use of college systems and networks by an individual or by the community at large, if the use of resources for such activities becomes excessive.

Privacy

The user must presume that the contents of any other users’ directory are private unless expressly designated otherwise, just as one would presume that the contents of someone’s apartment or office are private. An unprotected account or shared device are not considered to be public unless the name or service expressly indicates that it is. In such cases, any files or other data which would appear to be private in nature, by virtue of the file name or data stored, even if “publicly accessible” should be considered to be private. The user accessing such files has a responsibility to ask the owner of the files or service if the files are intended to be publicly accessible before the user does more than a “cursory glance” sufficient to cause the question.

A user can explicitly grant access to his or her directories and files. However, users who issue general or vague invitations to browse through their files incur a special obligation to protect any material that they do not wish others to see. Indeed, all users are urged to maintain protection levels on their files consistent with the access they are actually willing to give to other users.

Access to User Data

Electronic data on a user’s account, whether stored on a computer in the user’s office/room or elsewhere under the proprietary control of that user, may not be examined without the user’s consent, except in cases of emergency or security, in response to a valid subpoena, search warrant, order of a court, Information Security, or by specific request by the employees’ supervisor for the purpose of accessing work-related electronic data. Posting of data by a user on platforms available to the public or to users of the college shall be understood to imply consent, and electronic access given to specific parties by the user will likewise imply consent for those parties to access permitted data. Emergencies may include, for example, but are not limited to, the death, incapacity or disappearance of the user, or the search for and examination of files used for apparently malicious activity in an account which endangers the integrity of information systems, the network, or other aspects of the college's computing infrastructure.

Only specifically designated individuals are permitted to determine what passes for an "emergency." Such individuals may be specifically designated or may be designated by job position/description for employees. For students the Office of the Dean of Student Affairs will be the designated to determine what is defined as an "emergency" aside for what was stated above.

Whenever possible and legally permissible, notification must be given to the user whose data are subject to subpoena, search warrant, or order of court prior to compliance therewith. Any intrusion by an employee of the university into a user's electronic data must be reported to the user as soon as possible, and within five days of the event via electronic mail unless prohibited by order of court, or due to a continuance of an ongoing investigation by the College. Violation of any aspect of this policy is a sanctionable offense.

In cases where a staff member believes that electronic data in their account has been inappropriately accessed by another staff member, the incident should be reported to Human Resources. For students, it should be reported to the Dean of Student Affairs.

Note: Removable media such in a faculty or staff office, or in a residence hall suite are not subject to search by Technology Services, though Technology Services will assist authorized law enforcement agencies or authorities to read data after they are obtained, at the agencies' or authorities' request.

Protecting Confidential Information

Users who maintain confidential information, such as records relating to employees or students, are responsible for following privacy-related policies, laws, and data use agreements.

Protecting Personal Information

As is described throughout this policy, data transmitted across the college's network or stored on college systems may be accessed by others as a result of misuse by an individual, as an incidental result of the routine operation of the network and systems, or in response to a court subpoena or college investigation into suspected or alleged misuse. While complete privacy of personal data may not be possible, users who wish to ensure a higher degree of privacy for their data are encouraged to use encryption, PGP security, or other techniques to reduce the risk that others may access their data.

Misuse and Inappropriate Behavior

The following activities are expressly prohibited at Independence Community College:

Using a computer system without proper authorization granted through a college official. Some activities such as "port scanning" are not expressly prohibited. However, if the target of such scanning requests that an individual or system stop performing such actions, the person or system performing the scans must stop scanning the target machine and/or networks unless the scans are being carried out by a privileged user who has the authority and responsibility over the machine(s) being scanned or for the network being used.
Concealing your identity, or assuming the identity of another (e.g., by sending forged electronic mail). Note that some forms of electronic communication, such as browsing Web pages, passively "identify" users. Keeping your identity private either by not setting an identity in your browser or by using a Web-anonymizer in order to protect yourself from being put onto mailing lists is not a violation of this policy.

