

<b>DIVISION</b>	<b>REFERENCE NO.</b>
X. Information Technology	10.2 (1)
<b>CATEGORY</b>	<b>DATE</b>
10.2 Information Security Governing Policy	Adopted 5/06

**Purpose**

The Information Security Governing Policy (the “Policy”) serves to create an environment where the College’s electronic information resources, including data, applications, systems, hardware, networks, and software, are protected from information security threats that could compromise the privacy, integrity, physical security, and availability of these valuable assets. These assets are at risk from potential threats such as abuse from either internal or external users or physical disasters that threaten business continuity. The College’s goals for risk reduction are based on the principle that the level and type of security should reflect an assessment of the criticality of that information resource to the operation of the College, the sensitivity of the data residing in or accessible through the information resource, the cost of preventive measures and controls designed to detect errors or irregularities, and the amount of risk that management and the Board of Trustees is willing to take.

Any deviation from this Policy requires written approval by the President or the Board of Trustees. In the event that federal or state laws govern certain types of information resources, e.g. FERPA, that policy will take precedence.

General Policy is set forth in the following sections: the scope of the Policy, user classification, general policy, core procedures, exceptions, implementation, and enforcement.

**Scope**

This policy applies to all campuses of JJC and all of its members; students, faculty, staff, contractors, consultants, guests, volunteers and other members of the College community; including those who are affiliated with third parties, who access the College’s electronic information resources, must follow this Policy. This Policy applies to all electronic information resources either owned or used by the College under license or contract. Electronic information resources include application systems, operating systems, tools, communications systems, data – in raw, summary, and interpreted form – and associated computer mainframe, server, desktop, communications and other hardware used in support of the College’s administration or instructional delivery.

**User Classification**

All members of the College community share in the responsibility for protecting information resources for which they have access or custodianship. Each member will fall into one or more of the following classifications:

- **Users** - All members of the college community are “Users” of JJC’s information resources, even if they do not have responsibility for managing the resources. Users include, for example, students, faculty, staff, contractors, consultants, and temporary employees.

<b>DIVISION</b>	<b>REFERENCE NO.</b>
X. Information Technology	10.2 (2)
<b>CATEGORY</b>	<b>DATE</b>
10.2 Information Security Governing Policy	Adopted 5/06

- **Data Owners** - Responsible for information resources which are under their control. Ensure compliance with the College’s Policies and all Federal, State, and local laws regarding the information resource.
- **Systems Administrators** - Individuals in departments that manage significant information resources and systems for the purpose of making those resources available to others. They face more extensive requirements than users.

**Core Procedures**

The following are the core procedures governing Joliet Junior College: User Access and Accountability, Password, Physical Security, Business Continuity Planning/Disaster Recovery, Data Classification, Remote Access, Wireless Communication, Email, Storage Quota, Instant Messaging, Anti-Virus, Guidelines on Anti-Virus Process, Extranet, Virtual Private Network (VPN), Perimeter Firewall, Network Equipment, Software and Related Services Acquisition, Router Security, Server Security, Internet DMZ Equipment, Remote Control of End User Workstations and Security Patch Management Compliance, Incident Handling/Reporting, and Change Control. The Chief Information Security Officer (CISO) shall be responsible for recommending new or revised procedures for consideration and approval by the Technology Advisory Council.

**Exceptions**

In certain cases, compliance with specific policy requirements may not be immediately possible. Reasons include, but are not limited to, the following:

- Required commercial or other software in use is not currently able to support the required features;
- Legacy systems are in use which do not comply, but near-term future systems will, and are planned for;
- Costs for reasonable compliance are disproportionate relative to the potential damage.

In such cases, departments must develop a written explanation of the compliance issue and a plan for coming into compliance with the College’s Information Security Policy in a reasonable amount of time. Explanations and plans must be submitted to the CISO, who will involve the Information Security Policy Committee in the review process.

**Implementation**

The Technology Advisory Council (TAC) is responsible for adopting general procedures for the implementation of this policy. Academic or Administrative areas/units may adopt additional procedures for the use of their own systems and are responsible for making this policy and those procedures available to all users.

<b>DIVISION</b> X. Information Technology	<b>REFERENCE NO.</b> 10.2 (3)
<b>CATEGORY</b> 10.2 Information Security Governing Policy	<b>DATE</b> Adopted 5/06

**Enforcement**

Violations of this policy, including the supporting core procedures, shall be cause for discipline. Alleged violations shall be subject to the procedures outlined in the Joliet Junior College Board Policies, Personnel Procedures Manual, College collective bargaining agreements, the 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 Joliet Junior College treats violations of security policies seriously. The Joliet Junior College will pursue criminal and civil prosecution of violators when appropriate.