ICR FLORIDA
EDUCATION

ICR FLORIDA
EDUCATION

GLBA
CYBERSECURITY Policy

Find More Info:

633 NE 167TH RD ST SUITE # 913
NORTH MIAMI BEACH, FLORIDA 33162
FAX (850)-546-6119
✉ info@icrfloridaeducation.com
☎ (786)-254-0520
🌐 www.icrfloridaeducation.com

ICR FLORIDA
EDUCATION

CYBERSECURITY POLICY

POLICY STATEMENT:

Each member of the ICR Florida Education is responsible for the security and protection of electronic information resources over which he or she has control. Resources to be protected include networks, computers, software, and data. The physical and logical integrity of these resources must be protected against threats such as unauthorized intrusions, malicious misuse, or inadvertent compromise. Activities outsourced to outside entities must comply with the same security requirements as in-house activities.

REASON FOR POLICY:

This policy's purpose is to establish a framework for ensuring that ICR Florida Education information technology (IT) resources are managed securely. These resources include information, information systems, computing platforms, and networks. It also ensures that the college complies with state laws and regulations regarding the use of and security of information resources.

DEFINITIONS:

- ***Information Technology (IT) Resources*** includes all college-owned computers, applications software, systems software, databases, and peripheral equipment; the data communications infrastructure; the voice communications infrastructure; classroom technologies; communication services and devices, including electronic mail, voice mail, modems, and multimedia equipment. The components may be stand-alone or networked and may be single-user or multi-user systems.
- ***Critical Information System*** means a computer system that stores and processes information that is vital to college business such as the Student Information System (SIS) or the college financial systems.
- ***Sensitive Information*** is data in electronic or paper form that contains college privileged information such as financial information or strategic plans.
- ***Protected Health Information*** (PHI) is defined by the Health Insurance Portability and Accountability Act (HIPAA). PHI is individually identifiable health information that relates to the:
    - Past, present or future physical or mental health or condition of an individual.
    - Provision of health care to the individual by a covered entity (for example, hospital or doctor).
    - Past, present or future payment for the provision of health care to the individual.
    - PHI shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.
- ***Personal Information*** is data in electronic or paper form that contains personal data about a person such as their first name and last name or first initial and last name of a person in combination with any one or more of the following:
    - Social Security number.
    - Driver's license number or state-issued identification card number.
    - Financial account number (e.g., bank account) or credit or debit card number that would permit access to a person's financial account, with or without any required security code, access code, personal identification number or password.
    - For the purposes of this policy, PI also includes passport number, alien registration number or other government-issued identification number.

ENTITIES AFFECTED BY THIS POLICY:

All departments, faculty, staff, students, non-employees, and guests of ICR Florida Education.

REQUIREMENTS:

- *Security Management* - The security of corporate information, applications, systems, and networks is fundamental to the continued success of ICR Florida Education. Security management seeks to establish controls and measures to minimize the risk of loss of information and system resources, corruption of data, disruption of access to the data, and unauthorized disclosure of information. Security management is achieved through effective policies, standards, and procedures that will ensure the confidentiality, integrity, and availability of ICR Florida Education information, applications, systems, and networks for authorized Users.
- *Confidentiality* - Confidentiality relates to the protection of information from unauthorized access regardless of where it resides or how it is stored. Information that is sensitive or proprietary needs to be protected to a higher level than other information.
- *Integrity* - Integrity is the protection of information, applications, systems, and networks from intentional, unauthorized, or accidental changes. It is also important to protect the processes or programs used to manipulate data. Users accessing sensitive information, applications, systems, and networks must be identified and authenticated.
- *Availability* - Availability is the assurance that <Organization> information and resources are accessible by authorized Users as needed. There are two issues relative to availability: denial of services caused by a lack of security controls (e.g., destruction of data or equipment, a computer virus) and loss of services from information resources due to natural disasters (e.g., storms, floods, fires).
- *Authentication* - Authentication requires that the origin of a message be correctly identified with assurance that it is not a false or forged identity. Passwords are used to authenticate a User based upon the fact that only the User should know the password. Strong passwords will be used and must contain several rules such as combinations of letters and numbers with combinations of upper and lower cases. One-time passwords will also be implemented for high-risk applications as well as encryption to provide the authentication security service to identify the origin of messages. In addition to the use of passwords, Multi-factor Authentication must be implemented where it is possible and appropriate.
- *Information Assets* - All information, data, applications, networks, and equipment are the property of ICR Florida Education and are provided to its employees so that they can conduct their job responsibilities effectively. These assets should be treated with privacy and confidentiality in line with the Information Classification and Handling Policy when conducting business and should not be made available or accessible to anyone outside the enterprise without specific written permission of the Chief Executive Officer. ICR Florida Education information and information processing infrastructure are vital assets requiring protection commensurate with their value. Organizational information, applications, systems, and networks must be actively managed to ensure security, confidentiality, integrity, and availability
- *Accountability* - ICR Florida Education administrative and computing environments will maintain consistent standards for establishing the accountability and authenticity of system Users, which will be compatible with internal accounting control standards prescribed by ICR Florida Education. These environments will develop unique standards for protecting information, applications, systems, and network resources contained within these environments that will be commensurate with fulfilling the mission of ICR Florida Education maintaining the integrity of those will implement critical resources. To maintain accountability for system ICR Florida Education will implement the following access:
    - All individuals with access to the systems will use a User ID that has been authorized by company management and specifically assigned to that individual. Sharing of User IDs is prohibited except in specific, approved situations.
    - All individuals with network, system, and application User IDs will retain a confidential password that will be used to authenticate the identity of the individual. Intentional disclosure or sharing of passwords is prohibited.

