Process for Requesting High Risk Confidential Information
From Harvard Systems

The use of high risk information\(^1\) in local business processes is discouraged. When required, it must be used only with approval of the University or School CIO. Existing applications that use high risk information at present are subject to annual review for re-certification.

This approval process for requesting high risk confidential information must be completed as a prerequisite and updated annually. See form.

1. The requester must document the purpose for which the information is being requested. The description must include sound justification.

2. The requester must document the additional protections that will be employed to keep the high risk information secure. These protections must be in accord with the Enterprise Security Policy.

3. When the business purpose, justification, and protection description have been documented, the requester must send this to the approver of the data source from which the information is requested.

4. The approver will review the request, indicate whether this is an existing data transfer, and will forward to the University Technology Security Officer (UTSO).

5. The UTSO will review and work with the requester to obtain additional information or to clarify the request if needed.

6. The UTSO will send the request, along with a recommendation, to the CIO for review and a decision to be made after consultation by the CIO with the appropriate Vice President and relevant business leaders.

7. The CIO will inform the UTSO of the decision and will retain a copy in the CIO’s files for future reference and annual review of approved requests.

8. The UTSO will inform the requester and the data owner about the outcome of the request. If the CIO has approved it, the requester may then initiate the process for requesting the information.

9. If a request for high risk data is approved, the requester must arrange for a system audit through Harvard Risk Management and Audit Services (RMAS) prior to receiving access to high risk data.

---

\(^1\) First and last name or first initial and last name in combination with SSN, MA license or ID number, financial account or credit card number or biometric indicator.

Updated: 10/10/12