## Overview

The Information Technology Policies Manual ('The IT Policies Manual" or "Manual") provides a summary of IT policies at City University of Seattle ("CityU" or the "University").

Compliance with the University's policies is a condition of employment. With the exception of the At-Will Employment policy, which can only be modified in writing and signed by the President, City University of Seattle reserves the right to interpret, revise, modify, delete, amend, supplement or rescind policies, procedures, work rules, or benefits at any time in its sole and absolute discretion. This Manual complements all other City University of Seattle Manuals, Policies, and Practices relating to Information Technology. We may supplement or amend this Manual with additional Policies and Guidelines from time to time. Any new or modified policy/practices will be approved by the President before adoption.

## Purpose

This Manual summarizes IT policies and practices in effect at the time of publication. All previously issued IT policies (whether written, oral/expressed, or implied), memoranda, forms, or other communications that are inconsistent with this Manual are superseded.

The IT Policies Manual is not intended to be an employment contract of any kind and should not be construed as creating any expressed or implied contract terms or obligations on the part of City University of Seattle. In addition, neither the Manual nor any other documents create, or are intended to create, a promise/representation of continued benefits or employment, with the exception of written employment contracts that are approved and signed by the President. ***Any verbal or written representations inconsistent with these rules should be considered invalid***.

Please note:

- You are responsible for reading, understanding, and complying with City University of Seattle's IT Policies.
- No verbal statements or representations can alter the provisions of this Manual.
- When policies and procedures change, you are responsible for reviewing any updated policies, and if you have questions or concerns, you should seek clarification and guidance. In a discrepancy, the most recently revised and communicated policies will prevail.
- Violating any City University of Seattle policy may result in disciplinary action, including termination of employment. The policies, procedures, and practices described in this Manual have been designed and are expressly intended to comply with applicable local, state, and federal law fully. To the extent that any of the policies, procedures, or practices are inconsistent with applicable law, the applicable law will govern.

**individual written employment contracts, faculty agreements, or other policies may supersede some of the provisions of the IT Policies Manual. To be valid, an individual employment contract must be in writing and signed by the President and the employee for whom it was prepared.*

## Policy Enforcement

A Policy violation is an act that fails to follow existing statements in the policy itself. The City University of Seattle security policies describe behaviors, methods, security configurations, controls, and settings that conform to the security posture of the City University of Seattle infrastructure.

Each violation or failure to enforce any policy by anyone will be reported in writing by the Director of IT as a security incident. Unless overridden by the Director of Human Resources, the responsible party's supervisor is responsible for deciding on the penalty

Security Policies are reviewed and modified as needed or when significant changes in the City University of Seattle Information Technology, systems, and network entail different security requirements.

## IT Policies Review Schedule

IT Policies are reviewed on an annual basis.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200. 00 |
| | Policy Title: Information Technology Use Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

City University of Seattle relies upon every community member to act with integrity, professionalism, and responsibly and legally when utilizing the University's information technology resources. City University of Seattle expects everyone to review and abide by the Acceptable Use and Copyright Infringement Policy and promptly report situations that may violate this policy.

This policy applies to all users of information technology resources owned or managed by City University of Seattle and the City University of Seattle System. Individuals covered by this policy include all full-time and part-time employees; contingent workers, including leased workers; independent contractors and service providers; faculty, including staff and adjunct; students, alums as well as all persons of interest (POI), including vendors, volunteers, guests, visitors and trustees, and any external individuals or organizations accessing University information technology resources.

Information technology resources include all City University of Seattle and City University of Seattle System owned, licensed, or managed hardware and software and use of the University's network via a physical or wireless connection, regardless of the device's ownership.

## Rights and Responsibilities

City University of Seattle's information technology systems are a critical but finite resource. They must be used only for purposes that are consistent with the business and mission of City University of Seattle. These resources should only be used in an ethical, responsible, and lawful manner and only to fulfill one's assigned job duties or study activities. As a condition for receiving access to City University of Seattle information technology resources, users are expected to respect the University in all electronic interactions made within and outside the University. Users are responsible for reporting violations of this policy to their direct supervisor, the Director of Human Resources, or the Director of Information Technology.

## Adherence with Federal, State, and Local Laws

As a member of the City University of Seattle community, you are expected to:

- Abide by all federal, state, and local laws.
- Abide by all applicable copyright laws and licenses. City University of Seattle has entered into legal agreements or contracts for many information technology resources requiring each individual to comply with those agreements. Employees, workers, or contractor with questions or concerns about the terms of an agreement should contact their supervisor or

COO/CFO. Students and alums who have questions should contact the VP of Student Administration.

- Abide by laws that regulate and protect intellectual property as they apply to music, videos, games, images, texts, and other media for personal use and in the creation of electronic information.

## Conditions of Acceptable and Unacceptable Use

City University of Seattle information technology resources must not be used to engage in behavior or communications that violate the law or University policy. The following are conditions of acceptable and unacceptable use, including, but not limited to:

- **Violation of applicable federal or state laws and University policies,** including but not limited to the transmission of threats, harassment, defamation, obscenity, and pornography; theft of or unauthorized access or use of University resources; fraudulent offers of products, items, or services from any University account; or conduct unreasonably obstructing or disrupting working, teaching, learning or research.

- **Copyright infringement.** Be aware that reproduction, modification, or distribution of copyrighted works, including, but not limited to, images, text, or software, without permission of the owner is an infringement of U.S. Copyright Law and subject to civil damages and/or criminal penalties from fines up to and including imprisonment as well as disciplinary actions up to and including termination. Copyright infringement also includes the reproduction, modification, or distribution of web page graphics, sound files, videos, trademarks, software, and logos, unless you have the legal right to use, copy, or distribute the protected work. Other activities, such as making software available for copying on your computer and connecting that computer to CityU's network is also considered copyright infringement. For more information, see https://www.copyright.gov/.

- **Engaging in activities that compromise computer security or disrupt University services.** Intentionally introducing malicious programs into the network or server (e.g., viruses, worms, trojan horses, e-mail bombs, ransomware, phishing emails, or malware in general); and interfering with the proper operational function of the City University of Seattle wired or wireless network is prohibited. You must not use tools normally used to assess security or attack computer systems or networks unless you have been specifically authorized to do so by the IT Information Security Officer. You must not use University information technology resources in conjunction with the execution of programs, software, or other processes that are intended to disrupt (or that could reasonably be expected to disrupt) other computer or network users or damage or degrade the performance of software or hardware components of the system.

- **Making fraudulent offers** of products, items, or services originating from any University account.

- **Use of University resources to actively procure or transmit material that violates sexual harassment or hostile workplace policy.**

- **Exporting software, technical information, encryption software or technology in violation of international or regional export control laws** (e.g. sending encryption software to a prohibited country).

