Requests for Exception to Information Security Policy

I. Overview
The university community is expected to comply with information technology security policies and standards in order to provide for consistent protection of institutional information assets, and to ensure that individuals and units not assume an unreasonable IT security risk on behalf of the entire university.

However, in an institution as complex as U-M, there will be situations where the strict application of a policy or standard would significantly impair the functionality of a service, application, or research program. In such instances, this Standard provides for an exception process that:

- Accommodates specific circumstances where utilizing the security controls identified in Information Security and Assurance (SPG 601.27) and the associated supplemental Standards are not practicable, and
- Approves a variation from normally required policy compliance.

II. Scope
This Standard applies to the Ann Arbor, Dearborn, and Flint campuses, as well as all schools, colleges, institutes, and the U-M Health System. This Standard specifically applies to all units, faculty, principal investigators, and staff who maintain or store high or restricted data on any device that connects to the campus network and who are requesting an exception to SPG 601.27 or any of its supplemental Standards.

III. Standard
Under limited circumstances, units or individual faculty, researchers, and staff may submit an exception request that will be evaluated as follows:

1. Units, faculty, researchers, or staff should work with their Security Unit Liaison (SUL) or Information Security Liaison (ISL) to identify systems, applications, or research projects that maintain or store high or restricted data on any device that connects to the campus network and that potentially are or will not be not in compliance with requirements of SPG 601.27 and its supplemental Standards.
2. If a compliant solution or change to a business or research process is not feasible, the SUL or ISL should request an exception using the IT Security Compliance Exception Request Form [not yet designed]. Exception requests should include, as appropriate:
   a. System, application, or research project specific to the exception
   b. Prohibitive technical, operational, or financial obstacles to compliance
   c. Self-assessment of risk associated with non-compliance
   d. Plan, if any, for compensating or alternative controls
   e. Signature acknowledgement of designated unit authority
3. The exception request is then sent to the Office of the Chief Information Security Officer. Exception requests will receive a response within five (5) business days of receipt.
4. In general, the only reasons that will justify an exception being granted are
   a. When compliance adversely affects significant business or research objectives and another acceptable solution with equivalent protection is available;
   b. When the risks of non-compliance are outweighed by the compliance costs.
      Temporary exception, where immediate compliance would disrupt critical operations;
   c. When a legacy system is being retired, and a determination is made to avoid the staff and financial resources it would take to bring the system up to current requirements and the risk can be managed up to the retirement.
5. The Office of the Chief Information Security Officer, or Information and Infrastructure Assurance (IIA) as a delegated authority, will evaluate exception requests on a case-by-case basis, accounting for level of risk, potential threats and vulnerabilities, cost analysis, available staff resources, other priority commitments, and operational and technical limitations or constraints. IIA may involve additional stakeholder and subject matter experts during the evaluation process.
6. IIA may approve compensating controls for the assigned data security level to maintain security and reduce risk when certain standard controls prescribed for that level are not feasible. These compensating controls must be documented and agreed to by the requestor and IIA. IIA may also grant a short-term, temporary exception while working with the requester to establish a timeline for full compliance,
7. The Chief Information Security Officer, or IIA as a delegated authority, will approve or deny the request for an exception. Denied requests can be appealed to the Vice President and Chief Information Officer [position currently being hired] for a final review.
8. Temporary exceptions are valid for up to one year. When an exception expires, IIA will contact the requester to determine whether there is a continuing need for the exception. All other approved exceptions remain in force unless there is a significant change that requires a reevaluation.
9. Units, faculty, researchers, and staff that have been granted an exception to the information security policy or Standards should be especially vigilant to report an IT security incident within 24 hours of becoming aware of the incident.

IV. Violations and Sanctions
Non-compliant systems or applications that pose significant risk to the campus network or information resources may face removal from the network or other take-down action.

Any U-M department or unit found to have violated this Standard may be held accountable for the financial penalties, legal fees, and other remediation costs associated with a resulting information security incident and other regulatory non-compliance.
V. References
Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan (SPG 601.07)
Institutional Data Resource Management Policy (SPG 601.12)
Information Security Incident Reporting Policy (SPG 601.25)
Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data (SPG 601.33)
Statement on Stewardship-Stewardship of Information and Technology Resources

VI. Related NIST Security Controls