Sharing your account with the specific exception of staff or faculty members allowing their administrative support personnel to access their accounts in order to provide services appropriate to their job functions. Note that individual account password sharing is explicitly forbidden.

Using another person’s computer account, user id, files, or data without appropriate permission, as described in the previous bullet (e.g., using an account found “logged in”).

Deleting or tampering with another user’s files or with information stored by another user on any information-bearing medium (disk, tape, memory, etc.). Even if the user’s files are unprotected, apart from files obviously intended for public reading, such as Web pages, it is improper for another user to read them unless the owner has given permission (e.g., in an announcement in class).

Attempting to “crack” or guess other users’ passwords. Privileged Users or those specifically designated by the administrator or owner of a system may attempt to crack passwords in order to test and enhance the security of the system. In cases where an individual or department “owns” machines which use password files controlled by another organization (e.g., Information security course machines or their like), the owner may not attempt to crack passwords without explicit permission by the owners of the password database.

Obtaining passwords by other means, such as password capturing, phishing, and key logging programs.

Attempting to circumvent system security (e.g., breaking into a system or using programs to obtain “root” or “administrative” access), without the explicit permission of the owner of that system.

Denying permitted and appropriate access to resources to other users (e.g., Denial of service attacks.).

Releasing malicious code, malware, etc., that disrupt other users, damage software, or hardware, disrupt network performance, or replicate themselves for malicious purpose.

Sending commercial solicitations via electronic means (i.e., spamming) to individuals, or to newsgroups or mailing lists where such advertising is not part of the purpose of the group or list.

Any “mass mailing” which is solicitous in nature, unless the mailing is in the conduct of college business.

Reselling of services based on the college network, such as web hosting, mailing services or the selling of shell accounts.

Running a proxy server which results in inappropriate or unauthorized access to college materials to non-college members.

Advertising commercial businesses or ventures on Web pages hosted by Independence, unless prior authorization has been granted.

Using mail messages to harass or intimidate another person (such as by repeatedly sending unwanted mail or broadcasting unsolicited mail).

Violations of any local, state, or federal laws, such as the distribution of copyright-protected materials (e.g., the distribution of commercial software, music, or films in electronic format without appropriate permissions by the owner, even if the user distributing the materials notifies others of their copyright status).

Tampering with, willful destruction of or theft of any computer equipment, whether it belongs to the college or to an individual. Tampering includes any deliberate effort to degrade or halt a system, or to compromise the system/network performance. Willful destruction includes any deliberate disabling or damaging of computer systems, peripheral equipment such as scanners or

printers, or other facilities or equipment including the network, and any deliberate destruction or impairment of software or other users' files or data.
The unauthorized removal of college's or another's computing equipment, which constitutes theft.

This list should not be considered to be complete or exhaustive. It should, however, serve as a set of examples of obviously inappropriate behaviors. If you are in doubt about the appropriateness of something that you want to do, contact the Help Desk and ask first.

Enforcement

Inappropriate behavior in the use of computers is punishable under the information security policies and regulations regarding faculty, staff, and students. The offenses mentioned in this policy range from relatively minor to extremely serious, though even a minor offense may be treated severely if it is repeated or malicious. Certain offenses may also be subject to prosecution under federal, state, or local laws.

Appropriate disciplinary action depends not only on the nature of the offense, but also on the intent and previous history of the offender. The range of possible penalties includes reprimands, loss of computing privileges, course failures for students, disciplinary probation, suspension or dismissal from the college and/or criminal prosecution.

Offenses that are minor or appear to be accidental in nature are often handled in a very informal manner such as through electronic mail. More serious offenses involve formal procedures pursued through Student Affairs for students, Human Resources and/or the respective Vice-President for staff and faculty.

