HARVARD UNIVERSITY
Policy Title: Harvard Research Data Security Policy

Responsible Offices:	Office of the Vice Provost for Research & HUIT Information Security
Effective Date:	July 15, 2020
Revision Data:	February, 2020

INTRODUCTION

Harvard University's Information Security Policy effectively addresses the need to protect confidential and sensitive information that is maintained in the various spheres of University administration. The research setting poses particular information security risks and challenges, including regulatory and contractual constraints that require additional policy provisions and protective measures. While following the Policy Statements of the Harvard Information Security Policy, this Policy provides specific guidance for managing research data.

POLICY STATEMENT

Properly protecting research data is a fundamental obligation that is grounded in the values of stewardship, integrity, and commitments to the providers and sources of the data. This policy is particularly focused on the protection of research data that are confidential by reason of applicable law and regulation, agreements covering the acquisition and use of the data, intellectual property protections, and University policies.

To protect research data appropriately and effectively, the University's researchers, Institutional Review Boards, Information Security Officers, Negotiating Offices and research administrators must understand and carry out their responsibilities related to data privacy and security. The Data Security Levels described in the Harvard Data Classification Table and the corresponding Requirements reflect the basic principle that more exacting security requirements must be implemented as the risk associated with the research data increases.

SCOPE OF POLICY

This Policy and the accompanying Guidance applies to all Research Data, as such term is defined in the Retention and Maintenance of Research Records and Data Frequently Asked Questions guidance, regardless of the storage medium (e.g., disk drive, electronic tape, cartridge, disk, CD, DVD, external drive, paper, fiche, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.), physically housed at Harvard or stored remotely under the management of Harvard researchers. It applies to researchers and research team members who obtain, access or generate Research Data, in particular confidential or sensitive information, and information governed by a contract.

The Policy also applies to the research administrators and reviewing offices working with the Office of the Vice Provost for Research, in assisting researchers in identifying and assessing data confidentiality risks; and Information Security Reviewers working with researchers and research team members to ensure implementation of appropriate security controls for research information.

HARVARD UNIVERSITY
Policy Title: Harvard Research Data Security Policy

Responsible Offices: Office of the Vice Provost for Research & HUIT Information Security
Effective Date: July 15, 2020
Revision Data: February, 2020

I. INTRODUCTION

GUIDANCE

The Harvard community creates and exchanges many types of data and materials while engaging in its research-driven mission to promote the free exchange of academic, scientific and other types of intellectual works. Federal and state laws and regulations, as well as University policies and best practices, impose obligations on the University and its Researchers to protect the confidentiality, integrity and security of such data and information. This Guidance and the accompanying Harvard Research Data Security Policy (HRDSP) focus on proper management and stewardship of Research Data, inclusive of human subjects research, data exchanged pursuant to a data use agreement (DUA), and other data subject to foreign, federal or state regulations, sponsor requirements or intellectual property protections.

II. ROLES & RESPONSIBILITIES

1. Researchers

a. Managing Research Data: Researchers are responsible for creating and maintaining accurate Data documentation in the Harvard Compliance System as required by University policies and complying with approved data security and management plans. This includes:
   i. Implementing the security controls corresponding to the requirements of the Data Security Level (DSL) (for example, access management and destruction requirements);
   ii. Ensuring necessary reviews occur for Sensitive Data, Data exchanged pursuant to a DUA or sponsored award, and Data subject to foreign, federal, or state regulations (e.g. export controls, Family Educational Rights and Privacy Act (FERPA), Federal Information Security Management Act (FISMA), General Data Protection Regulation (GDPR)), or intellectual property protections and recording any relevant reference number on the submission in the corresponding application;
   iii. Developing and adhering to approved Data Security Plan and relevant procedures throughout the course of each project;
   iv. Completing required Research Data Security Training; and
   v. Informing the assigned Information Security Reviewer and of any Incidents (defined in Enterprise Policy) pertaining to the Research Data, in addition to reporting the Incident as required under the Enterprise Policy (see instructions here).

