INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICIES AND PROCEDURES MANUAL

TABLE OF CONTENTS

I. INTRODUCTION

This Information and Communication Technology (ICT) Policies and Procedures Manual has been developed as a guide towards providing a uniform understanding in the interpretation and administration of information technology matters in City College of Cagayan de Oro. Recognizing the significance of ICT in facilitating teaching, learning, and administrative processes, the City College of Cagayan de Oro is proud to present its ICT Policies and Procedures Manual. This manual serves as a comprehensive guide outlining the principles, guidelines, and protocols governing the use of ICT resources within the college community. It is one of the management concepts to establish a well-organized both external and internal control system that can contribute to productivity, accessibility, and IT capability organization through ICT.

With a commitment to promoting responsible and ethical ICT practices, these manuals address key areas such as network security, data privacy, acceptable use policies, and disaster recovery procedures. By establishing clear guidelines and protocols, the manual aims to ensure the integrity, confidentiality, and availability of digital resources, safeguarding sensitive information, and promoting a safe and secure computing environment for all users.

The faculty, staff and students of City College of Cagayan de Oro allows to use and access the computer and network resources to assist them in carrying out their work duties and responsibilities, that the institution expects that these resources be used for purposes related to their jobs and may not be used for unrelated purposes that can lead to lost and damages. These resources include all the Institution owned computer devices, licensed both hardware and software, and the use of the institution's network via physical and wireless connection. The purpose of this manual is to ensure that the users of the computer devices will provide betterment of achieving good performance to their work, to promote efficient, ethical and lawful use of the Institution's computer and network resources.

Furthermore, this manual also serves as a reference tool for students, faculty, staff, and administrators, providing clarity on ICT-related policies and procedures and promoting consistency in their implementation across all departments and units. It reflects the City College's dedication to fostering a culture of accountability, transparency, and continuous improvement in the management and utilization of ICT resources.

II. INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) POLICIES AND PROCEDURES MANUAL OBJECTIVES:

The following are the objectives of the manual:

1. Provide guidelines for the conditions of acceptance and appropriate use of the computer and network resources.
2. Ensure that the ICT resources are in an appropriate approach for security, accessibility and availability to users that support the Institution's mission and vision and goal.
3. Encourage users to understand their responsibilities for securing the Institutions ICT resources.
4. To protect the privacy and integrity of data stored on the Institutions network.
5. To establish good performance with the right usage of the ICT resources.
6. Enable the users to be vigilant and aware of any circumstances that may occur to the hardware and software.
7. To define the policies and guidelines for the staff of City College of Cagayan de Oro the utilization of the ICT resources.
8. To use the ICT in increasing the institute's efficiency and effectively deliver improved services to its employees.
9. Provides clear and comprehensive guidance on how to use ICT resources, including procedures for accessing and using systems, troubleshooting common issues, and obtaining support when needed.
10. To define the policies and procedures related to acceptable use, including guidelines for proper conduct, respectful communication, and responsible data management.

By achieving these objectives, the ICT Policies and Procedures Manual can help organizations to establish a clear, consistent, and effective approach to the use of ICT resources, which can lead to increased security, efficiency, and productivity to City College of Cagayan de Oro.

III. SCOPE OF THE POLICY

This policy applies to all City College of Cagayan de Oro faculty, staff and students as ICT Users. It also covers all Information Communication and Technology equipment, network resources and services (both hardware and software) that are owned by City College of Cagayan de Oro.

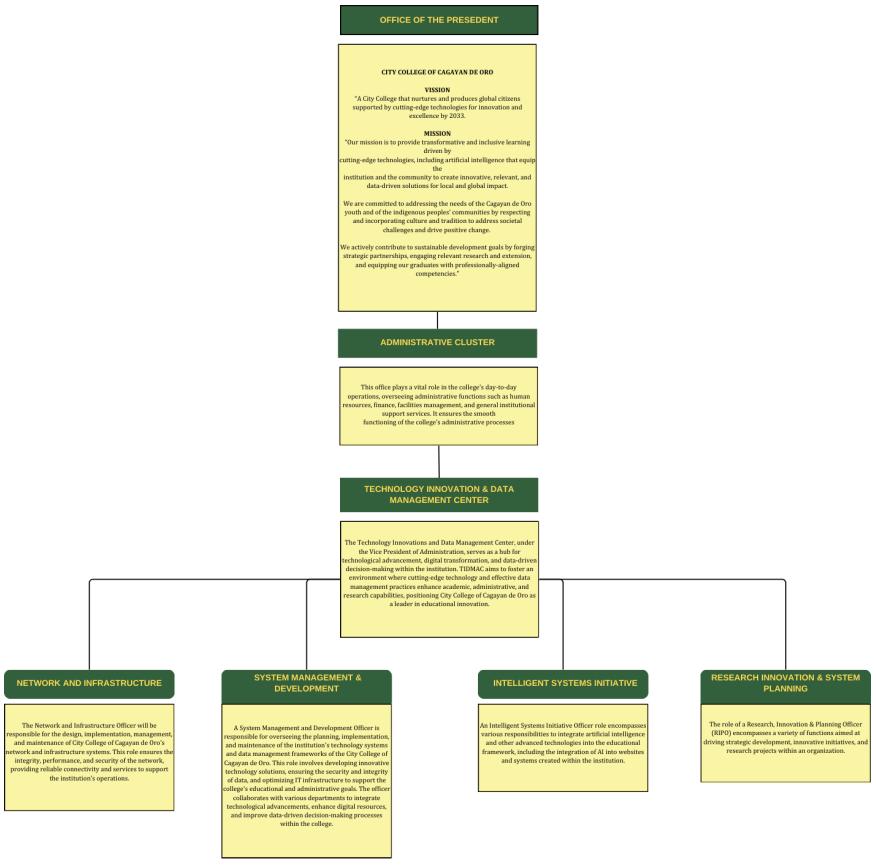
City College of Cagayan de Oro employees must be aware that the data created on any request forms, and data stored on any devices remains the property of City College of Cagayan de Oro.

ICT equipment includes:

- Laptops and Computers,
- Data storage devices and media,
- All software and applications installed,
- Network switches, router, and switches,
- Network cables
- Networking tools and equipment
- City College of Cagayan de Oro System
    - School Management System
    - School Website

IV. RESPONSIBILITIES AND OBLIGATIONS

ICT resources and faculty, staff & students have a range of responsibilities and obligations to ensure the effective, secure, and compliant use of ICT resources. These duties include security, maintenance and upgrades, backup and recovery, user support, acceptable use, compliance, reporting issues, training and awareness, password management, data management, and refraining from prohibited activities. By fulfilling these responsibilities and obligations, the institution can ensure the optimal use and protection of their ICT resources.



ICT HARDWARE AND SOFTWARE POLICIES AND GUIDELINES

1. INTERNET USAGE POLICY

This policy is to define the appropriate usage of the Internet by City College of Cagayan de Oro employees.