- **Unauthorized access** can include the following: using another user's account or attempting to

gain access to another user's account or information unless explicitly granted the right to do so by authorization from a Department/Division Head in consultation with the Director of HR and the Director of IT; allowing others to use an account they are not authorized for use (account sharing); revealing or sharing an account password to an unauthorized person(s); transferring or extending the privilege of using City University of Seattle technology resources to people or groups outside of the University unless the COO/CFO has explicitly authorized it. You must not attempt to access restricted portions of the University's network, servers, operating systems, security systems, or other administrative applications without appropriate written authorization. You may only use the information technology resources for which you have authorization.

- **Unauthorized use of resources, data, systems or an account** for political lobbying or campaigning, personal financial gain, interests or benefit, including but not limited to engaging in commercial enterprise or selling access to the University's systems or networks, is strictly prohibited.

- **Access or distribution of confidential and personal information** about University employees or students, unless explicitly authorized by CityU Departmental authority, is strictly prohibited. You are individually responsible for the appropriate use of all information technology resources assigned to you, including a computer, network address, software, and any other hardware devices. You should make a reasonable effort to protect your account passwords and to secure information technology resources against unauthorized use or access.

Categories for Authorization of Software

No person may use or facilitate the use of any software on City University of Seattle's computers unless the Information Technology Department specifically authorizes it. If it is the Information Technology Department authorizes its use must fall into one or more of the following categories:

- It is in the public domain.
- It is covered by a valid licensing agreement with the software authors, vendor, or developer, whichever is applicable, regardless of whether it was purchased or donated to the University.
- The user has purchased it, and a record of a bonafide purchase exists and can be produced by the user upon demand.
- It is being reviewed or demonstrated by the users, pursuant to the permission given by the owner, in order to reach a decision about possible future purchases or requests for contribution or licensing.
- It has been written or developed by City University of Seattle, including employees or contingent workers for the specific purpose of being used in the University's computer environment.
- A University official authorizes it with appropriate contractual signatory authority.
- It has been copied in compliance with the published copyright and licensing agreements provided with the purchase of all software.

Consequences of Information Technology Misuse

Violations of this policy can occur because of accidental or inadvertent actions or intentional misuse,

including illegal activity. The University reserves the right to determine what is appropriate and inappropriate. Failure to comply with this policy may result in revocation of user accounts and system access, up to and including suspension or termination of employment, enrollment, or affiliation with the University. Unauthorized use of City University of Seattle technology resources is illegal, constitutes theft and may be prosecuted by the University.

City University of Seattle reserves the right to remove or limit access to material posted on University-owned or administered systems or networks if University policies, contractual obligations, or if local, state, federal or other applicable laws are violated.

The University reserves the right to restrict the use of its computing facilities and limit access to its networks when faced with evidence of violations of university policies or standards, contractual obligations, and federal, state or local laws. Violations of the law may be reported to the appropriate civil authorities.

Misuse of City University of Seattle Information technology may result in the loss of computing privileges and may require financial restitution to the University for losses incurred by the University. Unauthorized use of City University of Seattle technology resources constitutes theft and may be prosecuted by the University.

Any actions which deter others from doing their work or which would be otherwise deemed malicious will result in the loss of access to the system, subject to disciplinary action and/or prosecuted in a civil and/or criminal action. Violations of this policy shall be referred to the appropriate University officials for disposition in accordance with the applicable policy governing the individual's conduct*, access to University technology resources and social media rules.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.03 |
| | Policy Title: Password/MFA Security Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

The goal of this policy is to define the user's behavior, clarify the responsibilities of University users regarding the Password and Data Security rules, and map out the steps they must take to help protect University information and information systems.

## Scope

Individuals covered by this policy include all full-time and part-time employees, contingent workers, including leased workers, independent contractors and service providers, faculty, including staff and adjuncts, students, alumni, as well as all persons of interest (POI) including vendors, volunteers, guests, visitors and trustees, and any external individuals or organizations accessing University information technology resources.

## Password/MFA Policy

Most of the University's Technology resources can be accessed by entering a password and/or a code. Passwords and codes are intended to prevent unauthorized access to information and are considered confidential information.

Passwords and codes do not confer any right of privacy upon any user. Thus, even though users may use passwords and codes for accessing Information Technology resources, users must not expect that any information maintained on the University's technology resources, including text, electronic mail, and voicemail messages, is private.

Users must not:

- Share their passwords/codes with anyone;
- Access systems of another worker or student without express authorization by the Director of Technology or Director of Human Resources;
- Include passwords in emails or any electronic format unless the file or media is encrypted;
- Write down the password and store it in the workplace (e.g. under keyboards or on the monitor).

It is a security best practice never to use the same password for multiple work systems (laptops/desktops. software or servers). It is strongly recommended that you not use the same username and password for work systems used on your personal devices or any third-party website login pages.

This policy, the password standard operating procedures and the internal University security controls

are safeguards in place to guarantee consistency of password rules, alignment with security best practices, and application password requirements and implemented to minimize the risk of jeopardizing the University security posture.

It is of paramount importance that when new technology is introduced into the University infrastructure, a security architecture review is performed by the IT team, and according to this policy, all default passwords must be changed.

The following guidelines should be used for a strong password: Use at least 12-character pass phrases (contains multiple words)

One or more of each of the following:

- lower-case letter
- upper-case letter
- number
- special character or punctuation mark (e.g.,#, ?, !, $)

Things to avoid when creating/using a passphrase:

- using dictionary words
- using personal information such as birthdays, pets, SSN or addresses consecutive repeated characters
- using words as part of the username common acronyms
- keyboard patterns, like qwerty or 12345 (Avoid sequences of numbers in order) the same password used for another application
- typing the password on computers that are not trusted or on unsecure networks, for example, in an Internet cafe

Privileged user accounts, service accounts and vendor accounts, which may pose additional security risks, must adhere to specific, more stringent complexity requirements. CityU reserves the right to change these requirements through the IT Standard Operating Procedures Password Rules at any time.

## Compliance

City University of Seattle is required to comply with several security frameworks and standards regarding password requirements such as The Gramm-Leach-Bliley Act (GLB Act or GLBA) and Payment Card Industry Data Security Standards (PCI-DSS) (at the time of writing version 3.2.1).

The Gramm-Leach-Bliley Act requires Financial Institutions (Higher Education Institutions are treated as Financial Institutions for this purpose) to protect their customers' private information. The following practices are followed:

- Prevent terminated employees from accessing customer information by **immediately** deactivating their passwords and user names and taking other appropriate measures.
- Encrypting sensitive user information when it is transmitted electronically via unsecured or public networks (web), including sending sensitive data/information by email.
- When user information is stored on a server or other computer, ensure that the computer is

accessible only with a "strong" password and is kept in a physically-secure area.
- Avoid storing sensitive user data on a computer with an Internet connection or employ encryption for sensitive data.