Restrictions of Privileges During Investigations

During the course of an investigation of alleged inappropriate or unauthorized use, it may be necessary to temporarily suspend a user's network or computing privileges, but only after determining there is at least a prima facie case against the individual, as well as a risk to the college or its information resources if privileges are not revoked. In these cases, it is important to recognize that the restriction of network or computing privileges is intended to protect the system rather than to punish the individual. For example, if a computer account has been used to launch an attack on another system, that account will be rendered inactive until the investigation and/or response effort is complete. This is a necessary action taken to prevent further misuse and does not presume that the account holder initiated the misuse. Unsubstantiated reports of abuse will not result in the suspension of accounts or network access unless sufficient evidence is provided to show that inappropriate activity occurred. For example, if someone reports that their computer was "attacked" by a Independence system, the burden will be upon the complainant to provide sufficient data logs or other evidence to show that the incident did, indeed at least appear to be an attack.

Adverse Impact on Shared Systems

The college reserves the right to discontinue communication with external systems that are known to harbor malicious actors and/or content (e.g., spammers, account crackers, and phishing sites) even though this may restrict certain acceptable communications. When deemed necessary, this action will be taken to protect the security and safety of our systems. Similarly, there may be cases where a particular service or activity on a given college system will, by the very nature of its legitimate operation, tend to generate attacks from other Internet sites. If these attacks are frequent and severe enough to cause service interruptions for larger parts of the campus community, it may be necessary to temporarily or permanently remove these systems from the campus network. In cases where such an action is deemed necessary, network administrators will work with the maintainers of the system to identify alternative methods of network access. In cases where the college restricts access to external sites or removes network access for internal sites, the purpose of the action is to maintain the security and reliability of the computer systems and networks rather than to punish an individual or a site, or to restrict the free expression of ideas.

Privileged User Agreement

Date of Issuance: 12 Dec 2022

Responsible Department: Office of the IT Director. Questions about this policy should be directed to the Information Security Team, infosec@indycc.edu.

INTRODUCTION

Privileged access enables an individual to take actions that may affect computing systems, network communication, or the accounts, files, data, or processes of other users. Privileged access is typically granted to system administrators, network administrators, staff performing computing account administration, or other such employees whose job duties require special privileges over a computing system, network or web-based resource account.

Individuals with privileged access must respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with any relevant laws or regulations. Individuals also have an obligation to keep themselves informed regarding any procedures, business practices, and operational guidelines pertaining to the activities of their local department.

In particular, the principles of academic freedom, freedom of speech, and privacy of information hold important implications for Technology Services. Individuals with privileged access must comply with applicable policies, laws, regulations, precedents, and procedures while pursuing appropriate actions required to provide quality, timely, reliable, Technology Services.

GENERAL PROVISIONS

1. Privileged access is granted only to authorized individuals. Privileged access shall be granted to individuals only after they have 1) completed Privileged User training and 2) read and signed this Agreement.
2. Privileged access may be used only to perform assigned job duties.
3. If methods other than using privileged access will accomplish an action, those other methods must be used unless the burden of time or other resources required clearly justifies using privileged access.
4. Privileged access may be used to perform standard system-related duties only on machines and networks whose responsibility is part of assigned job duties. Examples include:
    - installing system software;
    - relocating individuals' files from critically overloaded locations;
    - performing repairs required to return a system to normal function, such as fixing files or file processes, or killing runaway processes;
5. performing security functions;
6. monitoring the system to ensure reliability and security.
7. Privileged access may be used to grant, change, or deny resources, access, or privilege to another individual only for authorized account management activities or under exceptional circumstances. Such actions must follow any existing organizational guidelines and procedures. Examples include:
    - disabling an account apparently responsible for serious misuse such as: attempting to compromise root (UNIX) or the administrator account (Windows), using a host to send harassing or threatening email, using software to mount attacks on other hosts, or engaging in activities designed to disrupt the functioning of the host itself;
    - disconnecting a host or subnet from the network when a security compromise is suspected;
    - accessing files for law enforcement authorities with a valid subpoena.

In the absence of compelling circumstances, the investigation of information in, or suspension of, an account suspected to be compromised should be delayed until normal business hours to allow appropriate authorization and/or notification activities.