POLICY STATEMENTS

a.) Employees should always know how to check the URL first of the website before clicking if it is HTTPS to avoid computer malware.

b.) Employees are not allowed to download unnecessary applications or programs and play games using the unit or device.

c.) Employees should restrict or block unnecessary websites (e.g., pornographic, gambling, streaming etc.).

d.) Electronic mail exchanged via the Office Internet should not include any offensive and/or harmful content. Such content involves language and imagery that could be considered as harassment or vulgarity.

e.) Employees should not install inappropriate software that could be harmful to the device and network.

f.) Employees should not steal, using, or disclosing someone else's password without authorization.

g.) Employees should not use the computer and/or laptop to perpetrate any form of fraud, software, film or music piracy.

h.) Employees should not use computers and/or laptops for hacking into unauthorized websites.

i.) Employees should not use the internet to send offensive or harassing material to others.

j.) Employees must not download movies or music and other unpermitted pockets.

k.) **Purpose of Internet Access:**

- Internet Access is provided primarily for educational and professional purposes. All users are expected to use the internet responsibly, in a manner consistent with the College's mission and vision.

l.) **Network Resource Management:**

- This policy applies to all faculty, staff, students, and authorized users who access the City College of Cagayan de Oro's network resources, including wired and wireless

networks, internet access, and related services.

a. **Access Control**
   Network access is restricted to authorized users who have been granted appropriate permissions.
b. **Network Usage**
   Network resources are provided primarily for academic and administrative purposes. Personal use is permitted but should not interfere with institutional activities or violate any policies
c. **Security Measures**
   The TIDMAC department will implement and maintain robust security measures, including firewalls, intrusion detection systems, and encryption protocols, to protect the network.
d. **Data Protection**
   All data transmitted over the network must be encrypted using secure protocols to protect against interception and unauthorized access. Users are responsible for safeguarding their passwords and must not share them with others.
e. **Network Performance Management**
   The TIDMAC department will monitor network usage and performance to ensure optimal operation and to prevent congestion. Bandwidth-intensive activities that are not related to academic or administrative functions may be restricted during peak usage times
f. **Incident Response**
   Any suspected network security incidents or breaches must be reported immediately to the IT department. The IT department will investigate reported

incidents and take appropriate actions to mitigate any threats.

2. SAFEGUARDING PASSWORD POLICY

The overall objective of this policy is to establish a standard for the secure use and protection of all work-related passwords of City College of Cagayan de Oro (e.g., Biometric System password, Wi-Fi password, Network IP password).

POLICY STATEMENTS

a.) Employees are allowed to use authorized, approved password managers to store and manage all their work-related passwords securely.

b.) Employees must use a separate, unique password for each of their work-related accounts. Users may not use any work-related passwords for their own, personal accounts.

c.) A password must contain the following characteristics:

- Be at least eight (8) characters.
- Contain upper- and lower-case character at least with numbers and punctuations
- Must not be found in a dictionary or be a common slang word.
- Must not be a computer term, name, program, site, company name etc.
- Must not be name, birthday, phone number, or other personal information.
- Must not use word or number patterns such as aaabbb, qwerty, , zxywvuts, 123456, etc.
- Must not use any of the above spelled backward.
- Must not use any of the above proceeds or follow by a digit (e.g., secret1, 1secret, secret2, 2secret, etc.)

d.) All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months.

e.) Multi-factor authentication is highly encouraged and should be used whenever possible, not only for work-related accounts but personal accounts also

f.) Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.

g.) IT Personnel must Secure Network gateway and password to prevent Network attacks.

h.) ICT Personnel must Use WPA2 for password configuration in routers to ensure that data sent or received over your wireless network is encrypted, and only employees with the network password have access to it.
i.) Do not use the "Remember Password" feature of applications (for example, web browsers).

j.) Employees suspecting that their password may have been compromised must report the incident and change all relevant passwords.
k.) Secure CCTV System password.
l.) Passwords must not be shared with unauthorized employees, all passwords are to be treated as sensitive, Confidential information.
m.) Employees must not share the network password to anyone to avoid multiple users that might cause disconnection and slow connection.
n.) Passwords should not be written down on paper or stored on any computer/laptop.

3. WIRELESS NETWORK USAGE POLICY

The purpose of this policy is to inform the City College of Cagayan de Oro staff and students of the acceptable use regulations related to installed wireless networks. This policy has been put in place to protect the personnel, faculty, and students and to prevent inappropriate use of wireless network access that may expose Data to multiple risks including viruses, network attacks, and various administrative and legal issues.

POLICY STATEMENTS

a.) Employees may not extend or modify the network in any way. This includes adding access points and installing bridges, switches, hubs, or repeaters. Only the ICT personnel has the reserved right to remove or disable any unauthorized access points.
b.) Running any unauthorized data packet collection programs on the wireless network is prohibited. Such practices are a violation of privacy and constitute the theft of user data.
c.) Employees must not share Wi-Fi passwords with any unauthorized personnel.
d.) Any attempt to break into or gain unauthorized access to any computer or system from a wireless connection is prohibited.

4. ICT EQUIPMENT AND TOOLS BORROW POLICY

The purpose of this policy is to establish preventive measures to maintain and minimize the probability of losing and damaging the ICT equipment and tools that are used by the City College of Cagayan de Oro Employees. This policy
focuses on the circumstances of securing the functionality and availability of the equipment and tools.

POLICY STATEMENTS

a.) Employees must seek permission first before borrowing the equipment and tools.
b.) Employees only borrow necessary equipment or tools for work relations.
c.) Employees should return the borrowed equipment and tools at the exact time and date.
d.) Employees should not exchange to co-worker the borrowed equipment and tools to avoid loss and confusion.
e.) Equipment and tools must be in good condition upon returning.
f.) All ICT equipment and tools must be stored in cool and dry areas.

5. CLEAN DESK POLICY

5.1 OBJECTIVE

The purpose for this policy is to establish the minimum requirements for maintaining a "clean desk" – where sensitive/critical information about our employees, our intellectual property is secure in locked areas and out of sight.

5.2 POLICY STATEMENTS

a.) Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
b.) Computer workstations must be locked when the workspace is unoccupied.
c.) Computer workstations must be shut completely down at the end of the work day.

d.) Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the work day.
e.) File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
f.) Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
g.) Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
h.) Employees are responsible for protecting the confidentiality of any documents or information they work with and should take measures to ensure that sensitive information is not visible to unauthorized personnel.

6. REMOVABLE MEDIA POLICY

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by City College of Cagayan de Oro and to reduce the risk of acquiring malware infections on computers.

POLICY STATEMENTS

a.) Employees may only use City College of Cagayan de Oro removable media in their work computers.
b.) Employees must not download or install any applications on City College of Cagayan de Oro removable media that are not related to work.
c.) Eject flash drive "click eject flash drive icon" before removing removable media.
d.) IT Personnel should check every borrowed removable media disk to ensure the functionality and to avoid any viruses and/or malware that may occur.
e.) Employees who suspect any malware problem should seek assistance to the IT Personnel.
f.) Employees must not share their removable media devices with other employees without the proper authorization.

7. BIOMETRIC USAGE POLICY

The purpose of this policy is to ensure an efficient way of approach to the collection of information to City College of Cagayan de Oro Employees and handling the biometrics with proper usage, to keep it in good condition and functionality.

POLICY STATEMENTS

a.) Employees must be in dry hands before using the biometric to ensure the functionality of the device.
b.) Employees who have difficulty using the device should seek assistance from the IT personnel.
c.) Biometric data must be stored, transmitted and protected using reasonable standard care by the IT personnel.
d.) Only the IT personnel are authorized to access the biometric data.
e.) Unauthorized employees are prohibited in opening biometric systems.
f.) Unauthorized employees should not change the date and time to the connected computer device of the Biometric system.