b. IRB and Security Assessments and Determinations: Researchers are responsible for securing reviews from an Institutional Review Board (IRB) and Information Security Reviewer, providing the reviewer with all relevant supporting materials, and documenting the reviewer's determination in the Compliance System. This includes:
   i. For projects with a human subjects research component, Researchers will need to undergo IRB review in the Electronic Submission Tracking and Reporting (ESTR-IRB) Application. During their review, the IRB will make a determination regarding the sensitivity of the Data;

ii. If the Data is determined to be Sensitive, Researchers will create a corresponding record in the Research Safety Application requesting a security review and determination by an Information Security Reviewer and recording any relevant reference number on the submission in the corresponding application; and

iii. For non-human subjects research, Researchers are responsible for making a DSL determination based on the Enterprise Policy and applicable privacy and security concerns.

c. Data Use Agreements: Researchers are responsible for initiating the DUA review in the Agreements Application and facilitating any necessary reviews. This includes:

i. Ensuring that data protection requirements can be met and that all individuals who have access to the Data have received appropriate training on the DUA requirements and relevant policies and procedures related to security and access; and

ii. Creating a corresponding record in the Research Safety Application for any dataset(s) received pursuant to a DUA and recording any relevant reference number on the submission in the corresponding application.

d. Compliance System: Researchers are responsible for submitting review requests and project updates related to their Data in the appropriate application(s) in the Compliance System. Depending on the activity, submissions may be managed in the ESTR-IRB Application, the Agreements Application and/or the Research Safety Application. This includes:

i. Highlighting any known confidentiality and data security obligations, and information about (or a copy of) the relevant data management plan;

ii. Managing modifications and promptly responding to review and renew requests to ensure the record(s) associated with the Data is current;

iii. Recording any relevant reference number to related records on the submission in the applicable application(s), and

iv. Representing the current, accurate data management information including content, location, and approved personnel in the Research Safety Application, and updating such information as necessary.

2. Information Security Reviewers

a. Security Assessment Implementation: Information Security Reviewers are responsible for making a DSL determination for Sensitive Data, providing Researchers with information about methods to bring a Data Security Plan into compliance with the assigned DSL(s), and ultimately determining whether Researchers' use of tools and implementation of security controls is consistent with the Enterprise Policy and any associated DUAs, contracts, etc. This includes:

i. Determining applicable DSLs associated with Research Data, either at the project level or per dataset;

ii. Recording approval of Researchers' intended security controls and DSL determination in the Research Safety Application for projects determined to be Sensitive, and Data received or exchanged pursuant to a DUA or sponsored award;

iii. Supporting Researchers' DSL review and assessment for non-human subject research projects and Data that has been assessed as non-Sensitive;

iv. If certain controls prescribed for the DSL are not feasible, working with the Researchers to apply and approve any compensating controls or other controls for the management of Data under the assigned DSL; and

v. Assigning a review expiry date to each submission in the Research Safety Application to ensure regular record update occurs.

b. Data Use Agreements: Information Security Reviewers are responsible for reviewing and approving Data Security Plans associated with DUAs, as well as the terms of DUAs which contain security requirements that may exceed the bounds of the assigned DSL or otherwise require their expertise. This includes:
   i. Reviewing the relevant issues and recording completion of review in the Research Safety Application, or Agreements Application if a data security ancillary review is requested.

c. Compliance with Data Security Plans: Information Security Reviewers are responsible for reviewing Researchers' requests and updates in the Research Safety Application and ensuring the appropriate renewal process is implemented. This includes:
   i. Confirming with Researchers that requests are consistent with information recorded in the Compliance System (e.g. DUA expiration date, required training, collaborators) and adhere to relevant requirements of Harvard policies;
   ii. Confirming destruction of Research Data, when appropriate; and
   iii. As necessary, limiting access to Data and/or University resources, or taking other corrective actions as may be appropriate in instances of insufficient response to review related inquires or record updates, or identified noncompliance with the responsibilities or requirements set forth in this Guidance or the Enterprise Policy.