The Payment Card Industry Data Security Standard (PCI DSS) applies to any organization that does business using payment cards like credit cards and debit cards. The recent version 3.2.1 requires the following actions (in addition to what was required in version 3.1):

- Vendor-supplied defaults ("admin," "guest," "user," etc.) must be changed from any system that can be used to access payment card information.
- A unique identification must be assigned to every user with access to cardholder data, so that every action taken on the system can be tracked to a specific person.
- Two-factor authentication (or multi-factor authentication) must be required for all non-console administrative access and for remote access to cardholder data environment. This means an authentication system that asks for at least two of the following: something you know (like a password), something you have (like a token or smartcard), or something you are (physical/biometric information like a fingerprint).

## Data Security

While City University of Seattle is committed to protecting its technology resources, it is impossible to eliminate all risk of a data breach. Users must make every effort to secure data that is considered highly sensitive, confidential or personal.

## Least Privilege Rule

City University of Seattle enforces the "Least Privilege" rule for users. The day-to-day login on endpoint systems and servers is performed using standard user privileges on their account, with minimum permissions required to accomplish user's Statement of Work. When required to run applications or install programs that requires elevated privileges (in rare occasions) a different account must be used. This account must have a different password of the day-to-day account. City University of Seattle users must not login for day-to-day activity with the elevated privileged account also called "administrators" accounts.

## Confidentiality

Employees accessing data must observe requirements for confidentiality and privacy and must comply with CityU data protection and control procedures.

City University of Seattle users must not copy, report or distribute any personally identifiable, sensitive or confidential data that they are not authorized to access or to which they have been mistakenly been granted access. Users must report any such unauthorized access to the data owner.

Open, guest or public wireless networks not provided by City University of Seattle should not be considered trustworthy.

When connecting personally owned computers to City University of Seattle technology resources, the user of those computers must take steps to making sure that the computers are free from security

vulnerabilities and viruses. These computers must have operating systems that are supported by their manufacturers (e.g. Microsoft Windows OS and Apple OS/X) and it is recommended users have antivirus software packages installed which are updated with the latest antivirus data files. It is recommended users download and install the latest operating system and application software security patches on their own personal devices. (see also for reference the "Remote Access Policy" for more details).

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.04 |
| | Policy Title: Security and Training Awareness Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

This policy specifies an information security awareness and training program to inform and motivate all workers regarding their information security obligations.

The goal of this policy is to outline the user's behavior, responsibilities and actions regarding the Information Security and Data Protection rules

## Scope

This policy applies to all City University of Seattle users such as employees, contractors, faculty.

## Security Awareness Training Policy.

University employees are required to complete the Information Security training within the first ninety (90) days of employment and annually thereafter.

The training provides important information to help users safeguard their access to University information systems and understand the security controls implemented by the University Security Team.

The training addresses (1) regulations establishing security requirements that are focused on Data Protection, (2) security measures required to protect the University from common security threats and (3) complying to appropriate security standards.

University employees are also encouraged to attend security workshops, security best practices, and guidelines carried out by the CityU Information Technology Team.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.05 |
| | Policy Title: Information Security Plan Overview |
| | Prepared By: COO/CFO |
| | |

## Purpose

The Information Security Plan Overview is the policy that outlines a comprehensive risk-based approach to the implementation of security controls in all the City University of Seattle System areas.

This policy applies a security defense-in-depth approach to all City University of Seattle users, such as employees, contractors, faculty, and students, and the resources they use.

## Information Security Plan

The Information Security Plan focuses on the following areas:

- Confidentiality of personally identifiable information.
- Integrity of data stored in transit or processed on CityU information systems.
- Availability of information stored in transit or processed on CityU information systems.
- Securing and Hardening of CityU information systems.
- Compliance with applicable laws, regulations, CityU/campus policies governing information security and privacy protection such as PCI, FERPA, GDPR, GLBA.
- Effectiveness of the current security safeguards for controlling high risks and establishment of new security controls for data loss prevention.
- Identification and remediation of vulnerabilities and security weaknesses to CityU Information Systems.
- Incident Response to security incidents, prevention to security threats and risk mitigation to security breaches and breach notification.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.01 |
| | Policy Title: Institutional Data Governance Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

Data governance focuses on improving data collection, data quality, protecting access to data, establishing business definitions, maintaining metadata and documenting data policies. Data governance relies on the right people involved at the right time using the right data to make the right decisions. Its role is to ensure that the highest quality data possible is delivered throughout the university and provides valuable information to serve organizational needs. The university's institutional information is a valuable asset and must be maintained and protected as such. It is vital to have accurate, trusted data in order to make sound decisions at all levels of an organization. Data governance helps to provide data transparency and results in confidence among university faculty, staff and management to trust and rely on data for information and decision support.

This policy applies to all institutional data used in the administration of City University of Seattle and all of its Organizational Units, including but not limited to any and all employee, student, alumni, or financial data. Data collected and used for the specific purpose of an IRB research project are excluded from this policy and fall under the IRB policies. This policy covers, but is not limited to, institutional data in any form, including print, electronic, audio-visual, and backup and archived data.

## Governing Institutional Data

The following principles are set forth as minimum standards to govern the appropriate use and management of institutional data:

- Institutional data are the property of City University of Seattle and shall be managed as a key asset
- Institutional data use shall comply with federal, state, local and other regulatory agency guidelines
- Unnecessary duplication of institutional data is prohibited
- Quality standards for institutional data shall be defined and monitored
- Institutional data shall be protected (See Data Protection Policy)
- Institutional data shall be accessible according to defined needs and roles
- Institutional metadata shall be recorded, managed and utilized by Institutional representatives held accountable to their roles and responsibilities
- Necessary maintenance of institutional data shall be defined and followed
- Resolution of issues related to institutional data shall follow established policies
- Data stewards are responsible for the subset of data in their charge

## Data Quality

Data quality is crucial to operational and transactional processes and the reliability of data

analytics and business intelligence reporting. Data quality is defined by information's fitness to serve its purpose in a given context. Data quality dimensions include:

| | |
|---|---|
| - Accuracy and Precision | Currency and Relevance |
| - Compliance | - Non-duplication |
| - Completeness | - Validity |
| - Consistency and Reliability | - Accessibility, Availability and Timeliness |

## Rules Required to Govern Data

No one person, department, division, school, or group "owns" institutional data, even though specific units bear responsibility for certain data. Several roles and responsibilities govern the management of, access to, accountability for, and training for responsible use of institutional data. The President of City University of Seattle has ultimate authority over all City University of Seattle data.

- **Data trustees:** Data trustees are institutional officers (e.g., vice presidents, provost, and deans) who have authority over policies and procedures regarding business definitions of data and the access and usage of that data within their delegations of authority. Each data trustee appoints data stewards for specific subject area domains.
- **Data stewards:** Data stewards are university business officials (outside the Division of IT) who have direct operational-level decision-making responsibility for managing one or more types of institutional data. They are responsible for identifying and managing the data custodians for their area.
- **Data custodians:** Data custodians are system administrators responsible for the operation and management of systems and servers that collect, manage and provide access to institutional data.
- **Data users:** Data users are university units or community members who have been granted access to institutional data to perform assigned duties or fulfill assigned roles or functions within the university; this access is granted solely for the conduct of university business.