8. SOFTWARE INSTALLATION POLICY

The purpose of this policy is to ensure that the City College of Cagayan de Oro Employees understands and agrees to abide by specific guidelines for software, program and application installation and use on every division provided-computers and/or laptops, systems and networks. This is to minimize the risk of program functionality, the exposure of sensitive data information contained within the computer network, the risk of introducing malware and the legal exposure of running illegally unlicensed software.

POLICY STATEMENTS

a.) Employees are prohibited from installing any software programs and applications, including software purchase for personal use.
b.) Under no circumstances are users to downloads, install, copy, access, execute or otherwise employ any of the following:
- Illegal software, applications and programs

- Unlicensed applications
- Unlicensed operating system(cracked)
- Software purchased for personal or home use.

c.) Employees should not install applications/software on City College of Cagayan de Oro computer devices.

d.) Employees who are requesting to install applications related to work matters must seek authorization first to the IT Personnel or Head administration.

e.) ICT Personnel should always check the computer device applications, files and other crucial content that is installed.

f.) Employees are prohibited from installing any kind of "games" on the computer device.

9. ELECTRONIC SIGNATURE GUIDELINES

The purpose of this policy is to establish the process of designating transactions that can legally accept electronic signatures to signify agreement or approval. This will increase the effectiveness and efficiency of City College of Cagayan de Oro operations, on paper works, online applications, etc., and avoid unnecessary problems from peers.

POLICY STATEMENTS

a.) Employees who use the electronic signature must seek authorization from the IT Personnel or Administration as it will be attached to a document.

b.) Employees should not use another person's electronic signature without permission.

c.) Employees' first and last names must be visible and legible below the electronic signature.

d.) Employees who use another person's electronic signature will face consequences.

e.) Electronic Signature will only be used as a permit for any essential documents related to work.

10. PRINTER POLICY

The purpose of this policy is to ensure the functionality that gives efficient, cost-effective use of printing and copying assets. Also to facilitate an appropriate and acceptable use of all the printing devices in City College of Cagayan de Oro, to maintain in good condition.

POLICY STATEMENTS

a.) IT Personnel must maintain the maintenance for nozzle check, head cleaning and other printing properties.
b.) Waste Ink must be checked by IT Personnel at every end of the month.
c.) Avoid printing large files, as this puts a drain on network resources and interferes with the ability of others to use the printer. Report any planned bulk print jobs to the IT Personnel so that the most appropriate printer can be selected and other users can be notified.
d.) Printer Maintenance:
- Report any printer malfunctions or issues to the IT department immediately.
- Do not attempt to fix or modify printers on your own.
- Use only approved toner cartridges, paper, and other supplies.
- Clean printers regularly to prevent dust and debris build-up.

e.) Employees should seek assistance to the IT personnel upon connecting personal computers and laptops.
f.) Employees should not leave printed documents unattended at the printer.
g.) Employees must dispose of confidential printed documents securely.

11. MOBILE POLICY

This policy aims to ensure the secure, efficient, and responsible use of mobile technology by faculty, and staff. By doing so, the college seeks to protect sensitive information, enhance productivity, and maintain a conducive learning and working environment.

POLICY STATEMENT:

a. All issued mobile phones for communications are strictly designated for official use only as mandated by the office; any form of personal or unofficial use is strictly prohibited.
- **Exclusive Gmail Account**: All mobile phones used within the office are mandated to operate under a singular Gmail account.
- **Shared Visibility**: It is imperative to acknowledge that any transactions,

downloads, or subscriptions made on one mobile phone will be visible to all other devices linked to the shared Gmail account.

- **Heightened Accountability:** This shared visibility enforces a heightened level of accountability, ensuring transparency and awareness of all mobile activities across the designated devices.

b. Devices must remain within the office premises at all times and are explicitly forbidden from being taken home by any staff without permission; assign a specific, secured location for each device within the office premises.
c. Rigorously adhere to proper handling and safekeeping protocols, with an uncompromising commitment to responsible charging practices.
d. Mobilize mobile data only when necessary, exercising extreme caution to minimize data consumption.
e. The assigned numbers are exclusively for official communication within the designated offices, with a zero-tolerance policy for any external transactions.
f. Strict compliance with these guidelines is non-negotiable, and any failure to adhere will result in immediate and stringent administrative sanctions.

EDUCATION TECHNOLOGY LABORATORY MANUAL

This section outlines the general rules and expectations for laboratory users, guidelines for the proper use of equipment and resources, safety guidelines and precautions, compliance with relevant institutional policies and regulations, best internet practices, and considerations for confidentiality and data privacy. Please familiarize yourself with these guidelines to ensure a productive, secure, and responsible environment for all.

ICT LABORATORY GUIDELINES AND POLICIES

General Rules and Expectations for Laboratory Users

· Respect the laboratory space and maintain a quiet and conducive environment for learning.

· Follow the instructions provided by laboratory staff and instructors.

· Keep your personal belongings secure and avoid leaving them unattended.

· Observe proper conduct and engage in responsible and respectful behavior toward fellow students and staff.

Guidelines for the Proper Use of Equipment and Resources

· Use the laboratory computers and equipment solely for academic purposes.

· Do not tamper with or attempt to dismantle any equipment without authorization.

· Refrain from installing unauthorized software or making alterations to the system configuration.

· Report any equipment malfunctions or issues to the laboratory staff immediately. Safety Guidelines and Precautions

· Familiarize yourself with the emergency procedures and exits in the laboratory.

· Keep aisles and workstations clear of obstructions to ensure easy access and movement.

· Adhere to health safety protocols, including the use and wearing of protective equipment when necessary or required.

· Practice internet safety by avoiding suspicious websites, practicing safe browsing habits, and being vigilant against phishing attempts, malware, and social engineering incidents.

Compliance with Relevant Institutional Policies and Regulations

· Lock your workstation or log out when taking a break or leaving the laboratory.

· Turn off the computer system after use to conserve energy and resources.

· Use the laboratory computers and software solely for academic purposes.

· Do not install unauthorized programs or uninstall authorized programs without permission.

· Refrain from unauthorized troubleshooting or making changes to system settings.

· Report any concerns or issues regarding antivirus software to the laboratory staff.

· The laboratory staff will be responsible for updating antivirus programs and performing system scans to ensure cybersecurity.

· Avoid bringing food or beverages inside the laboratory to maintain cleanliness.

· Adhere to known computer etiquette, such as locking the workstation during breaks and shutting down the system when not in use.

· Respect the confidentiality and data privacy of fellow students and the institution.

Best Internet Practices

· Keep your operating system and software up to date with the latest security patches.

· Use strong and unique passwords for all accounts and enable two-factor authentication where available.

· Be cautious when sharing personal information online and avoid disclosing sensitive data to unknown or untrusted sources.

· Regularly backup important files and data to protect against data loss or ransomware attacks.

· Be vigilant against phishing attempts, suspicious links, and email attachments from unknown sources.

· Use reputable antivirus software and keep it updated to safeguard against malware and other cyber threats.

Confidentiality and Data Privacy Considerations

· Respect the confidentiality of fellow students' files, data, and personal information.

· Refrain from accessing, modifying, or sharing confidential or sensitive information without proper authorization.

· Be mindful of the institution's data privacy policies and adhere to them when handling personal or sensitive data.

· Report any suspected data breaches or confidentiality incidents to the appropriate authorities.