d. Training and Education: Consistent with University policies, Information Security Reviewers are responsible for developing and disseminating information security guidance as it relates to Research Data. This may include:
   i. Educating and training University personnel in information security matters;
   ii. Communicating information regarding the Enterprise Policy; and
   iii. Translating the Enterprise Policy into technical requirements, standards and procedures for Researcher use.

e. Institutional Oversight: Through the course of review and any subsequent actions, Information Security Reviewers are responsible for reporting concerns of noncompliance with administrative approvals and institutional policies to the appropriate research oversight bodies for further review.

3. Institutional Review Boards

a. Data Sensitivity Assessment: The IRBs are responsible for assessing data privacy risks associated with human subjects research, and additional studies within their authority, and determining the sensitivity of the Data developed, collected, received or otherwise used for that research. This includes:
   i. Undertaking the review and assessment of human subjects Data and other Data under their purview pursuant to applicable regulations and policies (e.g. identifiable individual level data, certain large-scale genomic data);
   ii. Establishing procedures to determine Data sensitivity, either on a project by project basis, or by category of Research Data (e.g. Worksheets, Standard Operating Procedures);
   iii. For Sensitive Data, ensuring that an Information Security Reviewer has initiated any required review relevant to the project;

iv. Highlighting the need for Researchers to review the DUA Policy and Guidance when exchanging Data and submit any DUA reviews in the Agreements Application, and link the relevant reference number in the Compliance System; and
v. Requesting relevant ancillary reviews pertaining to the Data (e.g. GDPR, Committee on Microbiological Safety (COMS), Provostial review), and confirming such ancillary reviews are properly recorded in the Compliance System.

b. Training and Education: Consistent with University policies, the IRBs are responsible for developing and disseminating human subjects research guidance as it relates to Research Data. This may include:
   i. Educating and training University personnel on human subjects research; and
   ii. Offering guidance regarding responsible practices for protecting the confidentiality of human subjects.
c. Ceded Review: The IRB is responsible for informing Researchers who are receiving Data pursuant to a study where Harvard's IRB has ceded review to another institution, that the Researcher must refer to the DUA Policy and Guidance to determine if a DUA is required, or speak to a representative from the relevant Negotiating Office, and create a record of the datasets in the Research Safety Application.
d. Institutional Oversight: Through the course of review and any subsequent actions, the IRBs are responsible for reporting concerns of noncompliance with administrative approvals and institutional policies to the appropriate research oversight bodies for further review.

4. Negotiating Offices

a. Sponsored and Data Use Agreements ("Research Agreements"): The Negotiating Offices are responsible for reviewing and approving the terms of Research Agreements, and working with other offices (e.g. Office of General Council (OGC), Office of Technology Development (OTD), Office of the Vice Provost for Research (OVPR), Harvard University Information Technology (HUIT)) to confirm that Research Agreements are compliant with applicable laws and regulations as well as Harvard's internal policies, as further described in the Negotiating and Signing Authority for Agreements Related to Research Policy and DUA Policy and Guidance. This includes:
   i. Requesting relevant ancillary reviews pertaining to the underlying Data (e.g. GDPR, COMS, provostial review), and recording such ancillary reviews in the Agreements Application;
   ii. Highlighting project-specific requirements of the DUA that necessitate Researcher action; and
   iii. Prior to executing a DUA, confirming that the Researcher has received any required approvals (e.g. IRB, Security Review, department administrator), and that the record of the approval is properly logged in the relevant Application(s).
b. Training and Education: Consistent with University policies, the Negotiating Offices are responsible for developing guidance on DUAs. This may include:
   i. Providing guidance and training for researchers and administrators on the processes and procedures pertaining to DUA review; and
   ii. Offering guidance on best practices for working with data providers.
c. Institutional Oversight: Through the course of review and any subsequent actions, the Negotiating Offices are responsible for reporting concerns of noncompliance with administrative

approvals and institutional policies to the appropriate research oversight bodies for further review.