## Accountability and Responsibility

A community is a grouping of users. Communities serve as taxonomies of high-level institutional data subject areas and are key to assigning accountability and responsibility. The following data governance communities will meet as separate groups to discuss data quality issues:

1. Student Data
2. Academic Data
3. Alumni Data
4. Administrative Data
5. Research Data

## Data Access Categories

City University of Seattle data shall be classified into one of the four following categories for the purpose of simplifying granting of access:

1. **Public Access Data:** Data that are openly available to all staff, students, and the general public.

2. **Internal General Data:** Data that are used for University administration activities and not for external distribution unless otherwise authorized.
3. **Internal Protected Data:** Data that are only available to staff with the required access in order to perform their assigned duties.
4. **Internal Restricted Data:** Data that are of sensitive or confidential nature and is restricted from general distribution. Special authorization must be approved before access or limited access is granted.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.06 |
| | Policy Title: Security Information Data Classification Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

The identification of the type of information processed in a system is essential to properly select the kind of security controls and ensuring the confidentiality, integrity, and availability of the University system and its data.

This policy is intended to consistently map security impact levels to security type: 1) information (e.g., PII, financial, education) and 2) information systems (e.g., mission critical or support, administrative).

This policy is intended to identify and define the data classifications and assign the proper methods for ensuring sensitive information is handled according to the risk it poses to the organization. This process is a critical step in safeguarding the confidentiality, integrity, and availability of data to the University system.

This policy applies to all City University of Seattle users such as employees, contractors, faculty, and students and the resources they use.

## Security Information Data Classification Policy

Security categorization starts with the identification of what information supports University critical business objectives. Data classification is fundamental to comply to security standards and regulations such as PCI and GDPR.

Classifying information properly is paramount to enabling the University to proactively implement appropriate information security controls. This assessed potential negative impact to information confidentiality, integrity, and availability supports the University's mission in a cost-effective manner through these preventative measures.

## Classification of University Data

The University's data is classified into one of the following four categories:

1. Internal Restricted Data: Personal information, such as personally identifiable information (PII) or sensitive personal information (SPI), as defined by information security and privacy laws, is information that can be used on its own or with other information to identify, contact, or locate a single person. Such personal or confidential data is classified as Internal Restricted Data and is not for general distribution. Special authorization must be approved before access or limited access is granted. Loss, misuse, modification, or unauthorized access to sensitive information can adversely affect the privacy or welfare of an individual and the

overall reputation of City University of Seattle.

City University of Seattle complies with several information security standards, such as PCI-DSS and FERPA to safeguard this type of sensitive information.

2. Internal Protected Data: Internal protected data are any University data that are only available to staff with the required access in order to perform their assigned duties. Such data is not personally identifiable information (PII). This data must be protected as confidential.

   Examples of internal protected data include student learning outcomes data, end of course faculty evaluations, and university financial records

3. Internal General Data: Internal General Data are any University data that are used for administration activities and not for external distribution unless otherwise authorized.

   Examples of Internal General Data include employee directory information, student attendance rosters and admissions, student starts, and enrollment statistics.

4. Public Access Data (Non-Sensitive or Public Information): Data are classified as Public Access Data when the unauthorized disclosure of that data would result in little or no risk to City University of Seattle or its Affiliates.

   Examples of Public Access Data include press releases, course information, and research publications or University data distributed for the purpose of regulatory compliance. Controls are not required to protect the confidentiality of Public Access Data; however, some level of control is required to prevent unauthorized modification or destruction of Public Access Data.

Related Policy Statements

https://www.cityu.edu/privacy-policy/

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.07 |
| | Policy Title: Information Security Risk Management Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

This Policy describes the process used to perform security risk management within City University of Seattle Information Technology. The University uses the process documented in NIST Special Publication 800-39, Managing Information Security Risk, as the basis for its security risk management methodology.

The risk management process is encompassed within City University of Seattle Information Technology Lifecycle (ITL).

This policy applies to all Departments at City University of Seattle including users such as employees, contractors, faculty, and students engaging in systems or software development activities.

## CityU Information Technology Lifecycle (ITL)

The CityU Information Technology Lifecycle (ITL) describes the requirements for developing and/or implementing new software, new applications and new systems at City University of Seattle as well as ensure all development work is compliant with CityU policies, procedures, and guidelines. It is a comprehensive approach for evaluating the extent of potential threats, vulnerabilities, and security risk associated with an information technology (IT) system. The output of this process helps to identify appropriate controls for reducing and/or eliminating risks.

All Departments at the University engaged in systems or software development activities, must follow the IT Lifecycle.

At a minimum, the following must be performed to ensure software is properly documented and tested before it is used on critical and/or sensitive CityU systems:

1. Preliminary analysis or feasibility study
2. Risk identification and mitigation
3. Systems analysis
4. General design
5. Detail design
6. Development
7. Security review and architecture
8. Acceptance testing
9. Implementation
10. Post-implementation maintenance
11. Periodical internal security audit

## Information Security Risk Management Process

The Information Security Risk Management process includes the following four (4) stages.

1. Risk Framing: Risk framing involves the development of a risk management strategy that defines how the University identifies, assesses, mitigates and monitors risks. This strategy defines the following items:

    - Assumptions: the assumptions made during the risk assessment and risk treatment are identified so that the risk management results can be evaluated within their context.
    - Constraints: any constraints that limit risk assessment, risk measurement or mitigation are identified and addressed.
    - Tolerances: risk tolerances are defined and adhered to when making risk-based decisions.
    - Priorities and trade-offs: tradeoffs are made considering priorities of cost, risk mitigation and other factors.

2. Risk Assessment: Risk assessment is a key part of effective risk management in identifying and assessing a risk. This stage facilitates decision making at all three tiers in the risk management hierarchy including at the organizational level, mission/business process level, and information system level.
3. Risk Response: Risk response is the process for responding to security risks. The following University processes describe different courses of action depending on the nature of the risks being addressed:

    - Vulnerability management process: addresses risks associated with newly discovered vulnerabilities.
    - Incident response process: addresses risks occurring as the result of security incidents, adversary attacks, zero- day vulnerabilities and other security events
    - Business continuity process: addresses catastrophic failures.

    CityU mitigation procedures follow an established plan that identify an owner for each risk, a course of action for risk mitigation, and a due date for completing the mitigation. High risk items identified in the University security risk analysis are immediately addressed as part of the security incident response process.