Personal Protective Equipment (PPE) for the ICT Laboratory:

· **Anti-Static Wrist Trap**: An electrostatic discharge (ESD), is a safety device used to prevent the buildup of static electricity on a person's body, which can damage sensitive electronic computer components when handling and assembling.

· **Anti-Static Mat**: An electrostatic discharge (ESD), is a protective device designed to safely dissipate static electricity. These mats are commonly used in areas where sensitive electronic components are handled, such as electronics assembly lines, repair stations, and computer laboratories.

· **Safety Goggles**: Safety goggles protect your eyes from potential hazards such as flying debris, chemicals, or accidental splashes. They should be worn whenever working with equipment, chemicals, or any activity that poses a risk to the eyes.


· **Closed-Toe Shoes**: Closed-toe shoes protect your feet from hazards like falling objects or electrical accidents. They help prevent injuries such as cuts, bruises, or burns. Choose comfortable shoes that have non-slip soles and offer good support.

· **Noise-Cancelling Headphones**: Specialized headphones designed to reduce unwanted ambient sounds using active noise control (ANC). This technology is particularly useful in noisy environments, allowing users to enjoy clearer audio without needing to increase the volume excessively.

· **Gloves**: Depending on the activities and materials used in the ICT laboratory, different types of gloves may be required:

· **Insulated Gloves**: also known as electrical safety gloves, are a type of protective gear worn to handle electrical equipment where there is a risk or electrical shock. These gloves are designed to provide insulation against electrical current and protect the wearer from electrical hazards.

· **Anti-static Gloves**: Anti-static gloves are used when working with sensitive electronic components to prevent static electricity discharge, which can damage the components.

· **Anti-vibration gloves**: To reduce the transmission of vibration from tools and equipment to the hands and arms of the wearer. This is use for equipment that may cause discomfort or potential health issues.

EMERGENCY PROCEDURE IN THE ICT LABORATORY

The ICT lab is a dynamic environment where emergencies, though rare, can occur. It is crucial to be prepared and knowledgeable about the appropriate actions to take in case of an emergency. Please familiarize yourself with the following procedures for various situations:

Fire Emergency

- Immediately alert others in the lab by shouting "Fire!" and activating the nearest fire alarm pull station.
- Evacuate the lab calmly and quickly, following the designated evacuation routes.
- Close doors behind you to prevent the spread of fire.
- Avoid using elevators and use the nearest stairs to exit the building.
- Once outside, move to a safe location at a considerable distance from the building.
- Call emergency services (fire department) to report the fire and provide relevant information.
- Do not re-enter the lab until it is declared safe by authorities.

Electrical Malfunction or Shock

- In the event of an electrical malfunction or shock, immediately disconnect the power supply by turning off the main switch or unplugging the equipment, if safe to do so.
- If someone is experiencing an electric shock, do not touch them directly. Instead, tur n off the power source or use a non-conductive object to separate them from the electricity source.
- Call for medical assistance if necessary.
- Inform the laboratory supervisor or instructor about the incident for further guidance and investigation.

Medical Emergency

- If someone in the lab experiences a medical emergency, call for emergency medical services immediately.
- Provide necessary first aid or basic life support if trained and if it is safe to do so.
- Clear the area around the affected person to allow medical professionals to provide assistance.
- Notify the laboratory supervisor or instructor about the incident for documentation and follow-up actions.

Other Emergencies (Natural Disasters, Security Threats, etc.)

- Follow instructions provided by the laboratory supervisor or instructor regarding specific emergency situations such as earthquakes, severe weather conditions, or security threats.
- Stay calm and follow the designated procedures for each type of emergency.
- Seek shelter in designated safe areas as instructed.
- Communicate with emergency services if necessary and provide relevant information.

ACCESS AND SECURITY

Access and security are fundamental aspects of the ICT laboratory. This section provides guidelines and procedures to ensure authorized access, protect equipment and resources, and maintain a secure environment.

Accessing the ICT Laboratory

- Obtain proper authorization from the laboratory supervisor or instructor before entering the lab.
- Present your valid student identification card or any required access credentials for verification.
- Follow any additional access procedures specified by the institution or department.

Security Measures

- Only authorized individuals are allowed entry into the lab premises.
- Security cameras are in place to monitor activities and deter unauthorized access.
- Restricted areas within the lab may require additional authorization or supervision.
- Report any suspicious activities or unauthorized access immediately.

Responsibilities of Users

- Do not share access credentials with others or allow unauthorized individuals to enter the lab.
- Maintain the confidentiality and security of personal accounts and data.
- Keep personal belongings secure and avoid leaving them unattended.
- Promptly report any security concerns or vulnerabilities to the laboratory staff.

Reporting Unauthorized Access or Suspicious Activities

- Report any unauthorized access or suspicious activities to the laboratory staff or supervisor.
- Provide specific details of the incident, including date, time, and a description of the individuals involved (if known).
- Cooperate with security investigations to maintain a secure environment.

EQUIPMENT AND RESOURCES

The ICT laboratory is equipped with various resources to support your academic endeavors. This section provides an overview of the available equipment and resources, guidelines for their proper usage and care, and procedures for reporting any issues or damages.

Overview of Equipment and Resources

- The ICT laboratory provides computers, software, peripherals, and other relevant equipment for academic use.
- Specific guidelines for using different types of equipment will be provided by the laboratory staff or instructor.

Proper Handling and Care

- Handle equipment with care and respect, ensuring proper usage and storage.
- Follow any instructions provided for specific equipment, such as printers, scanners, or specialized devices.
- Avoid exposing equipment to liquids, excessive heat, or other potential sources of damage.

Reporting Damages or Malfunctions

- Report any damages, breakages, or malfunctions of equipment to the laboratory staff immediately.
- Provide detailed information about the issue, including the nature of the problem and any error messages displayed.
- Do not attempt to repair equipment unless authorized to do so.

ACCOUNTABILITY AND PENALTIES

Accountability is essential for maintaining a responsible and productive learning environment in the ICT laboratory. This section outlines the individual

responsibilities of users, the penalties for misuse or violations, and the procedures for reporting incidents and appealing disciplinary actions.

Individual Accountability

- Users are personally responsible for the equipment and resources assigned to them.
- Do not share personal accounts, passwords, or access credentials with others.
- Adhere to the acceptable use policy and relevant institutional regulations.

Penalties for Misuse or Violations

- Misuse, damage, theft, or unauthorized use of equipment or resources may result in disciplinary actions.
- Penalties may include warnings, fines, temporary suspension of access, or other appropriate measures as outlined in the student handbook or institutional policies.

Reporting Incidents and Consequences

- Report any incidents of misuse, violations, or suspected violations to the laboratory staff or supervisor.
- Provide accurate information and cooperate with investigations.
- Consequences of violations will be determined based on the severity of the offense and in accordance with institutional policies.

Disciplinary Actions and Appeal Procedures

- Users have the right to appeal any disciplinary actions taken against them.
- Follow the appeal procedures specified in the student handbook or institutional policies.
- Appeals will be reviewed and considered by the appropriate authorities.

BREAKAGE AND DAMAGE

In the event of equipment breakage or damage, prompt reporting and appropriate actions are necessary. This section provides procedures for reporting damages, evaluating the extent of the damage, arranging repairs, and addressing repair costs.

Reporting Procedures

- Report any damages or breakages of equipment to the laboratory staff immediately.
- Provide accurate details about the incident, including the equipment involved and the circumstances leading to the damage.

