ADMINISTRATION - 200

Administrative Organization (200.1)

Date Adopted: December 19, 1989
Revised: February 21, 2023

The administrative organization of Illinois Eastern Community Colleges is outlined in the administrative charts adopted by the Board of Trustees. The Chancellor serves as Chief Administrative Officer of the District and as Executive Officer of the Board of Trustees. It is the responsibility of the Chancellor to recommend the administrative structure of the District to the Board of Trustees.

ADMINISTRATION - 200

Appropriate Use of Information Technology Resources Policy *(*200.2)

Adopted: June 11, 1996
Revised: August 17, 2005
Revised: April 19, 2016
Revised: May 16, 2017
Revised: October 17, 2017
Revised: May 18, 2021
Revised: April 22, 2025

Illinois Eastern Community Colleges (IECC) provides information technology (IT) resources as vital assets to support its mission and operations. These resources must be utilized and managed responsibly to maintain their integrity, security, and availability. This policy defines the appropriate use of IECC's IT resources, which are accessible only to authorized users who must comply with legal, ethical, and IECC requirements.

Scope
This policy applies to authorized users of IECC's IT resources, whether on-site or off.

Ownership
IECC maintains complete ownership rights of IT resources. IT resources that are leased, licensed, or purchased through contracts or grants will be managed according to this policy as long as they are within the lawful possession or control of IECC.

Access
Accessing IT resources without proper authorization, unauthorized use of computing facilities, and intentional or negligent corruption or misuse of IT resources is strictly prohibited.

IECC reserves the right, at its sole discretion and for any reason or no reason, to immediately revoke, restrict, or extend authorization to access or utilize any or all IT resources. IECC accepts no responsibility or liability for any unauthorized or personal use of its IT resources by users.

Terms of Use
As a condition for accessing and using IT resources, all users must:

- Comply with all applicable laws, IECC policies and procedures, contracts and licenses;
- Use only those IT resources that the individual user is authorized to use and only in the manner and to the extent authorized;
- Not attach any device that may, in any way, endanger or disrupt the continuous and stable operation of the IECC network or other IT resources or that may compromise the confidentiality or integrity of information stored on any technology resource;
- Not share or transfer individual IECC accounts, including network IDs, passwords, or other access codes that provide access to IT resources;
- Respect the privacy of other users and their accounts, devices, and data regardless of whether those elements are securely protected; and
- Respect the limitations of IT resources and manage usage so as not to interfere with the activities of others.

Privacy and Monitoring
IECC does not establish any general expectation of privacy regarding the use of IT resources, except as required by law. IECC retains the right to monitor and report on technology usage, including the use of personal devices connected to IT resources, to the fullest extent permitted by law. By using IT resources, all users consent to this monitoring and reporting. Authorized IECC employees may review the subject, content, and appropriateness of electronic communications or other computer files at any time, and

remove them if warranted, and report any rule violations to IECC administration and/or law enforcement officials. As allowed by law, IECC may disclose data stored in IT resources to third parties.

Account Security and Information Exchange
User IDs and passwords are provided for technology systems and are only for individual use. Users should not share passwords with anyone and should not use anyone else's password regardless of how the password was obtained. If a user suspects someone has discovered his or her password, the password should be changed immediately, and the IT Help Desk should be notified. Users shall not intentionally modify files, data, or passwords belonging to other users. When sending electronic communications, users should be cautious when including personal information. IECC is not responsible for personal information which is obtained by unauthorized recipients or interceptors of electronic communications.

Multi-factor Authentication
Multi-factor authentication (MFA) is also required for all users accessing IECC's systems. MFA is a method of computer access control in which a user is granted access only after successfully presenting multiple separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are). IECC utilizes four MFA verification methods: 1. The Microsoft Authentication App, 2. A text message to a cell phone, 3. A phone call to any 10-digit phone number, 4. A digital token key. Digital token keys will be available on a case-by-case basis. A lost or stolen MFA token should be reported immediately to the IT Help Desk. A replacement charge of $25.00 may be applied for any lost or stolen token.

Employee Account Setup Process
Supervisors must ensure their staff have access to those accounts necessary to perform their job functions. Written requests are submitted to Human Resources and the IT Department for verification and processing. Upon completion, IT personnel provide account information to the employee.

Employee Email and Electronic Communications
IECC provides email accounts to all employees with the expectation that all work-related electronic communications will be conducted exclusively through these accounts. As public employees, the utilization of the provided email accounts ensure proper recordkeeping, compliance with public records laws, and transparency. Likewise, IECC-provided email accounts are intended solely for work-related purposes and should not be used for personal communication.

