1120 Ruthven Building
1109 Geddes Avenue
Ann Arbor, MI 48109-1079

Ravi Pendse and Sol Bermann shared a number of links that help articulate some of the policies and practices in this space:

- SPG 601.07 - Responsible Use of Information Resources (which, among other things, allows for limited personal use of U-M information resources)
- SPG 601.11 - Privacy and the Need to Monitor and Access Records (which defines the rights, responsibilities, and expectations of the University and its employees regarding the conditions under which they may access records and monitor record systems)
- Role of ITS in supporting appropriately approved investigations (includes a link to the ITS IA Standard Investigatory Support Process)
- ITS Information Assurance Operational Transparency (describes some of the methods and protocols used to appropriately secure the U-M IT environment while also protecting the privacy of students, faculty, and staff)

Both Ravi and Sol are available for questions and further discussion.

Please see the following pages for the Information Assurance Standard Investigatory Support Process.

INFORMATION AND TECHNOLOGY SERVICES
UNIVERSITY OF MICHIGAN

Information Assurance Standard Investigatory Support Process

Requesting Parties:	Office of General Counsel	Law Enforcement	Student Life	Office for Institutional Equity	Human Resources	UMOR/Academic Integrity	Next of Kin
Authorized source for routine and sensitive requests:	OGC attorneys	Law Enforcement Officer with appropriate legal documents	Dean of Students or Crisis Management Team	OIE staff investigators	HR Partner, Unit HR official	UMOR Investigator, Department Administrator	Holder of Power of Attorney or court documents
Authorized source for highly sensitive requests:	General Counsel, Deputy General Counsel	Law Enforcement Officer with appropriate legal documents	Vice President for Student Life	Director of OIE	VP University HR	VP Research, School, College Dean	Holder of Power of Attorney or court documents

Request Submission Guidelines: Send email with details of request and supporting documentation to security@umich.edu
FOIA Requests: Do not need review or approval, so long as the request comes from the U-M FOIA office. Requests should be sent to security@umich.edu

Request Type:	**Routine** Involving disclosure that could cause limited harm to individuals and/or the university*	**Sensitive** Involving disclosure that could cause significant harm to individuals and/or the university*	**Highly Sensitive** Involving disclosure that could cause severe harm to individuals and/or the university*
Required Review:	• Information Technology User Advocate	• Information Technology User Advocate • Chief Information Security Officer	• InformationTechnology User Advocate • Chief Information Security Officer • Office of General Counsel
Required Consultations:	• None required; may consult with Office of General Counsel and others as needed	• Office of General Counsel and others as needed	• VPIT and Chief Information Officer • VP and General Counsel
Required Approvals:	• Chief Information Security Officer	• VPIT and Chief Information Officer • Chief Information Security Officer • Others as needed	• VP and General Counsel • VPIT and Chief Information Officer • Other Executive Officers as appropriate
Required Documentation:	• Documentation outlining justification of request	• Documentation outlining justification of request • Documented approvals	• Documentation outlining justification of request • Documented approvals

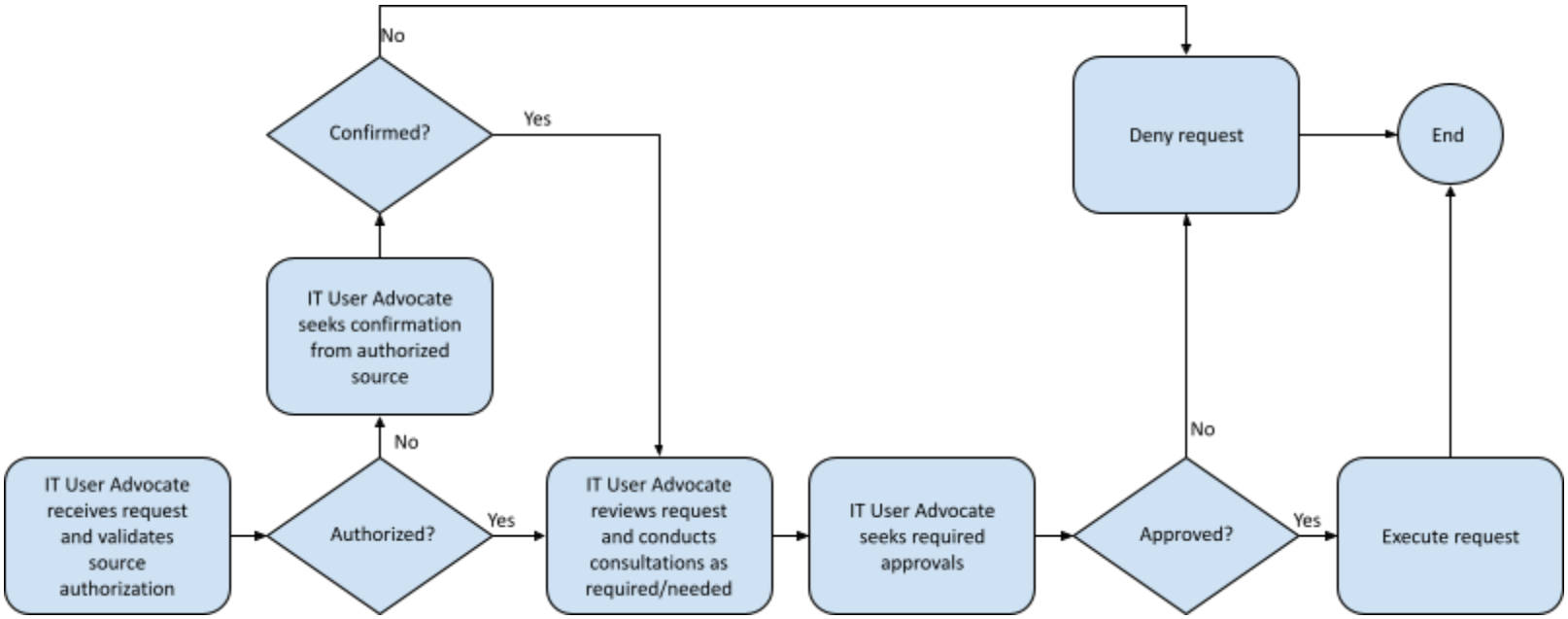
* Aligned with U-M Data Classification Levels at https://safecomputing.umich.edu/protect-the-u/safely-use-sensitive-data/classification-levels
** At no time should ITS staff directly provide information without engaging IA for consultation

Information Assurance Standard Investigatory Support Process

Examples of Requests for Investigation

Request Type:	**Routine** Involving disclosure that could cause limited harm to individuals and/or the university*	**Sensitive** Involving disclosure that could cause significant harm to individuals and/or the university*	**Highly Sensitive** Involving disclosure that could cause severe harm to individuals and/or the university*
Examples:	• Business continuity related to U-M staff (termination, death, etc.) • Next of kin • Routine investigations • Student wellness checks • Request to preserve data	• Business continuity related to faculty • Investigations related to faculty or U-M Deans, Directors, and Department Heads (3D-level staff) • Investigations and requests related to sensitive or controversial matters • Routine Law Enforcement Investigations/Requests	• Business continuity related to Executive Officers, Deans, Regents, and other high-ranking U-M officials • Investigations related to Executive Officers, Deans, Regents, other high-ranking U-M officials, and student athletes • Extraordinary Law Enforcement Investigations/Requests (ex: FBI)

Request Processing Flow**



* Aligned with U-M Data Classification Levels at https://safecomputing.umich.edu/protect-the-u/safely-use-sensitive-data/classification-levels

** At no time should ITS staff directly provide information without engaging IA for consultation