Evaluation Process

- The laboratory staff will assess the extent of the damage and determine the necessary steps for repair.
- Evaluation may include physical examination, diagnostic tests, or consultation with technical staff or service providers.
- Repair procedures and costs:

The Laboratory Staff or Technical Experts Will Handle the Repair Process

- Repair costs and responsibility will be determined based on the circumstances of the damage.
- Users may be held accountable for repair costs in cases of misuse, negligence,or unauthorized actions.

Alternative Procedures (if applicable)

- In situations where immediate repair is not feasible, alternative procedures or arrangements may be provided.
- These alternatives will be communicated to users to minimize disruption and ensure continued access to necessary resources.

PREVENTIVE MEASURES

Preventive measures play a crucial role in maintaining the functionality and longevity of equipment and resources in the ICT laboratory. This section provides guidelines for preventive maintenance, proper storage and handling practices, training sessions, and user education.

Preventive Maintenance

- Regular preventive maintenance activities will be scheduled by the laboratory staff or technical team.
- Follow any instructions or guidelines provided for backing up data, cleaning equipment, or updating software.

Proper Storage and Handling

- Store equipment in designated areas when not in use, following specific instructions if applicable.

- Avoid exposure to extreme temperatures, humidity, or other potential sources of damage.
- Handle equipment with care and caution to prevent accidents or breakages.

Training Sessions and User Education

- Training sessions will be conducted to familiarize users with equipment, software, and safety protocols.
- Stay updated with relevant training materials, guides, or resources provided by the laboratory staff or institution.
- Participate actively in workshops or awareness programs to enhance your knowledge and skills.

FEEDBACK AND SUGGESTIONS

Feedback and suggestions from users are valuable in improving the ICT laboratory's services, resources, and overall experience. This section provides channels for users to provide feedback, make suggestions, and contribute to the continuous improvement of the laboratory's offerings.

Providing Feedback and Suggestions

- Users are encouraged to provide feedback, suggestions, or comments regarding the ICT laboratory's facilities, services, or resources.
- Use the designated feedback channels, such as suggestion boxes, online forms, or email, to share your input.

Consideration and Evaluation

- Feedback and suggestions will be reviewed and evaluated by the laboratory staff or relevant authorities.
- Constructive input will be considered for potential improvements or future enhancements.

Acknowledgment and Response

- Depending on the nature of the feedback or suggestion, users may receive acknowledgment or a response regarding the actions taken.
- Not all suggestions may be implemented immediately, but they will be duly considered for future planning and development.

SPEECH LABORATORY MANUAL

The Speech Laboratory serves as a dedicated space where students, faculty, and staff can enhance their speech and language skills, refine their communication techniques, and gain confidence in public speaking.

The primary purpose of the Speech Laboratory is to provide a supportive and immersive environment for individuals to develop their oral communication abilities. Whether you are preparing for presentations, improving pronunciation, working on speech clarity, or refining public speaking skills, the Speech Laboratory offers a wide range of services and resources to meet your needs.

- Enhancing Speech Production: The laboratory aims to improve speech production by offering tools, exercises, and practice opportunities for pronunciation, articulation, voice projection, and intonation.
- Developing Effective Communication Skills: The laboratory focuses on fostering effective verbal and nonverbal communication skills, active listening, and engaging interpersonal interactions.
- Building Confidence in Public Speaking: The laboratory provides opportunities for individuals to develop confidence, poise, and effective delivery techniques in public speaking through practice sessions, simulations, and constructive feedback.

The Speech Laboratory offers a range of services and resources to support your speech and communication goals.

These include:

- **Recording and Playback Facilities**: Individual recording stations equipped with high-quality microphones, recording devices, and playback systems allow you to record, review, and analyze your speeches, presentations, or practice sessions.
- **Speech Analysis Tools**: The laboratory provides access to specialized software and resources for analyzing speech patterns, identifying areas for improvement, and tracking progress over time.
- **Communication Workshops and Consultations**: The laboratory offers workshops and one-on-one consultations with experienced speech and communication professionals who can provide personalized guidance, feedback, and coaching.
- **Self-Study Materials:** A collection of reference books, pronunciation guides, and online resources are available to support self-study and further exploration of speech and communication topics.

This manual will serve as your comprehensive guide to navigating the Speech Laboratory effectively. It will provide step-by-step instructions, guidelines, and tips

to help you make the most of the available resources and achieve your speech and communication goals.

We encourage you to explore the diverse offerings of the Speech Laboratory, engage in regular practice sessions, and seek support from our knowledgeable staff. Whether you are a student seeking to excel in presentations, a faculty member aiming to improve classroom communication, or a staff member looking to enhance your professional communication skills, the Speech Laboratory is here to support you on your journey to becoming a confident and effective communicator. Users are encouraged to attend orientation sessions or introductory workshops to familiarize themselves with the laboratory's equipment, resources, and best practices for effective utilization.

Please refer to the subsequent sections of this manual for detailed instructions, procedures, and additional information about the services and resources available in the Speech Laboratory.

SPEECH LABORATORY GUIDELINES

Access and Use of the Speech Laboratory:

- The Speech Laboratory is available for use by all registered students and faculty members of the City College of Cagayan de Oro.
- Users must present a valid ID card to the laboratory staff upon entering the facility.
- Prior reservation is required to ensure the availability of the laboratory.
- Users should strictly adhere to the scheduled time slots to avoid inconvenience to other users.
- No food or beverages are allowed inside the laboratory.
- Users are responsible for the proper care and handling of equipment and materials.
- Any damage caused to the laboratory equipment or facilities must be reported immediately to the laboratory staff.

Laboratory Hours:

- The Speech Laboratory is open from 8:00 am to 5:00 pm, Monday to Saturday.
- The laboratory may be closed during official holidays or special events. Prior notice will be given for any closures.

Note: The operating hours may be subject to change during holidays, semester breaks, or special events. It is recommended to check with the Speech Laboratory staff or refer

to the college's official schedule for any updates or adjustments to the operating hours.

We understand that flexibility is essential, and we strive to provide ample access to the Speech Laboratory to accommodate your needs. However, please be mindful of the closing time and ensure that you allow sufficient time to conclude your activities and return any borrowed equipment before the laboratory closes.

If you have any questions regarding the location or operating hours of the Speech Laboratory, our dedicated staff members are available to assist you. You can reach out to them by visiting the laboratory in person, calling the designated contact number, or sending an email to the provided email address. Accessing the Speech Laboratory is a straightforward process that ensures a smooth and efficient experience for all users.

Reservation of Laboratory:

- Users must reserve the laboratory in advance by contacting the laboratory
- coordinator or staff.
- Reservation requests should include the date, time, purpose, and estimated
- d. duration of the intended use.
- The laboratory staff will confirm the reservation and allocate the appropriate
- time slot.
- Reservations can be made up to two weeks in advance.

Laboratory Etiquette:

- Maintain a respectful and professional attitude while using the Speech Laboratory.
- Use headphones when working on individual tasks to avoid disturbing others.
- Refrain from using mobile phones or any electronic devices that may cause disruptions.
- Be respectful of others' space and property within the laboratory.
- Clean up after use, ensuring that all materials and equipment are returned to their proper places.
- The Speech Laboratory is primarily intended for academic purposes related to speech and communication. Engage in activities directly related to speech practice, rehearsal, research, or coursework.
- Use the scheduling system to reserve time slots for utilizing the Speech Laboratory resources. Respect the allocated time slots and vacate the area promptly at the end of your reservation.
- Handle equipment and resources with care and follow the provided instructions for operation.