Student Account Setup Process
Student accounts are generated during the application acceptance process. Credentials are sent to a student by encrypted email to setup their MyIECC account. Student Services in some cases may directly issue credentials to create an account using a GeneratedID and PIN. In either process the student must complete account setup and set a new password. The MyIECC account provides access to many services including email, electronic course materials, schedules, grades, account balances, and much more.

Student Email and Electronic Communications
IECC provides email accounts to students as a tool for sharing important and official information regarding registration, financial aid, deadlines, student life, and more. IECC expects that every student will receive email at his or her IECC email address and will read email on a frequent and consistent basis. A student's failure to receive and read IECC communications in a timely manner does not absolve that student from knowing and complying with the content of such communications.

Priority Usage of Computer Hardware, Software, and/or Facilities
Priority shall be given to classroom activities, assignments and/or research and to IECC faculty, staff, and students.

Lab User Age Restriction

Patrons under the age of 18 who are not enrolled students are not permitted to use the open lab computers without obtaining authorization from IECC staff.

Student Data Storage

Students are not allowed to store personal work and/or software on the hard drives in the open lab. Any files or software found on the hard drives will be deleted. IECC is not responsible for data lost for any reason including, but not limited to: power failure, computer failure, or any other planned or unplanned or unavoidable event or emergency.

Public Wi-Fi Internet Access

Wireless public Internet access is provided throughout most IECC's campus locations. **Please be advised that the public network does not enforce any security or encryption.** Transmissions of secure information such as ID's, credit card numbers, passwords, etc. may be intercepted by wireless users in or near the open networks. **IECC is not responsible for damage to personal property or other injury, including damage to personal computing devices resulting from software/hardware installation or Internet use.**

Personal and Commercial Use of IT Resources

IT resources may be used for incidental personal purposes. Personal use of IT resources must not occur under circumstances that interfere with employee work responsibilities, displace other IT resources, or require purchases of additional IT resources.

Users are prohibited from using IT resources for non-IECC commercial purposes or personal gain unless explicitly authorized.

Copyrighted Material

Users shall not: copy and forward, download, and/or upload to the IECC network or Internet server any copyrighted, trademarked, and other intellectual property without express authorization from the owner of the trademark, copyrights, or intellectual property right.

IECC prohibits the use of peer-to-peer file sharing applications on its network, including wireless network services, to transmit, exchange, or copy any music, software, or other materials which are protected by copyright or intellectual property rights.

Unauthorized copying, use, or distributions of software is illegal, strictly prohibited, and subject to criminal penalties. Penalties for copyright infringement are controlled by the U.S. Copyright Office and can be as high at $150,000 per incident. For additional information, please see the website of the U.S. Copyright Office at https://www.copyright.gov. Similarly, other intellectual property content owners may take criminal or civil action against a user for unauthorized copying, use or distribution of intellectual property materials. All the content transmitted via e-mail and web publishing must either be the users' own or must be transmitted with express authorization for distribution by IECC or by the individual who owns the trademark, copyright, or intellectual property right.

Enforcement

Access to and use of IECC's IT resources is a privilege, not a right, and may be revoked without notice if there is a reason to believe that the user has violated, or may have violated, IECC policies, procedures or applicable local, state, or federal laws. Additionally, employees in violation of this policy are subject to disciplinary actions up to and including termination. Students in violation of this policy are subject to disciplinary actions outlined in the Student Code of Conduct. IECC treats access and use violators of IT resources seriously and will pursue criminal and civil prosecution of violators deemed necessary.

Further, IECC has the right to remove, without notice, any material from its systems found to be inappropriate or illegal.

Definitions
The following are definitions for the purpose of this policy.

Account: refers to a digital identity or credentials assigned to an authorized user to access and utilize information technology systems, resources, or services. These accounts are integral to managing and securing access in computing environments.

Authorized User(s): students, employees, and other constituents of IECC. who have been granted permission to access and use specific IT systems, resources, or data based on their role, responsibilities, or needs.

Computing Devices: various classes of computers, servers, and mobile devices, whether owned or leased by IECC, or if owned by an individual and connected to an IECC-owned, leased, or operated network; use of these computing devices is covered by this policy.

Employee: anyone who works for IECC full-time, part-time, or on a temporary basis.

Information Technology (IT) Resources: include IECC-owned infrastructure, cloud services, software, hardware with computing and/or networking capabilities, and data. These resources include, but are not limited to, computers, computer systems, telephones, tablets, mobile devices, classroom presentation systems, voice communication and messaging equipment, networking systems, software, electronically stored institutional data and messages, similar resources, and any other technologies or services implemented to support them.

