JOLIET JUNIOR COLLEGE 1901

BOARD POLICIES

| DIVISION | ADOPTION DATE |
|---|---|
| X Information Technology | 05/2006 |
| **POLICY NAME** | **REVISIONS** |
| 10.01.00 Information Security Governance | Revised: 05/2021 |

10.01.00 INFORMATION SECURITY GOVERNANCE

**Introduction**

Joliet Junior College (College) is committed to protecting the confidentiality, integrity, and availability of information assets owned, leased, or entrusted to the College. This policy and associated procedures provide direction and support to campuses for information security, in accordance with College requirements and relevant laws and regulations. The College information security practices are designed to promote and encourage appropriate use of information assets and are not intended to prevent, prohibit, or inhibit the sanctioned use of information assets as required to meet the College's core mission and campus academic and administrative purposes.

**Scope**

The College expects all users, including students, faculty, staff, administrators, other employees, contractors, vendors and others who access the College's electronic information resources to adhere to this policy. Unauthorized modification, deletion, or disclosure of information assets can compromise the integrity of the mission of the College, violate individual privacy rights, and possibly constitute a criminal act.

The College retains ownership and stewardship of information assets owned or leased by the College or entrusted to the College. The College reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to others. This can include, but is not limited to the following actions: monitoring communications across the College network, monitoring the actions on College information systems, checking for security vulnerabilities, disconnecting information systems that have become a security hazard, or restricting data to/from College information systems and across network resources.

This policy applies to all users, including students, faculty, staff, administrators, other employees, contractors, vendors, guests, visitors and members of the general public who use the College's technology resources.

Implementation procedures supporting this policy must be adhered to and may be adapted or enhanced by each department to more fully address unique department security needs through consultation with campus officials and key stakeholders.

## Roles and Responsibilities

### College President

The role of the College President regarding information technology is to oversee and provide support to ensure College compliance with this policy in accordance with all existing local, state and federal laws pertaining to the security of College information and systems, along with the protection of the confidentiality, availability, and integrity of all data on such systems.

### Information Security Officer (ISO)

The role of the Information Security Officer (ISO) is to establish policy and procedures to protect the integrity of confidential and personal information. The ISO also has responsibility for investigating any potential breaches of this information.

### Chief Information Officer (CIO)

The role of the Chief Information Officer (CIO) is to lead the College's activities regarding information technology. The CIO will lead Information Technology (IT) staff in carrying out the College's technology support for information security, ensuring the security of all College information systems and protecting the confidentiality, availability, and integrity of all data on such systems.

### Administrative Staff (Vice Presidents, Deans, Directors, and other supervisory personnel)

The responsibilities of administrative staff include those of all campus users, in addition to the following responsibilities:

A. Authorize access to information systems for subordinates.
B. Designate a representative to communicate with the Information Security Office and be a member of the Information Security Incident Response Team (ISIRT).
C. Ensure subordinates have completed any and all confidentiality compliance forms.
D. Ensure subordinates have received appropriate training regarding computer security and handling of confidential information.

### Information Technology Personnel

All Information Technology Personnel are expected to comply with all responsibilities of campus users, in addition to the following responsibilities:

A. Confirming user identity when resetting user passwords.
B. Maintaining password security by not requesting user passwords at any time.
C. Not providing access to unauthorized external entities. Vendor, auditor or consultant access to any information system required to perform the scope of work initiated by the College must be approved by the Director of IT prior to access through the use of the College Third Party Network Connection Agreement form.

D. Reviewing and signing a confidentiality (non-disclosure) agreement related to the position's access to data, which is stored in their personnel file.

**All Campus Users**

All campus users, including vendors, are expected to comply with all federal, state and local laws pertaining to the protection of confidential information as well as campus policies meant to protect the security of information systems on campus. The responsibility of each and every campus user includes, but is not limited to:

A. Using secure passwords, per the College Password Guidelines provided by Information Technology to faculty, staff, and students via the portal to access any campus computer used to access the campus network.
B. Keeping the computer monitor and desktop area clear of any hand-written passwords.
C. Not sharing passwords with coworkers and student employees.
D. Securing all computers from unauthorized access when unattended.
E. Securely destroying all instances of files, digital or paper, containing identifying personal information (e.g. Social Security Number, driver's license number, etc.) per the College Records and Disposal Manual.

## Enforcement

Individuals or groups who act in a manner contrary to existing policy for information security or who take actions which have legal implications are subject to appropriate disciplinary sanctions. The College reserves the right, at all times, to suspend or revoke the privilege of access to College Technology Resources.

Violations of this policy, including the supporting core procedures, shall be cause for discipline. Alleged violations shall be subject to, but not limited to, the procedures outlined in the College Board Policies, College collective bargaining agreements, Employee Handbooks, Student Worker Handbook, Student Handbook, and the Student Code of Conduct. External service providers found to have violated this policy and the core procedures may be subject to financial penalties, up to and including termination of contract. The College treats violations of security policies seriously and will pursue criminal and civil prosecution of violators when appropriate.

## Amendments to Policy and Procedure

This policy shall be updated to reflect changes in the College's academic, administrative, or technical environments, or applicable federal/state laws and regulations. The College Information Security Office shall be responsible for overseeing a bi-annual review of the policy and procedures.

The College reserves the right to amend or otherwise revise this document as necessary to reflect future changes made to its technology resources. Employees, Faculty Staff, Students, Administrators, Visitors, Guests, Vendors and contractors (hereafter referred to as Users) are responsible for reviewing this Policy periodically to ensure continued compliance with all College policies, standards, procedures, and guidelines.