- Obtain consent from individuals involved before recording any speeches, presentations, or conversations in the Speech Laboratory.

- Maintain a quiet environment conducive to speech and communication activities.
- Keep conversations at a low volume to minimize disturbances for others.
- Use headphones when listening to audio materials to avoid disturbing others.

Laboratory Equipment and Resources:

- The Speech Laboratory is equipped with state-of-the-art audio and video recording equipment.
- Microphones, headphones, and amplifiers are available for individual and group use.
- Various software programs for speech analysis, pronunciation practice, and presentation skills enhancement are installed on the laboratory computers.
- Reference books, study materials, and audiovisual resources related to speech and communication are available for use within the laboratory.

Laboratory Assistance and Support:

- Trained laboratory staff will be available during operating hours to assist users with technical issues and provide guidance on laboratory equipment and resources.
- Users can seek assistance from the laboratory staff for specific speech-related exercises, pronunciation practice, or speech analysis.
- Scheduled workshops, training sessions, and tutorial services will be organized periodically to enhance users' speech and communication skills.

Academic Use of the Speech Laboratory:

- The laboratory may be used for instructional purposes, such as speech classes, public speaking workshops, and presentations.
- Faculty members may reserve the laboratory for specific class activities, assessments, or research projects.
- Students are encouraged to utilize the laboratory for individual practice, group discussions, or speech rehearsals.

Safety and Security:

- Follow all safety guidelines and procedures provided by the laboratory staff. Be aware of emergency exits, fire extinguisher locations, and other safety measures within the laboratory.

- Users should adhere to the college's safety regulations and guidelines while using the laboratory.
- Report any unsafe conditions or equipment malfunctions to the laboratory staff immediately.
- Do not tamper with or attempt to repair any laboratory equipment without proper authorization

PROCESS, REGISTRATION AND SCHEDULING REQUIREMENTS

Process in accessing the laboratory including any registration or scheduling requirements

1. Registration Form. Obtain a registration form from the Speech Laboratory or the designated department responsible for managing registrations. This form may be available in both digital and physical formats. Fill out the registration form completely and accurately. Provide all the necessary information requested, including personal details such as your name, student/staff ID number, contact information, and any relevant academic program information. Read through any terms and conditions or policies associated with registration and ensure that you understand and agree to them.

2. Submission Process. Once you have completed the registration form, follow the submission instructions provided. These instructions may vary depending on the college's procedures. If the registration form is physical, submit it to the designated drop-off location, such as the Speech Laboratory office or a specific department office. Ensure that you provide the form to the appropriate staff member or place it in a designated registration box.

3. Eligibility Criteria and Restrictions. To provide clarity and transparency, it is important to specify any eligibility criteria or restrictions associated with the registration process for the Speech Laboratory.

- Individuals must be currently enrolled as students at City College School to be eligible for registration in the Speech Laboratory.

- Individuals may be required to have successfully completed an introductory speech course as a prerequisite for accessing the Speech Laboratory.\

- Individuals may be required to obtain a recommendation from a faculty member who can attest to their communication skills and readiness to utilize the Speech Laboratory.

- Individuals may be required to attend an orientation session that provides an overview of the Speech Laboratory's resources, guidelines, and safety procedures.

- Certain programs or majors may require individuals to utilize the Speech Laboratory as part of their coursework or program requirements.

- It is important to note that these prerequisites or requirements may vary based on the specific policies and goals of the City College School and its Speech Laboratory.

4. Confirmation and Approval. After submitting your registration form, you may receive a confirmation or approval notification. This notification may come in the form of an email, letter, or online message.

LABORATORY LAYOUT AND EQUIPMENT

Location. The Speech Laboratory is located in a dedicated space within the City College campus, typically situated within the Department of Communication or a related department. Specify the building and floor where the laboratory is situated for easy navigation.

Reception Area. Upon entering the laboratory, there is a reception area where students and faculty members can check-in, seek assistance, or make inquiries. This area may also include a waiting area for individuals who are waiting for their scheduled sessions.

Workstations and Practice Areas. The laboratory is equipped with multiple workstations or practice areas where individuals can engage in speech-related activities. Each workstation is typically equipped with a computer, microphone, audiovisual equipment, and relevant software for recording, playback, and analysis of speech.

Recording and Playback Facilities. The Speech Laboratory features dedicated recording and playback facilities, allowing individuals to record their speeches or presentations for self-evaluation and review. These facilities may include specialized recording equipment, soundproof rooms, and software for analyzing and reviewing recordings.

Presentation Area. The laboratory may have a designated presentation area where individuals can deliver speeches or presentations in front of an audience.

This area may include a podium, projector or display screen, seating arrangements, and necessary audiovisual equipment for delivering effective presentations.

Resource Library. The laboratory may have a resource library or materials section containing books, journals, audiovisual resources, and reference materials related to speech, communication, public speaking, and related topics. Individuals can access these resources to enhance their knowledge and skills in the field of speech and communication.

SERVICES AND RESOURCES

The Speech Laboratory at our City College School offers a range of services to support the development and enhancement of speech and communication skills. It serves as a dedicated space for students, faculty, and staff to practice various aspects of oral communication, including speeches, presentations, interviews, and conversation exercises. The laboratory provides recording and playback facilities, allowing users to review and analyze their performances to improve their delivery, articulation, and overall communication effectiveness. Non-native English speakers can utilize the laboratory's resources and tools to work on pronunciation, reduce accents, and enhance language proficiency. Additionally, the laboratory offers support for public speaking and presentation skills development, including guidance on organization, delivery techniques, and visual aids. Users can also access speech analysis tools, engage in communication research projects, attend workshops and training sessions, and receive consultation and support from communication experts. The Speech Laboratory aims to create a conducive environment for individuals to refine their communication abilities and excel in various professional and academic settings.

In addition to the core services, the Speech Laboratory at our City College School offers a range of additional support services to further assist individuals in their speech and communication journey. One such service is individual and group tutoring, where students can receive personalized guidance and instruction tailored to their specific needs. These tutoring sessions are conducted by experienced communication experts who provide valuable feedback, tips, and strategies to help students improve their speech delivery, language skills, and overall communication competence. The laboratory also hosts workshops and training sessions on various topics related to public speaking, presentation skills, voice modulation, and non-verbal communication. These interactive sessions provide participants with practical techniques, hands-on practice, and the opportunity to learn from industry professionals. Moreover, consultation sessions are available for individuals seeking specialized guidance or support in specific areas of speech and communication. During these sessions, experts provide one-on-one consultations, feedback on specific projects or presentations, and assistance in developing effective communication strategies. These additional support services complement the existing resources of the Speech Laboratory, fostering a comprehensive learning environment where individuals can refine their skills, build confidence, and achieve their communication goals.

CITY COLLEGE OF CAGAYAN DE ORO SCHOOL WEBSITE & SCHOOL MANAGEMENT SYSTEM MANUAL

I. SCHOOL WEBSITE

I.a Website Access Guidelines and Policies

City College of Cagayan de Oro's website is a vital platform for providing information, resources, and updates to students, staff, and the public. To ensure secure and efficient access, the following guidelines and policies must be observed:

1. User Responsibilities
Users must conduct themselves responsibly and ethically while using the City College of Cagayan de Oro's website. This includes refraining from any activities that may disrupt website operations or compromise its security.

