HARVARD
Information Security

High Risk Confidential Information Request COVER

The undersigned have agreed that this Request for High Risk Confidential Information meets the requirements of the Harvard Enterprise Security Policy. This request must be reviewed for approval on an annual basis.

School or Unit Name	
Application Name	
Business Owner	Signature Date
Practice Manager (if applicable)	Signature Date
School or University Security Officer	Signature Date
School or University CIO	Signature Date

HARVARD
Information Security

High Risk Confidential Information Request DIRECTIONS

Use this form to request access or to use high risk confidential information for server-based applications. High-Risk Confidential Information includes a person's name in conjunction with the person's Social Security, credit or debit card, individual financial account, driver's license, state ID, or passport number, or a name in conjunction with biometric information about the named individual. High-risk confidential information also includes personally identifiable human subject information and personally identifiable medical information.

Please note that Massachusetts law requires Harvard to:

1. Only collect the HRCI for which we have a stated business reason.
2. Only permit access to the HRCI by those people who have a specific business reason to access it.
3. Only keep the HRCI as long as there is a specific business reason to keep it.
4. Properly destroy the data when we no longer need it.

Thus, the HRCI Request must be very specific. For example, statements addressing business requirement and retention of HRCI should be similar to the following.

> “This business unit must keep the SSNs of loan holders for 2 years after the loan is paid off because federal law XXXX requires it. On average the unit retains 1234 SSNs of this type.”

In all cases, the owner of the application receiving the high risk confidential information must re-apply for certification annually.

HARVARD
Information Security

High Risk Confidential Information Request DESCRIPTION OF PURPOSE

I. Describe the Business Purpose of the Application.

1	Date	
2	Name of Business Owner	
3	Business Owner Department	
4	High Risk Confidential Information (HRCI) requested	
5	Quantity of High Risk Confidential Information. Describe categories and estimate number. Examples: SSNs of all employees (17,000); Passport numbers of employees currently on foreign travel (500)	Category_______ Number________
6	Business requirements relating to the High Risk Confidential Information. a. Specify the reason for needing the information. b. Specify how long the information will be required. c. Specify how the information will be expunged when it is no longer required.	Reason_________ Retention_______ Removal________
7	What process will be used to work with the high-risk information? (e.g. use employee SSN when calling external vendor about that employee/one at a time; transfer a file containing all employee SSNs to a external vendor daily; report student SSNs to government annually)	Process___________
8	Who (staff, faculty) will be accessing the high-risk information?	
9	Will they access info about themselves or about others? Include approximate number of people who will be accessing the information.	Themselves________ Others ___________ Number___________
10	Where will the high-risk information be accessed from: (e.g. specific Harvard location; from employee's home).	Describe:
11	Will the high-risk information be forwarded outside of this system either electronically or on paper?	Y/N
12	If yes, explain to whom and what business reason requires that the high-risk information be forwarded.	Explain:

	Note: In most cases the receiver of the high-risk information will have to fill out a copy of this form.	

High Risk Confidential Information Request IT REQUIREMENTS

Describe the Local Environment and Support.

13	Where will the data be stored? Choose all that apply: • On a server housed at Harvard a) operated & maintained by Harvard people b) operated by Harvard people, maintained by vendor or consultant c) operated & maintained by external vendor or consultant • On a service housed, operated and maintained by external vendor • Other (describe).	Note: High Risk Confidential Information can *never* be stored on a user's desktop or laptop computer or any portable device (even if the data is encrypted). Answer:
14	If a server is housed at Harvard: • Where is server housed? • Who operates and maintains the server and software?	Location__________ Server/Software Maintainer________
15	If a server is provided by external vendor: • Does proposed vendor contract include confidential information rider(s)? • Attach a description of vendor security processes and configuration	Y/N Security program attached? Y/N
16	What special processes are proposed to ensure that the high-risk information is protected? Include a description of the encryption method if the information is being transported over a network.	Describe:
17	Can the high risk information be included in reports? If yes, describe the business reason for including the high-risk information in the report(s).	Y/N Describe:
18	If the information is used for development, is developer access to the high risk information controlled? • By having the high risk information only on the production system, not on development and test systems • By disabling developer access o the production system except when specifically needed and	Y/N Describe method:

	logging such access	
19	Please provide any additional supporting information.	