PROCEDURES:

RISK MANAGEMENT

ICR Florida Education will establish a risk management program that includes identifying critical information systems and performing a risk self-assessment annually. Departments are required to identify critical information control. Departments will classify and secure information according to its sensitivity to adhere to federal and state laws.

The classified data (either in electronic or paper form) may include "Personal Information" such as student data or a combination of "Personal Information" and "PHI" such as employee data. All student records will be handled in accordance with and complying with FERPA regulations.

Departments will devise local policies and procedures for protecting sensitive information in their care. IT will establish a program to identify and resolve critical vulnerabilities in all campus information systems. Any critical vulnerability found must be resolved in a timely manner.

ACCESS CONTROLS

No one may access confidential records unless specifically authorized to do so. Even authorized individuals may use confidential records only for authorized purposes. Each authorized user (specific individual) is assigned a unique password that is to be protected by that individual and not shared with others, difficult to crack, and deleted when no longer authorized. Users are responsible for creating and protecting passwords that grant them access to resources.

Passwords must adhere to the following policy:

- Passwords must be complex. Passwords must be ten or more characters long.
- Password must contain characters from all of the following four categories:
  - Uppercase characters A-Z (Latin alphabet)
  - Lowercase characters a-z (Latin alphabet)
  - Digits 0-9
  - Special characters **(@, !, $, #, %, etc.)**
- Users must change passwords on all computer systems (Microsoft 365, Populi, Campus IVY, etc.) at minimum every 90 days
- Multifactor Authentication must be enabled on individual applications to protect the integrity of the user account and to prevent compromise.

IT and all Departments shall maintain and periodically review user access privileges and revise them as required by changes in job function, transfers, and affiliation with ICR Florida Education.

Individuals must take care to ensure that their systems are configured to prevent unauthorized access. When remote access is allowed, special care shall be taken to select safe implementation options and ensure that passwords and other access controls are respected. Remote access to the campus network shall use the most secure communications method where possible.

IT will ensure that controls are in place to avoid unauthorized intrusion of systems and networks and to detect efforts at such intrusion.

PHYSICAL SECURITY

Appropriate controls must be employed to protect physical access to resources, commensurate with the identified level of acceptable risk. These may range in scope and complexity from extensive security installations to protect a room where network devices are located, to simple measures taken to protect a user's display screen. Users shall provide physical security for their information technology devices. Access to secure areas should be restricted to individuals with job responsibilities requiring them access. Authorized visitors shall be supervised. Locks, cameras, alarms, etc. must be installed in technology closets to discourage and respond to unauthorized access.

ICR FLORIDA
EDUCATION

- **CREDIT CARD PCI COMPLIANCE**

ICR Florida Education is committed to maintaining compliance with the Payment Card Industry Data Security Standards (PCI DSS) to protect payment card data regardless of where that data is processed or stored. All staff members must adhere to these standards to protect our customers and maintain the ability to process payments using payment cards.

ICR Florida Education prohibits the retention of complete payment card primary account numbers (PAN) or sensitive authentication data in any college system, database, network, computer, tablet, cell phone, or paper file. Storing truncated numbers, in approved formats (first six digits or last four digits) is permissible.

Goals and PCI DSS Requirements

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti- virus software or programs. 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know. 8. Identify and authenticate access to system components. 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

- **COMPUTER SECURITY**

All computers (i.e., workstation, desktop computers, notebook computers, personal digital assistants and any other portable device used for ICR Florida Education work or accessing college information that processes/transmits/stores data) must be secured against unauthorized access. The level of controls must be commensurate with the information accessed, stored, or processed on these devices. All microcomputers must be secured using user identification and password. Standard virus protection programs must be installed, updated, and maintained on all computers connected to the computer network. Computer Operating Systems (e.g., Microsoft Windows) and third-party applications must be patched monthly to maintain computer integrity.