- I*n all cases, access to other individuals' electronic information shall be limited to the least perusal of contents and the least action necessary to resolve a situation.*
- *Individuals with privileged access shall take necessary precautions to protect the confidentiality of information encountered in the performance of their duties.*
- *If, during the performance of their duties, individuals with privileged access inadvertently see information indicating serious misuse, they are advised to consult with their supervisor and the office of Information Security. For cases involving. If the situation is an emergency, intervening action may be appropriate.*

Authorization

Under most circumstances, the consent of the named account user must be obtained before accessing their files or interfering with their processes. If consent cannot be obtained, then conditions for "Access Without Consent" must be met and access documented.

Notification

In either case, the employee or other authority shall, at the earliest opportunity consistent with law and Institutional policy, attempt to notify the affected individual(s) of the action(s) taken and the reasons for those action(s).

AGREEMENT

- I have read this *Privileged User Agreement*, the Independence Community College Information Security Policy, and the completed the Privileged User training.
- I agree to comply with the provisions of this *Privileged User Agreement*.

Signature ______________________________ Print Name ______________________________	Date ______________________________
Systems or Resources Approved for Privileged Access: ____ ____ ____ ____	
Authorizing Signature ______________________________ Print Name ______________________________	Department ______________________________ Date ______________________________

Minimum Security Standards

Overview

These standards are intended to reflect the minimum level of care necessary for Independence’s sensitive data. They do not relieve Independence or its employees, partners, consultants, or vendors of further obligations that may be imposed by law, regulation, or contract.

Independence expects all partners, consultants, and vendors to abide by Independence's information security policies. If non-public information is to be accessed or shared with these third parties, they should be bound by contract to abide by Independence's information security policies.

Cybersecurity is a rapidly evolving field that continuously presents us with new challenges, these standards will be revised and updated accordingly.

Endpoints

An endpoint is defined as any laptop, desktop, or mobile/internet of things (IOT) device.

Determine the risk level by reviewing the data risk classification examples, server risk classification examples, and application risk classification examples and selecting the highest applicable risk designation across all. For example, an endpoint storing Public (Low Risk) Data but utilized to access a Restricted (High Risk) application is designated as Restricted (High Risk).

Follow the minimum-security standards in the table below to safeguard your endpoints.

Standard		What to do	Risk		
			Low	Moderate	High
Patching		Apply security patches within seven days of being published. Use a supported operating system version.	X	X	X
Whole disk encryption		Enable FileVault (MacOS) or BitLocker (Windows).		X	X
Endpoint protection		Install EDR and for Windows ensure Defender is enabled. Set the applicable profile based on the system’s risk level.	X	X	X
Backups		Backup official local user data at least daily. College provided OneDrive is recommended.	X	X	X
Inventory		Review and update asset management records at least quarterly. One endpoint per record.	X	X	X
Host based firewall		Enable host-based firewall in default deny mode and permit the minimum necessary services.	X	X	X
Equipment Disposal		All media should be wiped using Crypto-shredding SOP. All equipment should be logged in a disposal log.	X	X	X
Credentials and Access Control		Review existing accounts and privileges quarterly. Enforce password complexity requirements.	X	X	X
Regulated Data Security Controls		Implement PCI-DSS, HIPPA, NACHA, and GLBA, as applicable and NIST 800-171 Rev. 2, as a baseline.		X	X
Configuration Management		Manage Windows devices with MDM and/or policy solution and MacOS with Apple Configuration Manager.	X	X	X

Centralized Logging		Forward logs to a remote server and configure NTP to point to the specified NTP server.		X	X
Physical Protection		Store systems in areas protected by access controls or other locking containers.			X
Dedicated Admin Access		Access administrative accounts only through a Secure Access Workstation (SAW) or Trusted Keyboard.		X	X
Security, Privacy, and Legal Review		Request a Security, Privacy & Legal review and implement recommendations prior to deployment.		X	X
Session Locking		Session lock that terminates after a defined condition with pattern hiding displays will be implemented to prevent access and viewing of data after a period of inactivity.		X	X

Servers

A server is defined as any host that provides a network accessible service.