2. Data Security
Users must adhere to data security protocols to protect sensitive information, in compliance with the Data Privacy Act of 2012 (Republic Act No. 10173). This includes:

- Confidentiality: Ensure that personal and sensitive information is handled confidentially and not disclosed without proper authorization.
- Data Integrity: Maintain the accuracy and completeness of the data accessed, processed, or stored.
- Security Measures: Employ appropriate security measures, such as strong passwords and secure connections, to protect data from unauthorized access and breaches.
- Reporting Breaches: Report any suspected data breaches or security incidents to the website administrators immediately.
- Compliance: Adhere to all relevant provisions of the Data Privacy Act and related guidelines from the National Privacy Commission (NPC).

3. Content Usage
The content on the City College of Cagayan de Oro website is provided for academic and informational purposes only. Users must:

- **Use Content Responsibly**: Utilize the website's content solely for its intended educational and informational purposes.
- **Prohibited Activities**: Reproducing, distributing, or modifying website content without explicit authorization is strictly prohibited. This includes copying text, images, or other materials for commercial or personal use outside the scope of permitted activities.

4. Compliance with Policies

Users must adhere to all City College of Cagayan de Oro's website usage policies, as well as local and international laws governing online conduct, privacy, and information security:

- Institutional Policies: Abide by the college's policies regarding the appropriate use of website resources, data management, and user conduct.
- Data Privacy and Security: Follow protocols outlined in the Data Privacy Act of 2012 (Republic Act No. 10173) and relevant data protection regulations to ensure the confidentiality and security of personal and sensitive information accessed through the website.
- Regulatory Compliance: Adhere to applicable local and international laws governing online conduct, privacy, and information security. This includes compliance with standards set by regulatory bodies such as the National Privacy Commission (NPC) for data privacy and security.

5. Accessibility

The City College of Cagayan de Oro website is designed to be accessible to all individuals with or without disabilities. To enhance accessibility, the following features are available:

- **ChatAIms**: An AI chat assistant named chatAIms is integrated into the website to provide real-time support and guidance. Users can interact with chatAIms for assistance with navigating the website, accessing information, and resolving issues.
- **Text-to-Speech**: The website includes a text-to-speech feature to assist visually impaired users. This functionality allows users to have the website's text read aloud, improving accessibility and usability for those with visual impairments.

  Users requiring additional accommodations or facing accessibility challenges should contact the website administrators for personalized assistance. The college is committed to ensuring an inclusive online experience for all users.

6. Website Updates

The website will undergo regular maintenance and updates to enhance functionality and content. Users will be notified in advance of any significant changes or scheduled maintenance.

7. Content Posting Requests

Faculty, staff, and students can request content to be posted on the City College of Cagayan de Oro website. To submit a content posting request, users have two options:

- **Online Request Form**: Complete the content posting request form available at bit.ly/request-content-posting. This form allows users to provide details about the content they wish to have posted.
- **In-Person Submission**: Alternatively, requests can be submitted in person at the Technology Innovation and Data Management Center (TIDMC) office, where assistance is available for the submission process.

8. Reporting Issues and Providing Feedback

Users are encouraged to actively contribute to the improvement of the City College of Cagayan de Oro's website by reporting technical issues, broken links, or content errors, and by providing feedback on their overall experience.

- **Reporting Issues**: For technical problems, broken links, or content errors, users should promptly contact the website administrators. This can be done by emailing **ict.citycollege.cdo@gmail.com**, which is visible in the footer of every page on the website.
- **Providing Feedback**: The website values user input on functionality, content relevance, and overall user experience. Users can submit their feedback directly via the same email address, **ict.citycollege.cdo@gmail.com**, or through designated feedback forms available on the website.

II. SCHOOL MANAGEMENT SYSTEM

II.a POLICY AND GUIDELINES FOR THE CITY COLLEGE SCHOOL MANAGEMENT SYSTEM USAGE

The aims.citycollegecdo.edu.ph web application serves as the centralized school management system designed to efficiently deliver essential information and services to students, faculty, and staff of City College of Cagayan de Oro City.

1. **User Responsibilities**

1.1 **Access**: Users must use their designated login credentials responsibly.

1.2 **Content Usage**: Users are expected to adhere to copyright laws and respect intellectual property rights when accessing the website.

2. **Privacy and Data Protection**

2.1 **Confidentiality**: *The college is committed to protecting user data in compliance with the Data Privacy Act of 2012 (Republic Act No. 10173) and other applicable privacy laws in the Philippines. We ensure that personal data collected, stored, and processed through the school management system is treated with the highest level of confidentiality. Access to personal data is restricted to authorized personnel only.*

2.2 **Data Collection and Usage**: The collection and use of personal data are conducted in accordance with the principles of transparency, legitimate purpose, and proportionality, as mandated by the Data Privacy Act. Users are informed of the specific purposes for which their data is collected, and only the minimum necessary data is gathered to fulfill these purposes.

2.3 **Data Subject Rights**: Users have the right to access, correct, and request the deletion of their personal data, as provided under the Data Privacy Act. Requests can be made through the designated Data Protection Officer (DPO) of the college, who will ensure that user rights are respected and upheld.

2.4 **Data Security**: The college implements appropriate organizational, physical, and technical security measures to protect personal data against unauthorized access, alteration, disclosure, or destruction. Regular security audits and risk assessments are conducted to ensure ongoing compliance with data protection laws.

2.5 **Breach Notification**: In the event of a data breach, the college will promptly notify the affected individuals and the National Privacy Commission (NPC) in accordance with the Data Privacy Act. Measures will be taken to mitigate the impact of the breach and prevent future occurrences.

2.6 **Compliance and Accountability**: The college is committed to complying with all relevant provisions of the Data Privacy Act and holds all users accountable for adhering to the established privacy and data protection policies. Regular training and awareness programs are conducted to ensure that all users understand their responsibilities in safeguarding personal data.

3. **Security Measures**

3.1 **Account Default Login**: Users are provided with their default password after the account registration. Users are advised to change the account default password to a strong and unique password.

3.1 **Account Security**: Users are responsible for maintaining the confidentiality of their login credentials, including passwords and other authentication methods. It is imperative to use strong, unique passwords and to change them regularly. Users must immediately report any suspicious activity or potential security breaches to the IT support team.

3.2 **Access Control**: Access to the school management system is strictly role-based, ensuring that users can only access data and perform actions relevant to their roles. The principle of least privilege is applied, meaning users are granted the minimum level of access necessary to perform their duties.

3.4 **Data Encryption**: Data transmitted between users and the school management system is encrypted using industry-standard protocols (e.g., SSL/TLS) to protect it from interception or unauthorized access. Additionally, all login credentials stored within the system are encrypted to ensure its security.

3.5 **Regular Security Audits**: The college conducts regular security audits and vulnerability assessments of the school management system to identify and address potential weaknesses. Any identified vulnerabilities are promptly addressed, and system updates are applied to maintain a robust security posture.