4. Monitoring Risk: The risk monitoring process consists of the following elements:

    - Internal security assessment: The University reviews compliance with its policies and security standards (PCI DSSv3, FERPA, GLBA, GDPR) on a quarterly basis using internal security assessment audits.
    - External security assessment: The University performs an external audit of its compliance with its policies and security standards (PCI DSSv3.2.1) on a quarterly basis using a third-party certified report.
    - Security alerting process: The University reviews security alerts from US-CERT, Microsoft, Cisco, and other vendors daily and addresses potential threats and vulnerabilities via its vulnerability management process or incident response process, as appropriate.

- Security event monitoring process: The University reviews security events on a continual basis via its Security Information and Event Monitoring (SIEM) system.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.08 |
| | Policy Title: IT Change Management |
| | Prepared By: COO/CFO |
| | |

## Purpose

The purpose of the Change Management policy is to set out the guidelines for preventing security risks to changes made to the information processing environment.

## Scope

This policy applies to the City University of Seattle infrastructure, services that are hosted in this infrastructure, and the people that use, develop, maintain, manage, and support City University of Seattle Information Technology.

## Change Management Process

Types of security risks the University could be exposed to if the change management and change control procedures are not followed, include, but are not limited to:

- Security breaches and associated exposure to reputational risks;
- Information being corrupted and/or destroyed; and
- Systems availability and performance being disrupted and/or degraded.

Change Management prevents unintended consequences and reduces the security risks posed by changes to the information processing environment by ensuring appropriate authorization and accountability.

Change Management ensures that when all modifications are made, it is done systematically so that stakeholders, users, and administrators are consistently notified in advance.

All changes to City University of Seattle's IT architecture or systems, including installing a new IT resource in CityU production environment, as well as changes to existing configurations of systems, applications, and services are evaluated and follow the ITL process described in Policy XXX.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.09 |
| | Policy Title: Procurement and Vendor Security Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

The purpose of this policy is to identify security requirements for City University of Seattle technology procurement and supply chain security.

## Scope

These requirements apply to all vendors.

## Supply Chain Security Requirements

City University of Seattle Information Technology relies on a complex and interconnected vendor supply chain that consists of multiple layers of outsourced services and is geographically distributed. This vendor and service environment is composed of both public and private entities (e.g., acquirers, system integrators, suppliers, and external service providers) with technology, law, policy, procedures, and practices that interact to design, manufacture, distribute, deploy, and provide IT products and services.

The IT supply chain may introduce risks, including, but not limited to, counterfeit hardware and software, tampering, such as the insertion of malicious software and hardware, or poor manufacturing and development practices. These risks are associated with an organization's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services.

All employees attempting to acquire a technology-related product or service must request approval from the Information Technology Department.

The following security requirements apply to all technology products and services that are integrated into City University of Seattle infrastructure. A vendor assessment and a security review are mandatory for all the new application and software introduced into CityU networks.

1. Identification of Critical Components

   CityU IT reviews all CityU technology components and identifies those items that are critical to maintaining the security of the University. These technology products and services shall be designated as Critical

2. Tracing Origin of Critical Components

   CityU IT requires its vendors to identify the country of origin for the products and services offered for sale to CityU.

3. Information and Communication Technology Products and Services

   The US Department of State maintains a list of Designated Countries that pose some risk or threat to the United States (US Department of State Designated Countries) (as of Oct. 24, 2018 - see internal links for updates). Products or services that originate from one of these designated countries shall be assessed in terms of the risks of cyber-espionage or sabotage. Components or services that originate from one of these designated countries, but are not evaluated to be Critical Components, may be considered for purchase.

   Internet connectivity services should only be purchased from vendors who are listed by the U.S. General Services Administration as having undergone the Trusted Internet Connections (TIC) compliance validation process or who resell the services of TIC-compliant Internet service providers (TIC-compliant Internet Service Providers List).

4. Detection of Unwanted Features

   Prior to the purchase of a critical component or service whose country of origin is a US Department of State Designated Country, the Information Security Officer reviews the product or service to detect any undocumented or unwanted features that may compromise CityU infrastructure security.

5. Sharing of Information

   CityU IT requires its suppliers to share any information they obtain that identify any potential issues in supply chain security.

6. Component Lifecycle, Availability and Security Risks

   CityU IT requires that all technology components and services must operate within the security support period offered by their supplier, be available to the period forecasted by the University, and be replaced prior to the end of the supplier's support lifecycle. The security review of architecture components of the application/software is a mandatory requirement both:

   - at the time of the procurement of new hardware/software/application/service and
   - at least annually thereafter

   by the Information CityU IT Team to uncover potential security risks associated to security exposure of vulnerability exploits.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.10 |
| | Policy Title: Data Protection (DP) Policy-GDPR |
| | Prepared By: COO/CFO |
| | |

## Purpose

The purpose of this policy is to explain what rights EU citizens and other GDPR-protected individuals have regarding their personal data, how the University is using their data, and how it is processed and eventually deleted even if they are not in the country where the data is located.

This policy applies to all City University of Seattle students, faculty, clients, employees, contractors, suppliers, and partners.

## GDPR Statement

City University of Seattle is committed to the compliance, protection and privacy of personal data and is subject to the principles of the European Union's General Data Protection Regulation (GDPR). The GDPR establishes rules for the protection of natural persons regarding the processing of personal data and the free movement of such data. The GDPR protections are not limited to citizens of EU member countries. The GDPR defines the rights of all individuals whose information is collected in or processed within the EU. The GDPR includes the right to be forgotten, the right to know when personal data falls into the wrong hands and requires explicit consent (in certain cases) prior to processing personal information.

The Information Security Officer/Data Protection Officer has established objectives for data protection and privacy, which are contained in the Global Information Security and Privacy Program. The Data Protection Officer is responsible for reviewing the processing of personal data annually or when required by data protection impact assessments.

Partners and any third parties working with or for City University of Seattle, who have or may have access to personal data, must acknowledge and comply with this policy. No third party may access personal data held by City University of Seattle without first entering into a data confidentiality agreement and/or other applicable data protective agreements.

## Related Policy Statements

https://iso.nu.edu/NUS-EU-GDPR-Policy.html

https://www.cityu.edu/privacy-policy/

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.11 |
| | Policy Title: Vulnerability Management Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

The purpose of this document is to categorize the vulnerabilities in City University of Seattle information technology systems and resources as Critical, High, Medium, and Low risk in order to prevent the exploitation of information security weaknesses that exist within City University of Seattle.

## Scope

This policy applies to all information technology resources, including all City University of Seattle and City University of Seattle System owned, licensed, or managed hardware and software.

## Vulnerability Scan and Remediation

The goal of vulnerability management is to reduce the time and money spent dealing with vulnerabilities and any exploitation of those vulnerabilities. The vulnerability management process is executed on a monthly cycle. The Information Security Team performs specialized network scans of all City University of Seattle Internet Protocol (IP) addresses. Scan results are filtered to include only Critical, High and Medium risk vulnerabilities (as identified by the vulnerability tool). These are the only vulnerabilities addressed as part of this process.