5. Office of the Vice Provost for Research

a. Implementation: Procedures to implement this Guidance will be developed and maintained by OVPR, in consultation with the Office of the University Chief Information Security Officer and research oversight bodies, as appropriate. OVPR will work with other stakeholders to foster compliance, awareness and understanding of requirements and best practices associated with the Policy and Guidance; and

b. Revisions: OVPR is responsible for working with other research oversight bodies, as necessary, to identify data security risks, policy gaps, and additional resources that should be incorporated into the Policy and Guidance.

III. PROCESSES AND PROCEDURES

1. Researcher-Determined Security Level

Harvard allows for Researchers to identify the DSL for certain types of non-human subjects Research Data. Researchers' assessment must consider relevant University policies, and specifically the Enterprise Policy that classifies all Research Data as DSL 2 or above. Data that is not otherwise restricted pursuant to this Guidance, federal or state regulations, contractual requirements or intellectual property protections can be stored in compliance with the Enterprise Policy without necessitating review by the IRB or an Information Security Reviewer. All Research Data that is assessed at DSL 3 or above, regardless of medium or genre, must be recorded in the Research Safety Application and reviewed and approved by an Information Security Reviewer. Additionally, all Data that is received under a DUA must be recorded in the Agreements and Research Safety Application, even if the Researcher has determined the DSL to be 2. If Researchers are developing or receiving large datasets, it is recommended that they speak with their local IT representative to ensure proper handling and storage. Questions about selecting a DSL or implementing security controls can be directed to an Information Security Reviewer or submitted through the Research Safety Application.

2. Use of Data about Persons

One major category of Data involving information about individuals is "human subjects research", which is reviewed and approved by IRBs in the ESTR-IRB Application. In order for IRBs to approve a research project, they must conclude that adequate provisions have been made for protecting the privacy of subjects and the confidentiality of personal information. Accordingly, it is the responsibility of IRBs to specify the sensitivity of the Data for projects involving human subjects research, and to confirm that relevant confidentiality risks are addressed. The procedures for IRB review and approval are set out in Section 2(a) below.

a. Human Subjects Research

i. When applying for IRB approval for research potentially involving human subjects, Researchers must submit their review request in ESTR-IRB (See the ESTR Study Submission Guide for more details).

ii. The IRB will consult with the Researcher, obtain additional information as needed, and direct the Researcher to the Research Safety Application if the study is determined to

involve the use of Sensitive Data, and/or the Agreements Application if the Researcher is exchanging Data.

- DUAs may dictate additional security measures, which will be evaluated by an Information Security Reviewer (See Sec. III(3), DUAs for more details).

iii. For projects determined to include only non-Sensitive Data, the IRB will complete its review, including any ancillary reviews pertaining to the Data (e.g. provostial review, GDPR, COMS), and issue a determination or approval.

iv. For projects determined to include Sensitive Data, the IRB will only issue an approval or determination upon receipt of approval from required ancillary reviewers or confirmation that a record has been approved in the Research Safety Application.

v. Submitting Data Security Attestation

- For projects involving only non-Sensitive Data that is not otherwise restricted pursuant to this Guidance, Researchers can implement the security controls set out in the Enterprise Policy without contacting an Information Security Reviewer, though those offices are always available to provide assistance as needed.
- For projects involving Sensitive Data, Researchers must create a record of the project in the Research Safety Application and receive approval from an Information Security Reviewer prior to receiving or sharing Sensitive Data.

vi. Researchers must inform the reviewing IRB of any reportable occurrence, as defined in the Investigator Manual, pertaining to the Research Data within five (5) business days.