Determine the risk level by reviewing the data, server, and application risk classification examples, server risk classification examples, and application risk classification examples and selecting the highest applicable risk designation across all. For example, a server running a Public (Low Risk) application but storing Restricted (High Risk) application is designated as Restricted (High Risk).

Follow the minimum-security standards in the table below to safeguard your endpoints.

Standard		What to do	Risk		
			Low	Moderate	High
Patching		Based on National Vulnerability Database (NVD) ratings, high severity security patches apply within seven days of being published and all other security patches within 30 days. Use a supported operating system version.	X	X	X
Whole disk encryption		Enable FileVault (MacOS), BitLocker (Windows), or the equivalent (Cloud/Virtual).		X	X
Endpoint protection		Install EDR and ensure Defender is enabled for Windows.	X	X	X
Backups		Backup at least daily. College provided SOLUTION is recommended.			
Inventory		Review and update asset management records at least quarterly. One endpoint per record.	X	X	X
Host based firewall		Ensure the firewall is enabled. Ensure Defender Advanced Firewall is enabled for all profiles (Windows).	X	X	X
Equipment Disposal		All media should be wiped using Crypto-shredding SOP. All equipment should be logged in a disposal log.	X	X	X

Credentials and Access Control		Review existing accounts and privileges quarterly. Enforce password complexity requirements.	X	X	X
Regulated Data Security Controls		Implement PCI-DSS, HIPPA, NACHA, and GLBA, as applicable and NIST 800-171 Rev. 2, as a baseline.	X	X	X
Configuration Management		Manage Windows devices with group policy and MacOS with Apple Configuration Manager.	X	X	X
Centralized Logging		Follow audit guide and install Elastic Agent / the appropriate beats. If a logging process failure occurs, then the organization will be alerted.		X	X
Vulnerability Management		Perform a monthly Nessus scan. Remediate critical and high vulnerabilities within seven days of discovery and moderate vulnerabilities within 30 days.	X	X	X

Risk Classification Guide

Date of Issuance: 12 Dec 2022

Responsible Department: Office of the Chief Information Officer. Questions about this policy should be directed to the Information Security Team, infosec@indycc.edu.

Overview

Independence Community College ("College") has adopted the following Risk Classification Guide ("Guide") as a standard to classify its information assets into risk-based categories for the purpose of determining who should access the information and what security precautions must be taken to protect it against unauthorized access. This is to protect the confidentiality of Institutional Data.

This guide applies to all Institutional Data as well as any other College affiliate. This guide should be used by all faculty, staff, and third-party Agents of the College as well as any other College affiliate, including student workers, who are authorized to access, manage, or create Institutional Data.

Violations of this guide may result in suspension or loss of the violator's use privileges, with respect to Institutional Data and College owned Information Systems. Additional administrative sanctions may apply up to and including termination of employment or contractor status with the College. Civil, criminal, and equitable remedies may apply. Exceptions to this guide must be approved by the Information Security Team and formally documented. Policy exceptions will be reviewed on a periodic basis for appropriateness.

Data Risk Classification

The set of classifications established for institutional data and systems are: Public (Low Risk), Private (Moderate Risk), and Restricted (High Risk).

Risk Levels

Public (Low risk)	Data and systems are classified as Low Risk if they are not considered to be Moderate or High Risk, and: 1. The data is intended for public disclosure, or 2. The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our mission, safety, finances, or reputation.
Private (Moderate risk)	Data and systems are classified as Moderate Risk if they are not considered to be High Risk, and: 1. The data is not generally available to the public, or 2. The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on our mission, safety, finances, or reputation.
Restricted (High risk)	Data and systems are classified as High Risk if: 1. Protection of the data is required by law/regulation, 2. Independence is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed, or 3. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

Data Risk Classification Examples

This Use the examples below to determine which risk classification is appropriate for a particular type of data. When mixed data falls into multiple risk categories, use the highest risk classification across all.