Network: a system of interconnected devices, such as computers, servers, routers, and other hardware, that communicate and share resources with one another using a set of standardized protocols.

Personally Owned Data: refers to information that was neither created nor collected for institutional purposes; rather, it belongs to an individual. This data includes, but is not limited to, income tax records, medical information, banking details, financial data, family information, or any other personal details that an individual might reasonably consider private or sensitive.

Software: the programs and other operating systems that enable a computer or electronic device to perform specific tasks.

Student: an individual who has enrolled in a class offered by IECC.

Systems: refers to an integrated set of components that work together to perform specific functions or solve specific problems.

User(s): see Authorized User(s)

Disclaimers
Users utilize IT resources at their own risk. While IECC makes reasonable efforts to secure its IT resources and strives to ensure they are effective and efficient, it cannot guarantee their confidentiality, integrity, or availability. IECC does not provide any warranty or promise that IT resources will function as designed or as the user expects. IECC IT professionals are not available to recover any personally owned data that is lost or compromised. IECC assumes no legal responsibility for any damages or losses of any kind, including but not limited to the loss of personally owned data or devices, resulting from the failure of IT resources. Users can reduce the risk of data loss by consistently backing up their data.

ADMINISTRATION - 200

Information Technology (IT) Change Management Policy (200.3)

Effective date: June 20, 2012
Revised: September 19, 2023

Purpose

Modifications to IT resources require serious forethought, testing, coordination, appropriate communication, and post-change evaluation in order to achieve intended impact and avoid unintended consequences. The purpose of the Information Technology Change Management Policy is to ensure a consistent and systematic approach is used for modifying IECC's IT resources. This approach streamlines processes while mitigating security risks and potential loss due to system outages.

Scope

Changes that may affect IT resources that are critical to IECC'S operations are within the scope of this policy.

Procedures

Procedures have been developed to provide details pertaining to planned and unplanned modifications to IT resources.

ADMINISTRATION - 200

Information Technology (IT) Remote Access Policy (200.4)

Effective date: June 18, 2013

This Information Technology Remote Access Policy establishes the requirements for gaining off-campus access to the IECC network, computing resources and data for all users of IECC resources. The standards are designed to minimize the risk of exposure and protect IECC internal computer systems, networks, and data.

Anyone requiring remote access to IECC systems must adhere to the Remote Access Procedures.

ADMINISTRATION - 200

Trustee Adoption, Amendment, or Repeal of Policies (200.5)

Effective date: December 10, 2013
Deleted by Board Action: April 25, 2023 (See Procedure 100.1)

ADMINSTRATION- 200

<u>Allied Health Technology Requirements Policy</u> (200.6)

Date Adopted: December 12, 2017
Deleted by Board Action: November 15, 2022

ADMINISTRATION – 200

Human Subjects Research Policy (200.7)

Date adopted: July 20, 2021

Illinois Eastern Community Colleges (IECC) is committed to ensuring the safety, rights, and welfare of all participants involved in human subjects research. All research involving human subjects must be conducted in compliance with all applicable federal, state, and local regulations, including the HHS regulations for the protection of human subjects in research (Code 45CFR 46). All prospective research projects will be reviewed by the HSR Coordinator, who will make a decision or convene the Institutional Review Board (IRB) for further review and determination. IECC prohibits any research involving participants under the age of 18.

The purpose of the HSR review process is to ensure:

1. Equitable selection of subjects.
2. The risk to subjects is minimized.
3. Any deception is justified.
4. Data collection is confidential and subject privacy is protected.
5. Informed consent is obtained prior to the involvement of subjects.
6. Subjects can withdraw from the study at any time.

ADMINISTRATION - 200

Campus Closures and Interruptions (200.8)

Date Adopted: March 19, 2024

Illinois Eastern Community Colleges (IECC) prioritizes the safety and well-being of its community members in situations involving inclement weather and other non-critical events necessitating decisions regarding campus closures or interruptions. The decision-making process involves collaboration among IECC administration to ensure timely and informed actions. It’s important to note that closures of this nature fall outside the purview of the policy and plans related to Policy 100.24, Emergency Response Plans.

Closure Dissemination

In the event of such occurrences, IECC will promptly disseminate information through multiple communication channels to reach students, faculty, and staff. This includes Regroup Mobile alerts via text/email, website messaging, and engagement with primary news outlets within the District.

Procedures and Guidelines

Clear procedures and guidelines will be developed to ensure students, faculty, and staff are well-informed about the notification processes and associated expectations. These protocols will be readily accessible on the official IECC website and other relevant publications to facilitate awareness and understanding among the college community.