b. <u>Non-Human Subjects Research</u>

i. These procedures cover two types of studies: projects that have been determined to be "not human subjects research" or "not research" by an IRB, and projects that a Researcher has independently determined to be "not human subjects research" or "not research" as defined by federal regulation.

ii. If an IRB has concluded a project is not human subjects research:

- An IRB can make this determination in two ways – (i) the Researcher requests a not human subjects research determination by submitting the "Not Human Subjects Research Determination Request Form" in ESTR-IRB, or, (ii) after assessing the Protocol and materials submitted in ESTR-IRB, the IRB determines the project is not human subjects research.
- Based on the materials submitted by the Researcher, the IRB will provide a determination of Sensitive or non-Sensitive.
- For non-Sensitive Data, the IRB will direct the Researcher to the Enterprise Security Policy's applicable requirements and inform the Researcher of the availability of assistance from an Information Security Reviewer to implement those controls.
- For Sensitive Data, Data that requires approval from an ancillary reviewer (e.g. GDPR, intellectual property, or federal restrictions), or Data that is governed by a DUA or sponsored award, the IRB will inform the researcher of the requirement to submit a request for review in the appropriate application in the Compliance System and reference the submission number in ESTR-IRB.

iii. If the Researcher has deemed a project not human subjects research, refer to Section III(1), Researcher-Determined DSL.

3. DUAs

The administrative review procedures for the review and approval of DUAs is similar whether Harvard is requesting or providing the Data. For additional information pertaining to the processes and procedures surrounding the DUA (as well as related agreements, such as non-disclosure, confidentiality, software and collaboration agreements) review process, please read the DUA Policy and Guidance or reach out to the relevant Negotiating Office.

a. Submission: Researchers requesting Data from a data provider or sharing Data with an external organization are required to submit a request for DUA review by a Negotiating Office through the Agreements Application, in addition to any other related reviews required to be submitted in the Compliance System.
b. Review: Concurrent with a Negotiating Office's review and negotiation, an Information Security Reviewer will work with the Researcher to review the security requirements of the DUA to determine whether any specific protections need to be employed. Similarly, if the project involves human subjects research, an IRB will work with the Researcher to ensure appropriate provisions are in place to protect confidentiality and privacy. Each review should be initiated in the relevant Application in the Compliance System and referenced in the corresponding submission.
c. Approvals: Required approvals (including ancillary reviews, e.g. GDPR, OGC, OTD, local data storage personnel or department representative) will be recorded in the Compliance System. Human subjects review and approval will be recorded in ESTR-IRB by the reviewing IRB. Security Review of the dataset and DUA terms will be recorded in the Research Safety Application. The relevant Negotiating Office and Researcher will sign-off on the project via the Agreements Application.

4. Data Deposition or Submission Agreements

Researchers may be required by data banks or repositories (any third party that accepts data depositions) to sign a contract agreeing to certain terms and conditions pertaining to the type of data, mode of transfer or security controls, among other requirements or certifications. All such contracts and related documents should be submitted to the Research Safety Application for review.

5. Laboratory Animal Care and Use (Animals covered by Intuitional Animal Care and Use Committee (IACUC) Policy)

a. The Guide for the Care and Use of Laboratory Animals identifies two areas of risk management that include data security protection, and are applicable to Researchers:
    i. Medical Evaluation and Preventive Medicine for Personnel, implicating personal health information; and
    ii. Personnel Security calling for "physical and information technology security" to protect against "threats that criminal activities such as personnel harassment and assault, facility trespassing, arson and vandalism pose to laboratory animals, research personnel, equipment and facilities."
b. Researchers whose projects include laboratory animal studies are required to:
    i. Consult with their IACUC committee to assist them in identifying categories of laboratory information that require secure storage and use, and the appropriate security levels for that information; and

ii. Should the Research Data be assessed at Level 3 or higher, the Researcher will submit a request for a security review by an Information Security Reviewer in the Research Safety Application.