The results of the vulnerability scans are prioritized by risk level and potential impact. Remediation of individual vulnerabilities may require IT staff or impacted users to implement new security controls, make configuration changes, and/or take additional measures to address the identified vulnerability. IT will continue to pursue appropriate technology solutions to address new information security threats and vulnerabilities, including zero-day threats for which there are currently no available remediation solutions.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.12 |
| | Policy Title: Red Flag Policy |
| | Prepared By: COO/CFO |
| | |

Purpose

The purpose of this policy is to demonstrate that City University of Seattle has implemented its Red Flag Program in order to ensure compliance with the Federal Trade Commission's Red Flag Rule regulation.

This policy applies to all users of information technology resources owned or managed by City University of Seattle and/or shared with National University.

Red Flag Rules

The Federal Trade Commission's Red Flag Program requires businesses and organizations to implement a written identity theft prevention program. The program is designed to detect the "red flags" of identity theft in day-to-day operations and take steps to prevent the crime and mitigate any damage. The program is designed to help businesses spot suspicious patterns of behavior and prevent the costly consequences of identity theft.

Identity theft is defined as fraud committed or attempted using the identifying information of another person without appropriate authority. Identifying information is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including, but not limited to:

- Name
- Address
- Telephone number
- Social Security number
- Date of birth
- Government-issued driver's license or identification number
- Alien registration number
- Government passport number
- Individual identification number
- Bank or other financial account routing code

When a change occurs to one or more items of a user's identifying information, the user is automatically notified of the change. If the user believes the change was unauthorized, they are encouraged to contact redflag@nusystem.org for more information.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.13 |
| | Policy Title: Incident Response (IR) Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

The purpose of this policy is to describe the plan and process by which City University of Seattle's Incident Response team responds to formalize the information security incident response capabilities and handling incidents efficiently and effectively at City University of Seattle.

## Scope

This policy applies to all users of information technology resources owned or managed by City University of Seattle. Individuals covered by this policy include all full-time and part-time employees, contingent workers including leased workers, independent contractors and service providers, faculty including staff and adjunct, students, alumni as well as all persons of interest (POI) including vendors, volunteers, guests, visitors and trustees, and any external individuals or organizations accessing University information technology resources.

## Incident Response (IR) Team

The City University of Seattle Core IT Incident Response Team includes the Director of IT, the COO/CFO, and ad-hoc Departmental representatives. The President services as ad hoc legal representation.

## Incident Response (IR) Plan and Process

Incident response is the process by which City University of Seattle investigates and manages information security incidents. Information security incidents include any events that are considered suspicious in nature. The incident response team investigates these suspicious events to determine whether the event is real and to contain and remediate the impact of the event as necessary.

The Incident Response process may include, but is not limited to the following steps:

1. Incident Documentation
2. Incident Communication and Escalation
3. Collection of Evidence
4. Containment
5. Termination
6. Eradication
7. Damage Assessment
8. Recovery
9. Breach Declaration

10. Breach Reporting
11. Incident Closure

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.14 |
| | Policy Title: Security Information and Event Management (SIEM) Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

The purpose of this policy is to describe how City University of Seattle utilizes Security Information and Event Management (SIEM) tools to identify inappropriate or unusual activity in its information technology resources and analyze such activity for vulnerabilities or risks in support of the university's Incident Response Policy.

This policy applies to all users of information technology resources owned or managed by City University of Seattle and the City University of Seattle System. Individuals covered by this policy include all full-time and part-time employees, contingent workers including leased workers, independent contractors and service providers, faculty including staff and adjunct, students, alumni as well as all persons of interest (POI} including vendors, volunteers, guests, visitors and trustees, and any external individuals or organizations accessing University information technology resources.

## SIEM Rules

City University of Seattle analyzes the vulnerability of scanning information, performance data, network monitoring, and system audit record (log) information using Security Information and Event Management (SIEM) tools. SIEM tools are a type of centralized logging software that can facilitate aggregation and consolidation of logs from multiple information system components.

The Network Administrator, in collaboration with the Director of IT, analyzes information security events reported by SIEM to determine whether they constitute a potential security incident. A security event is only re-classified as a security incident when it is determined the event requires further investigation. Once a security event is classified as a security incident, IT responds according to procedures identified in the Incident Response Process and Procedures.

Analysis of security events reported by the SIEM is required for the following reasons:

- Reported security events may be false positives
- Reported security events may be the result of authorized actions
- Reported security events may be used as a cover by an attacker for other attacks

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.15 |
| | Policy Title: Identity and Access Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

The purpose of this policy is to define access to technologies as well as outlining an approval procedure for university users to access protected information technology resources

## Scope

This policy applies to all university full-time and part-time employees, contingent workers including leased workers, independent contractors and service providers, faculty including staff and adjunct, students, alumni as well as all persons of interest {POI) including vendors, volunteers, guests, visitors, and trustees, and any external individuals or organizations accessing University information technology resources.

## Access Control Rules

Access to University data is governed by rules that encompass classification of data, user and employee roles and responsibilities in order to appropriately grant requests for authorization and access to specific data and technology resources. In general, usernames and passwords are used to provide access for users to assigned systems and software.

City University of Seattle has implemented Multi-Factor Authentication {MFA) in order to improve the security of the computer system login process. MFA requires the use of two or more security factors to authenticate a user. These factors will include a password and additional identifying information, often generated using one-time passcodes, hardware tokens, or smartphone apps, including, but not limited to Okta Verify and Google Authenticator.

University employees are required to use MFA when accessing information technology resources from a work or personal device and may choose to use one of the authenticator apps on their work or personal smartphone or similar device. When an employee is going to be terminated, both HR and IT Information Security must be notified in advance in order to perform the necessary following preventative actions:

1. Prepare appropriate documentation;
2. Protect University resources;
3. Minimize any potential security risks related to the termination of the employee
4. Complete tasks related to potential legal actions (maintain a chain of custody, perform digital forensics, remove access to sensitive systems); and
5. Ensure that all equipment is recovered, and all employee system access is completely removed.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.16 |
| | Policy Title: Remote Access Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

The purpose of this policy is to define the role of remote access technologies as well as outlining procedures for university employees and contractors to request remote access approval.

This policy applies to all university full-time and part-time employees, contingent workers including leased workers, independent contractors and service providers, faculty including staff and adjunct, students, alumni as well as all persons of interest (POI) including vendors, volunteers, guests, visitors, and trustees, and any external individuals or organizations accessing University information technology resources.

## Remote Access Rules

When authorized, City University of Seattle employees and contractors may use remote access technologies to perform work from non-university locations. Remote access technologies permit access to protected university resources from external networks. City University of Seattle employees and contractors are required to use only those remote access technologies approved by the Information Technology department and only with the approval of the Vice Chancellor Information Technology.

Remote access technologies must support several security objectives using a combination of security features within the remote access technology and security controls applied to the remote computer.

