**Brown University**

**Request for Authorization to Use, Store and/or Transmit Social Security Numbers (SSN)**

**Exception Form**

The purpose of this form is to document and gain authorization to use SSN for a specific business process. This business process could include entering in a vendor/developer agreement, a new application or system component, using SSN in an internal/external electronic transmission, storing in electronic/paper form, as a validator or checksum, and/or displaying SSN in some fashion.

Departments currently using, or wishing to collect, store, or use SSNs in any way must:

* Show institutional need,
* Receive approval from the DPRM Steering Committee, and
* Permit audits (including server and application security) at a minimum of annually to ensure safe SSN handling.

Please send completed form to the University’s Chief Information Security Officer at:

CISO

CIS

Box 1885

The CISO will facilitate the review by the Data, Privacy and Records Management (DPRM) Executive Committee. One form must be filled out for each distinct business use of SSN.

The complete University usage and protection procedures can be found at:

<http://www.brown.edu/cis/policy/ssn.php>

**Requesting Department Information**

Business Process/Application Name:

Business Unit:

Department:

Dean/Executive/Director/Chair:

Requestor/Contact Name:

1. Describe the specific purpose for SSN use, indicating the names of the required application or business process, system components, and vendor/developer information. Please include alternatives considered, and why other methods or the use of other forms of identification is insufficient.

|  |
| --- |
|  |

2. For applications/processes both currently in production in in implementation, please document all departments, groups, job positions, or specific individuals who will have access to view the SSN. (Please note: All individuals with privileged access to University-held restricted data, such as SSN, must have completed a confidentiality agreement and have taken the Protecting Brown Information course.)

|  |
| --- |
|  |

3. If SSN will be transmitted or shared, please describe the process. Please include whether SSN are received or transmitted, the purpose, method, frequency and format of transmission, whether or not SSN are encrypted, sent between campus parties or externally, etc.

|  |
| --- |
|  |

4. If SSN will be stored, describe the specific purpose of storage. Please include why the SSN must be stored, where, in what format (electronic, paper, etc.) and for how long it will be stored.

|  |
| --- |
|  |

5. If SSN will be displayed, describe the specific purpose of display. Please include whether you are engaged in data entry and specify the type (automated or manual), if SSN are retrieved from another source, if SSN can be edited, if any application in use displays SSN, if reports are created containing/displaying SSN and how the reports are handled, format they are in and who the audience of the reports is, etc.

|  |
| --- |
|  |

6. Describe any other specific usage, storage or transmission of SSN not previously described within this request.

|  |
| --- |
|  |

**Additional information relevant to this request.**

Requirements:

* All applicable University policy related to Restricted Information and SSN must be met.
* Media Requirements:
* Media used to store/transmit data will be marked “confidential”.
* Media used to store/transmit data will be secure and traceable.
* Media used to store/transmit data will be kept physically secure.
* Media and/or data will be destroyed upon completion of approved use.

Date of Request:

Printed name of requestor:

Requestor’s Phone extension:

Date received by CISO:

Date of DPRM review:

DPRM decision: APPROVED REJECTED

CISO Approval: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DPRM Approval #\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Rev. 11/2012