6. Data Subject to Export Controls

In general, it is safe to assume that, if an item or technology is subject to export controls, the Data related to the item or technology is also subject to export controls. Researchers who think their projects may be subject to export control regulation are required to:

a. Consult with their School's representative on the Export Control Council to identify any data security obligations that are associated with export control requirements;
b. Consult the Export Control Guidance for Outsourcing Information Technology Services when seeking to outsource information technology services; and
c. Consult with an Information Security Reviewer to determine what security measures need to be implemented and documented in the Research Safety Application.

7. Biosafety: Select Agents and Toxins

Data security measures are necessary to protect against the release of Data that would allow an unauthorized individual to gain access to select agents or toxins. The COMS reviews research that presents biohazard risks, including research that involves biological toxins subject to the Federal Select Agent Program. Researchers who work with infectious agents or other biohazardous material should:

a. Ensure that their work is compliant with specific federal and state security requirements;
b. Consult with COMS to assist them in identifying categories of laboratory information that require secure storage and use, and the appropriate security levels for that information; and
c. Consult with an Information Security Reviewer to determine what security measures need to be implemented and documented in the Research Safety Application.

8. Radiation Safety: Radioactive Materials

Data security measures are necessary to protect against the release of Data that would allow an unauthorized individual to gain access to radioactive materials. The Radiation and Safety Committee reviews research that presents radiation risks, including research that involves materials subject to federal and state radiation control programs. Researchers who work with radioactive material should:

a. Ensure that their work is compliant with specific federal and state security requirements;
b. Consult with the Radiation and Safety Committee to assist them in identifying categories of information that require secure storage and use, and the appropriate security levels for that information; and
c. Consult with an Information Security Reviewer to determine what security measures need to be implemented and documented in the Research Safety Application.

9. Genomic Data

Researchers intending to submit large-scale human genomic data to a National Institutes of Health (NIH)-designated data repository must first secure an Institutional Certification that the submission of data to the repository is appropriate and consistent with the NIH Genomic Data Sharing Policy. For additional information regarding the NIH Policy and Harvard's process for review and certification of

such submissions, please review the University's Policy and Procedures for Human Genomic Data Sharing or contact your relevant IRB.

Researchers requesting genomic data from a third party, including the NIH, should submit a review request in the Agreements Application.

10. Sponsored Research

As addressed elsewhere in this Guidance, certain Research Data collected, developed or exchanged pursuant to a sponsored project for which Harvard is the prime recipient must be reviewed by an Information Security Reviewer in the Research Safety Application

If specific data security controls or regulations are required by a sponsor, such as National Institute of Standards and Technology (NIST), FISMA, GDPR or FERPA, the Researcher must submit the project's Data Security Plan (including the sponsor's security requirements) for approval by an Information Security Reviewer, at latest, prior to execution of the sponsored agreement. The Researcher will provide documentation of such approval (via link or Letter of Approval) to the Negotiating Office.

For projects involving Sensitive human subjects research, Data subject to foreign, federal, state regulations or intellectual property protections, or Data otherwise required by University policy to receive approval from an Information Security Reviewer, Security Review should occur prior to Data collection, development or exchange. If such projects involve exchanging Data with subrecipients, Researchers must obtain approval of their Data Security Plan prior to execution of the subaward and provide documentation of such approval (via link or Letter of Approval) to the Negotiating Office.

Data Security Plans associated with sponsored projects should comprehensively address the exchange and use of Data for each collaborator (e.g. subrecipient, vendor, consultant, unpaid research partner) under the award. Additionally, the Researcher will ensure that the controlling Research Safety Application submission includes a reference or link to the relevant Grants Management Application Suite (GMAS) project.