These security objectives include, but are not limited to, the following:

- Confidentiality: ensuring that remote access communications and stored user data cannot be read by unauthorized parties.
- Integrity: detecting any intentional or unintentional changes to remote access communications that occur in transit.
- Availability: ensuring that users can access resources through remote access whenever needed.

To achieve these objectives, all the components of remote access solutions, including client devices, remote access servers, and internal servers available via remote access, must be protected against information security threats.

These threats fall into the following four major categories:

1. Lack of physical security controls
2. Unsecured networks
3. Infected devices on internal networks

4. Unrestricted external access to internal resources

Remote access technologies address these threats by:

- Using Operating System (OS) and application security to hardening both endpoint workstations and servers.
- Requiring both multi-factor authentication and Virtual Private Network {VPN) authentication to protect internal services and resources.
- Requiring the use of VPNs that use cryptographic tunneling to encrypt the data flowing between the client device and the university resources.
- Requiring encryption of data at rest for critical systems and mobile computing devices.

Remote Access User Responsibilities

- Procure Internet Service Provider (ISP) connection.
- Ensure that unauthorized users are not allowed access to City University of Seattle's internal networks.
- Always use remote access in support of university business.
- Refrain from the unauthorized use of remote access technologies in order to access protected university information technology resources. Such use is strictly prohibited.
- Install and enable the network firewall feature on their remote workstations.
- Install and enable anti-malware software on their remote workstations.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.17 |
| | Policy Title: Bring Your Own Device (BYOD) Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

The purpose of this policy is to explain what is considered authorized or unauthorized use of personal computing devices while conducting university business.

## Scope

This policy applies to all university full-time and part-time employees, contingent workers including leased workers, independent contractors and service providers, faculty including staff and adjunct, students, alumni as well as all persons of interest (POI) including vendors, volunteers, guests, visitors, and trustees, and any external individuals or organizations accessing University information technology resources.

## BYOD Rules

Computing devices used to access university information technology resources that are not provided by the university, including, but not limited to desktop workstations, laptop computers, tablets, phones, and other mobile devices, represent a significant risk and are therefore subject to additional information security controls as defined in this Bring Your Own Device (BYOD) policy.

Industry-standard user authentication technologies make use of Multi-Factor Authentication (MFA) in order to improve the security of the computer system login process. MFA requires the use of additional identifying information, often generated by the use of one-time passcodes using tokens or smartphone apps, including, but not limited such tools as Microsoft Authenticator, Verify, and Google Authenticator. University employees are required to use MFA when accessing information technology resources from a personal device. They may choose to use one of the provided authenticator apps on their personal smartphone or similar device.

## Use of Personal Computing Devices for University Business

Employees are generally not required to use their personal computing devices to conduct university business. The use of personal computing devices for university business must be authorized by the employee's supervisor and approved by the Information Technology Department. Employees are provided with university equipment to conduct university business. If the employee is provided a computing device by the university, they must abide by all relevant IT use policies.

Employees are entitled to a reasonable percentage of their monthly invoice and/or data plans for personal computing devices such as smartphones. See Policy 4100.26 Cell Phone Policy and Approval

Form and Wi-Fi Reimbursement Procedure in HR Manual.

Ensuring Proper Security

For CityU, permitting teleworkers to access its internal network and computing resources remotely gives attackers additional opportunities to breach City University of Seattle's infrastructure. When a telework device uses remote access, it is essentially an extension of the University's own network. The same is true when a BYOD device is directly connected to the organization's local network. Therefore, if the telework device is not secured properly, it poses an additional risk not only to the information that the teleworker accesses but also to the organization's other systems and networks. For example, a telework device infected with a worm could spread it through remote access to the CityU' s internal systems. Therefore, telework devices must be secured properly and have their security maintained regularly.

## Verification

The IT Team will verify the security health of each telework device that attempts to use remote access to ensure that it complies with City University of Seattle's security policies, best practices guidelines. This verification is performed periodically or at least every quarter.

### Periodic System Checks

Examples of the checks performed by IT are verifying that a PC's OS is fully patched, antivirus software is installed and up-to-date, a personal firewall is enabled, or checking if a smartphone has been rooted or jailbroken. Some remote access solutions can also determine if the organization has secured the device and what type it is (e.g., desktop/laptop, smartphone, tablet). Based on the results of these checks, the device can be permitted for remote access.

### Periodic System Scans

Additionally, periodic vulnerability scans are performed by the Information Security Team on the City University of Seattle network in order to detect vulnerabilities. These scans help to provide better protection against security threats from personally connected devices.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.18 |
| | Policy Title: Email Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

The purpose of this policy is to ensure the proper use of the City University of Seattle e-mail system and make users aware of what the NU deems as acceptable and unacceptable use of its e-mail system.

## Scope

This policy applies to all full-time and part-time employees of City University of Seattle, including administrators, faculty and staff.

## E-mail Rules

If there is evidence that a user does not adhere to the guidelines set out in this policy, the University reserves the right to take disciplinary action, including termination and/or legal action. If the user has any questions or comments about this e-mail policy, he/she must contact their supervisor.

City University of Seattle reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

## Legal Risks

All messages distributed via the university's e-mail system, even personal e-mails, are City University of Seattle's property. This includes, but is not limited to, electronic: mail messages, calendar entries, contacts, and any other items stored on or sent through city U's e-mail systems. Therefore, it is important that users are aware of the potential legal risks of e-mail:

- If a user sends or forwards e-mails with any libelous, defamatory, offensive, racist or obscene remarks, the user and City University of Seattle can be held liable.
- If a user unlawfully forwards confidential information, the user and City University of Seattle can be held liable.
- If a user sends an attachment that contains a virus, the user and City University of Seattle can be held liable.

By following the guidelines in this policy, the e-mail user can minimize the legal risks involved in the use of e-mail. If any user disregards the rules set out in this e-mail policy, the user will be fully liable, and the University will disassociate itself from the user as far as legally possible.

Legal Requirements

The following rules are required by law and are to be strictly adhered to. It is prohibited to:

- Send or forward e-mails containing libelous, defamatory, offensive, racist or obscene remarks. If a user receives an e-mail of this nature, that user must promptly notify his/her supervisor.
- Send unsolicited e-mail messages or chain mail.
- Forge or attempt to forge e-mail messages, or illegitimately impersonate or attempt to disguise your identity when sending mail.
- Illegitimately send e-mail messages using another person's e-mail account.
- Inadvertent identification of group user members receiving confidential information or sensitive information (e.g., all external group e-mailings must have groups members in the "bcc" field to assure anonymity)
- Disclose, reproduce or distribute any e-mail distribution lists.

University-Wide Bulk E-mail Distribution

The IT department maintains several university-wide bulk electronic mail distribution lists, because of the potential strain to our electronic mail resources (depending on the size, frequency and number of recipients), and the potential for "spamming" or introducing "junk mail" to our e-mail users, these University-wide lists should be limited to extremely significant announcements and/or emergencies. The President's Office determines the appropriate venue for all City University of Seattle and external communications. In many cases, messages may be sent to more targeted audiences, posted on the public website, the mycityu.edu portal, or printed for distribution.