3.6 **Incident Response**: A comprehensive incident response plan is in place to handle any security incidents, including data breaches. This plan includes procedures for detecting, reporting, and responding to incidents, as well as for mitigating any impact and restoring normal operations as quickly as possible

3.7 **Compliance with Legal and Regulatory Standards**: The college ensures that all security measures comply with relevant laws, regulations, and standards, including the Cybercrime Prevention Act of 2012 (Republic Act No. 10175) and other applicable Philippine legislation. This commitment to legal compliance helps safeguard the integrity of the school management system..

II.b USER GUIDE FOR STUDENTS

1. Accessing the Website

1.1 URL: Students should open their web browser and navigate to aims.citycollegecdo.edu.ph. Once the page loads, they should click on the "Login as Student" button to proceed to the student login page.

1.2 Login Instructions:

- Enter Credentials: Students must input their student ID in the designated field, which serves as their username.
- Password: Students should enter the password provided by the administrator. If it is their first time logging in, they should use the default password given by the college and follow the prompts to change it to a more secure password.
- Security: Students are required to keep their login credentials confidential and avoid sharing them with others. For issues with credentials, they should contact the IT support team.

2. Dashboard Features

2.1 Class Schedule:

- View Schedule: Students can click on the "Class Schedule" tab to view their current semester's class timetable.

2.2 View and Download COR:

- Certificate of Registration (COR): Students should navigate to the "Academic Records" section and select "View COR" to view and download a PDF copy of their current semester's registration details.

2.3 Campus Events:

- Calendar of Activities: Students can stay updated with campus events by clicking on the "Campus Events" tab, where they will find a comprehensive calendar listing all upcoming activities, including academic deadlines, cultural events, and special lectures.
- Event Notifications: Students may subscribe to events of interest to receie reminders and updates.

2.5 Memorandum :

- Official Communications: Students can access the "Memorandum" section to view and download official memoranda issued by the college administration. These may

include policy updates, academic guidelines, and other important communications.

II.c USER GUIDE FOR SCHOOL ADMINISTRATORS AND FACULTIES

1. Accessing the Webapplication

1.1 URL: Administrators and faculty should visit aims.citycollegecdo.edu.ph using their preferred web browser. They should select the "Login as Faculty" option to enter the administrative portal.

1.2 Account Login/Registration:

- **Authorized Credentials**: They must enter the email and password that is registered by the administrator sent via email.
- **Account Registration**: Faculty account registration is processed by the administrator to provide a respective role and access to the system. After the account registration the faculty should validate the email provided to complete the account registration.

1.3 Account Portal/s:

- **Account Portal System**: Faculty accounts are divided into different portals that are assigned and managed by the administrator on the account registration process. Different portals provide different sets of tools that are based on how much privilege is given to the account.
- **Account Sub Portal/s**: Accounts can have multiple portals depending on how many roles/functions the faculty is assigned to. Users can swap portals anytime if necessary to perform their duties.

2. Sidebar Features

2.1 Registrar:

- Student Record: Registrar can access comprehensive student records, including enrollment status, and course registration details. They can use this feature to update and maintain accurate student information.
- Reports: Administrators can generate detailed reports on student enrollment trends, statistics, and other essential administrative data reports to meet specific departmental needs.

- Enrollment Forms: Registrar can access the student enrollment form for paperless enrollment for both TSTI and HEI enrollees.
- Enrollment Screening: After the student successfully submit the enrollment form, the registrar can screen the in-coming student data to confirm the submission and send the student to the next enrollment step. For TSTI enrollees, enrollment screening can assign a facilitator to the student for qualification screening.

2.2 Dean:

- Department Oversight: Deans can monitor departmental activities, including curriculum management, faculty performance, and adherence to academic policies. This feature provides a centralized view of all departmental operations.
- Faculty Management: Deans can assign faculty members to courses, evaluate their performance, and track their professional development. This includes managing faculty schedules and coordinating with other departments as needed.

2.3 Program Head:

- Program Administration: Program heads can administer all aspects of their specific program, including curriculum updates, course scheduling, and adjustments. This feature allows for efficient management of program-specific data and activities.
- Curriculum Updates: Program heads can propose and implement updates to the program curriculum, ensuring alignment with academic standards and industry requirements.

2.4 Faculty Members:

- Input Grades: Faculty members can enter and submit student grades for all assigned courses. The system allows for real-time updates and automated calculation of final grades based on the inputs.
- Attendance Tracking: Faculty can record student attendance directly through the portal, with automated alerts for students who fall below attendance requirements.

3. Notifications and Communication

3.1 Calendar of Activities:

- Campus Events and Meetings: Administrators and faculty can stay informed about upcoming campus events, academic meetings, and important departmental activities. The calendar feature

integrates with personal schedules to provide reminders and alerts.

3.2 Memorandum:

- Official Communications: Administrators and faculty can view and acknowledge memoranda and other official communications from the college administration. These documents are critical for staying updated on institutional policies and procedures.

II.d REVIEW AND COMPLIANCE

1. Feedback Mechanism

- User Feedback Collection: Users are encouraged to submit feedback on the functionality and user experience of the school management system. Feedback can be sent by clicking the email address provided in the footer of the website: ict.citycollege.cdo@gmail.com.
- Review and Action: The IT department and relevant administrative personnel will review the feedback received. Based on this feedback, necessary updates and improvements will be implemented to enhance the service delivery and overall user experience.
- Continuous Improvement: The college is committed to using user feedback to drive continuous improvement of the system. Updates and changes will be made as needed to ensure the platform effectively meets user needs and expectations.

2. Policy Compliance

- Adherence to Policies: All users must adhere to institutional policies related to data privacy, security, and the responsible use of the school management system. This includes following guidelines for data protection, respecting intellectual property rights, and maintaining the confidentiality of login credentials and other sensitive information.
- Compliance Monitoring: Regular audits and assessments will be conducted to ensure compliance with these policies. Any breaches or non-compliance issues will be promptly addressed with appropriate corrective actions.
- Training and Awareness: Users will receive ongoing training and updates about policy changes and best practices to ensure compliance with institutional standards and legal requirements.

III.E. Downtime, System Failure, and Troubleshooting Management Measures

1. **Preventive Downtime System Failure measures Automation - Information Management System (AIMS)**

Preventive Measure	Process	Personnel in-charge
Regular System Updates	Schedule and apply updates to software and firmware to patch vulnerabilities and improve system performance.	System Developer
Automated Backups	Implement automated backups of system data and configurations to ensure recovery in case of failure.	System Developer
System Monitoring	Utilize monitoring tools to track system performance, detect anomalies, and receive alerts for potential issues.	System administrator
Security Audits	Conduct regular security audits to identify and address potential vulnerabilities and compliance issues.	Network & infrastructure officer
User Training	Provide ongoing training for users on best practices for system usage and security to minimize human errors.	System training officer

2. **Restoration Measures for Automation Information Management System (AIMS) Downtime System Failure**

Restoration Measures for Automation Information Management System (AIMS) Downtime System Failure

Restoration Measure	Process	Personnel in-charge
Restore from Backup	Use the most recent backup to restore system data and configurations to the state before the failure occurred.	System Developer
System Diagnostics	Run diagnostic tools to identify and troubleshoot the cause of the system failure.	System administrator
Emergency Patch Application	Apply emergency patches or updates to fix vulnerabilities that caused the system failure.	System Developer
Service Restoration	Restart affected services or components to return the system to normal operation.	System Developer /Network & infrastructure officer
Incident Review and Reporting	Review the incident to determine its cause, impact, and actions taken; generate a report for future reference.	System administrator