As part of their Security Review, if the Information Security Reviewer cannot determine whether a collaborator is capable of managing the Data based on the Data Security Plan as proposed, the Reviewer may instead complete an institutional assessment of the collaborator in order to better consider the feasibility of the activities described in the Plan. Should the Information Security Reviewer determine the collaborator cannot appropriately secure the Data, the Reviewer will notify the Chief Compliance Officer and Chief Information Officer per the escalation process defined herein.

11. Inventions and Proprietary Data

Research may lead to the creation of inventions for which patent applications should be prepared to protect the relevant rights and interests. Researchers who are working with proprietary Data should submit a request in the Research Safety Application to ensure appropriate security controls are in place to protect the Data. Researchers who have particular concerns about protecting or managing new technology or innovation should contact the Office of Technology Development (OTD).

12. Education and Training

a. Administrators: The University and its administrators are charged with providing helpful and effective resources to Researchers. Inherent to this charge is the development of training and outreach materials that promote compliance with institutional policies and processes. Specific to

the Research Data Security Policy, Information Security Reviewers and the IRBs have the responsibility of informing Researchers of applicable requirements and best practices aligned with Data privacy, confidentiality and security pursuant to the scope of their authority.

b. Researchers: Researchers at Harvard who work with Research Data are required to complete annual Research Data Security Training, and maintain an active certificate of approval to continue utilizing Harvard's resources.

13. Setting and Implementing a Security Certification for University Resources

Researchers may only utilize DSL-appropriate tools, storage and facilities to manage Research Data. In order to have a tool, storage option, facility or other resource (including certain vendors) approved by an Information Security Reviewer for use for Research Data, the Researcher or facility manager must submit a request in the Research Safety Application (independent of any specific research data use), or otherwise engage the Information Security Reviewer with purview of the resource to receive official approval, as is required by the Enterprise Policy.

14. Non-Compliance

IRBs, Information Security Reviewers, Negotiating Offices and other research administrators involved with the management of Research Data are responsible for reporting instances of noncompliance with the Research Data Security Policy and this Guidance, as well as the policies referenced herein to the appropriate research oversight bodies for further review. Instances of identified noncompliance with the Research Data Security Policy and this Guidance should be reported to the Chief Compliance Officer and Chief Information Officer, and may impact a Researcher's access to his or her Data and University resources, in addition to other mitigating and corrective measures imposed by the Chief Compliance Officer and Chief Information Officer, or as may be required by a data provider or sponsor.

15. Escalation

Should there be confusion pertaining to the interpretation of this Guidance or a request for an exception to one of the requirements, the administrator reviewing the relevant project will discuss their concerns with the Researcher, and thereafter communicate the issue to the Chief Compliance Officer and Chief Information Officer for review and determination.

DEFINITIONS

Agreements Application: Application for submitting DUA requests for review by a Negotiating Office.

Compliance System: The Compliance System is made up of various applications (e.g. ESTR, Agreements, Research Safety) that support institutional compliance with internal policies as well as external laws and regulations. Both researchers and administrators have access to the Compliance System, as it is intended to provide transparency and consistency to Harvard's research processes and procedures.

Confidentiality: The treatment and management of information and materials that an individual or organization has disclosed in a relationship of trust and with the expectation that it will not be disseminated to others in ways that are inconsistent with the understanding of the original disclosure.

Data Security Plan: Researcher's approved submission to the Research Safety Application.

Data Use Agreement (DUA): A binding contract governing access to and treatment of nonpublic data provided by one party (a "Provider") to another party (a "Recipient"). DUAs are often required by external parties before they permit data to be received by Harvard and may also be necessary for Harvard data to be disclosed to another organization. DUA terms and conditions vary depending on the laws and regulations governing the specific type of data to be shared, as well as the policies and/or requirements of the Provider and Recipient.

Enterprise Information Security Policy (Enterprise Policy): University-wide policy applicable to confidential and sensitive information that is maintained in the various spheres of University administration.

Electronic Submission, Tracking & Reporting (ESTR-IRB): Application for submitting requests for IRB review.

Human Subjects Research: As defined in relevant federal regulations.