Guidelines for Bulk E-mail Distribution

- No attachments
- Brevity of the message is required
- Plain text only, with links in the message to more elaborate graphics
- An "opt out" capability must be included for the bulk mail message recipients
- The "opt out" list is managed by the list owner/bulk mail message sender
- No more than two hundred fifty (250} mass messages per day may be sent
- Bulk mail exceeding two hundred fifty (250) external domain names (other than NU.edu) should use a third party or outside vendor
- The message must be pre-approved by the Office of the President and/or VC of IT or his Delegated of Authority (DOA).

Personal Use

Although City University of Seattle's e-mail system is meant for business use, CityU allows personal usage if it is reasonable and does not interfere with work. However, note that all messages distributed via the university's e-mail system are the CityU' s property.

As such, no user should copy, resend or forward any City University of Seattle email to a private or personal account. without prior authorization from his/her Department's Headcount Authority.

External emails received from an email outside of the University are tagged in the subject with the

word "EXTERNAL" which means that the email originated from outside of the organization from an untrusted mail server. That will facilitate the users to identify emails that require more attention for phishing attempts and to contact the help desk.

## Privacy and Confidential Information

Never send any confidential information via e-mail with encryption. "Confidential Information" includes, but is not limited to, personal data such as names, addresses, phone numbers and social security numbers and information that can be identified as being about a specific person.

Users must have no expectation of privacy in anything that users create, store, send or receive on the university's e-mail system. User e-mails can be monitored without prior notification if CityU deems this necessary.

## System monitoring

Users expressly waive any right of privacy in anything they create, store, send or receive on the university resources. NU can, but is not obliged to, monitor e-mails without prior notification. If there is evidence that users are not adhering to the guidelines set out in this policy, CityU reserves the right to take disciplinary action, including termination and/or legal action.

## E-mail accounts

All e-mail accounts maintained on CityU e-mail systems are the property of City University of Seattle System. Passwords should not be given to other people.

Email accounts that have been determined as compromised will be deleted. Once an account has been deleted, it will no longer be retrievable.

## Passwords

Using passwords to gain access to the computer system or to secure specific files does not provide users with an expectation of privacy in the respective system or document.

## Encryption

Users that are sending confidential student or employee data (pii) are required to use the University licensed encryption program provided via their university accounts.

## Volume and Performance Issues

The performance and cost of electronic mail systems for all users can be adversely affected by inconsiderate use by individuals. Therefore, IT reserves the right to set limits on:

- The size of individual e-mail items sent and received.
- The total volume of e-mails sent and received.
- The amount of e-mail retained on central electronic mail servers.

## E-mail Archiving and Retention

City University of Seattle does not maintain central or distributed electronic mail archives of all e-mails sent or received. E- mail is normally backed up only to assure system integrity and reliability, not to provide for future retrieval, although back-ups may sometimes serve the latter purpose incidentally. IT operators of CityU's e-mail services are not required by this policy to retrieve e-mail from such back-up facilities or delegate privileges to any mailbox upon the holder's request unless authorized by the appropriate Division/Department Head.

Only the mail items stored on the CityU's e-mail server will be backed up. Any mail stored or archived on local desktop machines will not be backed up. It is the user's responsibility to back up any mail items stored on their local computers.

## SPAM

City University of Seattle makes every attempt to block and stop spam messages from reaching the users of its e-mail systems. However, it is impossible to block and stop all unsolicited e-mail messages. The System further reserves the right to block e-mail from specific mail domains to prevent further abuse of spam senders. Users are discouraged from posting their e-mail address on list-serves, website advertising or responding to on-line solicitations to provide their e-mail addresses. These practices significantly increase the volume of spam to the respective user e-mailbox.

| | |
|---|---|
| CityUniversity of Seattle | Revision Date: 7/1/2023 |
| | Policy #: 4200.19 |
| | Policy Title: Business Continuity Plan (BCPI) and Disaster Recovery Policy |
| | Prepared By: COO/CFO |
| | |

## Purpose

The purpose of a Business Continuity Plan (BCP) is to provide a written and tested plan directing the recovery process in the event of an interruption in continuous service resulting from an unplanned and unexpected disaster for both business operations and critical business systems.

## Business Continuity Plan

City University of Seattle, recognizing the need of their users to have a reliable point of contact and a continued high level of service, has developed this BCP. The plan recognizes the potential loss of revenue and operational control that may occur in the event of a disaster. The Continuity planning process as developed, authorizes the preparation, implementation, and maintenance of a comprehensive BCP.

The BCP preparation process includes the following steps:

- Identify key critical business processes that have the highest priority for recovery
- Identify the Systems and Applications currently in use
- Analyze the impact loss of critical systems or the location of business operations to these critical business units
- Identify the critical recovery time frames
- Determine a recovery strategy
- Document the Recovery Team organization
- Document Recovery Team Responsibilities
- Develop and Document Business Continuity emergency procedures
- Document the BCP training process
- Document the BCP maintenance process
- Train the Recovery Team

## Responsibilities

The Director of IT, under the supervision of the COO/CFO, assumes responsibility for the development, maintenance, and testing of the plan. All members of the Business Recovery Team will have the following responsibilities:

- Keep two (2) paper copies of the current plan (one at the office and a second in a secure offsite location)
- Keep an electronic copy on their work laptop
- Take their work laptop home every night

- Keep a mobile device with them 24/7
- Advise of any change in status that would prevent them from carrying out their duties during a Business Recovery event

## Key Plan Assumptions

This plan will be based on a strategy to recover all critical functionality to meet the business objectives. The following assumptions have been established as the basis for the development of the BCP:

The plan is designed to recover from the "worst case" destruction of City University of Seattle's service facility, which includes CityU offices and the primary data centers.

In case of loss to the primary data center, which serves CityU's users, the secondary data center is the only resource to recover operation equipment such as servers, networks, etc.

Equipment at the original data center is not expected to be salvageable and used for recovery.

This plan assumes that all business applications provided/maintained by CityU IT (Telephone system, email system, order management system, etc.) are covered by the IT Business Continuity Plans.

Key personnel will either work from home, from a location where they can reach the internet or will relocate to other City University of Seattle offices. In some cases, City University of Seattle may shift support of some critical functions to other teams and locations.

The plan assumes that, in the short term, key personnel will be able to access these systems from a remote location, giving them the ability to work anywhere that high speed internet and phone access (mobile or hard line) is available.

Key personnel will be required to have a University laptop, a paper copy of the BCP, and a phone with them at all times.

Although the plan is designed for the worst case, inherent in the plan strategy is the ability to recover up to the most minor interruption.

The plan is based upon the assumption that there will be ample key CityU staff members with the capacity to implement and affect recovery.

During the emergency, non-business critical operations will be suspended so that all resources are available to recover existing critical business operations.