Public (Low risk)	Independence email addresses Information authorized to be available on or through Independence's website without authentication Policy and procedure manuals designated by the owner as public Job postings Information in the public domain Publicly available campus maps
Private (Moderate risk)	Student records and admission applications Faculty/staff employment applications, personnel files, benefits, salary, birth date, personal contact information Non-public Independence policies and policy manuals Non-public contracts Independence internal memos and email, non-public reports, budgets, plans, financial info College and employee ID numbers Project/Task/Award (PTA) numbers Engineering, design, and operational information regarding Independence infrastructure
Restricted (High risk)	Health Information, including Protected Health Information (PHI) Health Insurance policy ID numbers Social Security Numbers Credit card numbers Financial account numbers Driver's license numbers Passport and visa numbers Donor contact information and non-public gift information

Server Risk Classification Examples

Public (Low risk)	Servers used for academic computing purposes without involving Moderate or High-Risk Data File server used to store published public data
Private (Moderate risk)	Servers handling Moderate Risk Data Database of non-public College contracts

	▪ File server containing non-public procedures/documentation ▪ Server storing student records
Restricted (High risk)	▪ Servers handling High Risk Data ▪ Servers managing access to High-Risk systems ▪ College IS and departmental email systems ▪ Core campus infrastructure

Application Risk Classification Examples

Public (Low risk)	▪ Applications handling Low Risk Data ▪ Online maps ▪ College online catalog displaying academic course descriptions
Private (Moderate risk)	▪ Applications handling Moderate Risk Data ▪ Human Resources application that stores salary information ▪ Directory containing phone numbers, email addresses, and titles ▪ College application that distributes information in the event of a campus emergency ▪ Online application for student admissions
Restricted (High risk)	▪ Applications handling High Risk Data ▪ Human Resources application that stores employee SSNs ▪ Application that stores campus network node information ▪ Application collecting personal information of donor, alumnus, or other individual ▪ Application that processes credit card payments

Approved Application, Platforms, Clouds, and Services

	Public	Private	Restricted	
	Low	Moderate	High	
			Non-PHI	PHI
Audio and Video Conferencing: Zoom, Skype, WebEx	X	X	X	X
Calendar: Office 365	X	X		
Cloud Infrastructure: Microsoft Azure	X	X	X	X
Content Management: Jadu	X	X		
Database Hosting: MySQL	X	X		
Document Management: Office 365 OneDrive	X	X	X	
Document Management: Office 365 SharePoint	X	X	X	
Document Management: Office 365: Word, Excel, PowerPoint, OneNote, and Forms	X	X	X	
Electronic Signature: AdobeSign	X	X	X	
Electronic Signature: DocuSign	X	X		
Email: Office365 (with “Secure:” in subject line)	X	X	X	X
Email: Office365 (without “Secure:” in subject line)	X	X		
Email: Other Departmental Systems	X	X		
Encryption: Bitlocker Encrypted Device	X	X	X	X
File Storage: AFS, CIFS, NFS	X	X		
File Storage: Secure AFS, Secure File Storage	X	X	X	X
Form Builder: (X-Forms, Independence Forms) Web Forms	X	X		
Instant Messaging: Jabber, Skype for Business	X	X	X	X
Instant Messaging: Microsoft Teams	X	X		
Network Access Control: ClearPass	X	X	X	X
ServiceNow	X	X		
Shared Computing: VDI, Commons Computers	X	X		
Survey Tool: Qualtrics, Excel Forms	X	X		X
Voice Messaging (Voice Mail)	X	X		
VPN: VPN Clients	X	X	X	X
Web Programming: CGI	X	X		

1 Payment Card Industry (PCI) data has special regulatory requirements that preclude using the services above. Contact the PCI team for assistance with handling this type of data.

2 Protected Health Information (PHI) data has special regulatory requirements that govern using the services above. Contact the DRA team for assistance handling this type of data.

This table indicates which classifications of data are allowed on a selection of commonly used Independence College Technology Services.