

**SCOPE:** This policy applies to all University Users (as defined below) in their use of and access to University information, information systems and supporting infrastructure (as defined below). As used throughout, the term “University” shall be understood to include all entities within the University of Rochester.

**PURPOSE:** The information assets of the University must be available to the University community, protected commensurate with their value and legal requirements, and must be administered in compliance with federal and state law. Reasonable measures shall be taken to protect these assets against accidental or unauthorized access, disclosure, modification or destruction, as well as to reasonably assure the confidentiality, integrity, availability, and authenticity of information. Reasonable measures shall also be taken to promote the availability, integrity, and utility of information systems and the supporting infrastructure, in order to protect the productivity of members of the University community, in pursuit of the University mission.

### **POLICY STATEMENT:**

Therefore, the University will:

1. Designate one or more individuals to identify and assess the risks to non-public or business-critical information within the university and establish a University information security plan.
2. Develop, publish, maintain, and enforce information security policies, procedures and procedures for protection of University information, information systems and supporting infrastructure.
3. Provide training to authorized university users in the responsible use of information, applications, information systems, networks, and computing devices.
4. Encourage the exchange of information security knowledge, including threats, risks, countermeasures, controls, and best practices both within and outside the university.
5. Periodically evaluate the effectiveness of information security controls in technology and process.

**PROCEDURES:** Compliance with information security procedures developed pursuant to this policy will be mandatory. Violations of the procedures will constitute violations of this policy. Any division within the University may have additional, more restrictive Information Security policies or procedures which must be followed. For the Medical Center and its affiliates’ policies and procedures please see <http://intranet.urmc-sh.rochester.edu/policy/hipaa/policymanual/>.

**DEFERRALS:** Deferrals to this policy and the procedures may be granted for certain specific types or sets of information, systems and networks. Therefore, a Deferral Procedure is established to approve and document requests for deferrals to this policy and the procedures. The Deferral Procedure allows University leadership to make an informed decision on whether or not the requested deferral to this policy or the procedures should be allowed. No deferral will be permitted unless the Deferral Procedure has been followed and approved.

---

**ENFORCEMENT:** Violations of this policy and the procedures will be handled under normal University disciplinary procedures applicable to the relevant persons or departments. The University may suspend, block or restrict access to information and network resources when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of University resources or to protect the University from liability. The University may refer suspected violations of applicable law to appropriate law enforcement agencies.

Violations of this policy and the procedures can result in disciplinary action up to and including separation from the University and/or exclusion from University programs, facilities and privileges. Violations of law can lead to fines and imprisonment.

In the event of an information security breach caused by a violation of this policy or the procedures, departments and divisions whose staff, faculty or students are responsible may be required to bear the resulting costs, which may include the costs of notifications to affected individuals, legal fees, and/or fines, settlements or judgments.

### **DEFINITIONS:**

**University information, information systems and supporting infrastructure:** Information in its analog and digital forms and any media, software, hardware or other technology that support the use of information.

**University Users:** includes authorized university faculty, staff, students, volunteers, as well as contractors, (including outsource-partners or cloud providers) using any of the university information, information systems and supporting infrastructure.