Information Security Reviewer: An employee of HUIT or an individual school who is responsible for assessing the appropriateness of collaboration tools and security measures, and working with Researchers to implement the relevant Data Security Level. Roles that may fall within this designation, or who may have assigned someone as a designee for these responsibilities, are:

- Chief Information Officer
- Information Security Officer
- IT Compliance Officer

Institutional Review Board (IRB): An Institutional Review Board provides ethical and regulatory oversight of research that involves human subjects.

Negotiating Office: For Cambridge and the Business School, the office authorized to review and execute DUAs and sponsored awards is the Office for Sponsored Programs (OSP). For the Medical and Dental School, the office authorized to review and execute DUAs and sponsored awards is the HMS Office of Research Administration (ORA). For the Harvard T.H. Chan School of Public Health, the office authorized to review and execute DUAs and sponsored awards is the Office of Research Administration (ORA, formerly "SPA").

Privacy: Control over the extent, timing, and circumstances of sharing information and materials about oneself with others.

Research Data and Materials ("Research Data" or "Data") include recorded, tangible, or intangible research information, regardless of form or the media on which it may be recorded, that is created or collected in the process of performing research, whether supported by University resources or by external funders. Research Data and Materials include, but are not limited to, computer software (computer programs, computer databases, and documentation thereof), materials such as unmodified and modified biological Page 2 of 3 specimens, new or modified chemical entities, laboratory notebooks, notes of any type, materials submitted to and/or approved by IRB, IACUC, or other research oversight committees (e.g., applications, outreach/advertising materials, consent forms, survey routines/questionnaires and debriefing scripts), photographs, films, audio recordings, digital images, original or modified biological and environmental samples, gels, spectra, cell lines, reagents, protocols, algorithms, graphs, charts, numerical raw experimental results, instrumental outputs, other deliverables under sponsored agreements; intangible data such as statistics, findings, conclusions, other deliverables under sponsored agreement; and any other records of, or in any form that could be used for, reconstruction and evaluation of reported or otherwise published results of research. Pursuant to the Research Data Ownership Policy, the University asserts ownership over Research Data generated at Harvard for projects conducted at the University, under the auspices of the University, or with University resources.

Research Data Security Training: The following courses have been approved to satisfy the Research Data Security Training requirement:

- CITI: Information Privacy and Security for Researchers
- Research Data Security Training Course

Researcher: Any investigator (e.g. Faculty, student, post doc, etc.) who seeks to exchange Data with a third party, or conducts research where data are generated or used.

Research Safety Application: Application for submission of Data Security Plans and other requests that require Security Review by an Information Security Reviewer.

Security Control: A safeguard measure to reduce a risk of data breach. There are sets of security controls that are required for each Security Level of the Data Classification Table.

Security Level: The assigned information risk designation for a research project, on the HUIT Data Classification Table. For Sensitive Data (as determined by the IRB), the Information Security Reviewer assigns the security level. Security levels should be designated for confidential Research Data that does not involve human subjects by the researcher in consultation with an Information Security Reviewer, as appropriate, as set forth in this Guidance.

Sensitive and Non-Sensitive Data: Sensitive Data is data historically assessed at Level 3, 4 or 5, including data subject to foreign, federal or state regulations. Non-Sensitive Data is data historically assessed at Level 1 or 2, such as public information.

RELATED POLICIES

- Data Use Agreement
- Enterprise Information Security
- Genomic Data
- Intellectual Property
- Legal Agreements Workflow and Signature Authority
- Open Access
- Publications
- Research Data Ownership
- Retention of Research Data and Materials

RELATED REGULATIONS

- Family Educational Rights and Privacy Act (FERPA)
- Federal Information Security Management Act (FISMA)
- Export Administration Regulations (EAR)
- General Data Protection Regulation (GDPR)
- Gramm-Leach-Bliley Act (GLB Act or GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- National Institute of Standards and Technology (NIST)