- **NETWORK SECURITY**

IT will maintain network security through a combination of technologies including, but not limited to, switched networks, strong authentication, encryption, intrusion detection/prevention systems, and firewalls where appropriate. IT will periodically check the network and network servers for vulnerabilities, using software tools designed for this purpose.

- **DISASTER RECOVERY AND BUSINESS CONTINUITY**

IT will implement and regularly update, and IT disaster recovery process to counteract interruptions to ICR Florida Education activity and to protect critical processes from the effects of failures or damage. Data and software essential to the continued operation of critical ICR Florida Education functions will be backed up by IT. This includes cloud applications such as the ICR Florida Education Microsoft 365 and SharePoint environments and the Intuit QuickBooks Online application that can be backed up by third party tools. Environments such as Campus IVY must be backed up by the vendor on a regular basis and they must provide certification of data retention.

The security controls over the backup resources will be as stringent as the protection required of the primary resources. Backup of data and software stored on centrally administered computer systems is the responsibility of IT. Each department is responsible for developing, testing, and maintaining a business continuity plan consistent with ICR Florida Education standards.

- **INFORMATION SECURITY AWARENESS PROGRAM**

IT shall implement a security awareness program and shall provide information and further training in information security matters to answer requirements. All ICR Florida Education staff will receive information security awareness training annually.

- **INCIDENT HANDLING AND REPORTING**

Users must report suspected or known compromises of information resources, including contamination of resources by computer viruses, to their managers. Users shall cooperate with any investigation. Incidents will be treated as confidential unless there is a need to release specific information.

- **ENFORCEMENT**

Failure to comply with this policy may result in immediate deactivation of the user's account or denial of network access to the user's device. Disciplinary action may also be taken, including employment termination. ICR Florida Education may routinely monitor network traffic to assure the continued integrity and security of college resources in accordance with applicable policies and laws.

K. REVIEW OF POLICY AND PROCEDURES

This policy will be reviewed annually or as state and federal regulations are revised and necessitate a change in the policy or procedures.

ICR FLORIDA
EDUCATION

APPENDIX A
SECURITY AND PRIVACY INCIDENT REPORT

INSTRUCTIONS: This report (Section 1) shall be completed to the extent possible by the person reporting or involved in a security or privacy incident (or their manager/supervisor). If the Reporting Individual does not initially have enough information to complete the report currently, fill out as much as possible.

DO NOT DELAY reporting this or any other incident, even if the incident is not yet confirmed!

All suspected information security and privacy incidents must be reported to the office of the CEO within one hour of initial detection.

Section 1: Incident Information

(This section to be completed by the Reporting Individual to the extent possible at the time of the report.)

Date/Time of Initial Report: Date/Time

Activity First Detected: Incident Tracking

Number:

<table>
<tr><th colspan="4">Reporting Individual Contact Information</th></tr>
<tr><th colspan="2">First Name</th><th colspan="2">Last Name</th></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><th>Office Number</th><th>Cell Number</th><th>Dept</th><th>Email</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

PII/PHI Breach Information	
Is PII/PHI suspected to be compromised (Yes/No)?	
(If Yes) Estimated Total Number of PII/PHI Records Impacted:	
(If Yes) Estimated Total Number of Users Impacted:	

Incident Description *(Please describe the incident. This section should be updated as the incident is handled.)*	**Last Update Date/Time**
How was this incident detected/discovered?	
What triage/analysis has been performed?	
Is the incident contained? How?	
What recovery/remediation action has taken place?	

Section 2: Estimated Incident Impact

Functional Impact

□ No Impact

□ Minimal Impact to Non-Critical Services

□ Minimal Impact to Critical Services

□ Significant Impact to Non-Critical Services

□ Denial of Non-Critical Services

□ Significant Impact to Critical Services

□ Denial of Critical Services/Loss of Control

Information Impact

□ No Impact

□ Suspected But Not Identified

□ Privacy Data Breach

□ Proprietary Information Breach

□ Destruction of Non-Critical Systems

□ Critical Systems Data Breach

□ Core Credential Compromise

□ Destruction of Critical System

Recoverability

□ Recoverable

□ Not Recoverable

Attack Vector

□ Unknown

□ External/Removable Media

□ Improper Usage

□ Loss or Theft of Equipment

□ Impersonation/Spoofing

□ Attrition

□ Web

□ Email/Phishing

□ Other

Location of Observed Activity

□ – Unknown

□ L1 – Critical Systems (Financial, Campus IVY)

□ L2 – Hosted Student Application (e.g., Populi, Microsoft 365

□ L3 – Campus Network

□ L4 – End User Computer