University of Kentucky
Data Security Compliance Program

Table of Contents
Data Security Compliance Program

University of Kentucky
Data Security Compliance Program

For U.S. Department of Justice's Data Security Compliance Program

1. **Statement of Purpose**: The purpose of this University of Kentucky Data Security Compliance Program ("DSCP") is to assist the University of Kentucky and its affiliated corporations ("University") in its efforts to comply with its data security obligations under 28 CFR 202. Specifically, this DSCP is intended to adhere to the expectations of those federal regulations, and in the event of a possible failure, to detect and remediate breaches of the University's procedures and violations of the Data Security Program established by the United States Department of Justice ("DOJ") under 28 CFR 202 (also known as "DOJDSP").

2. **General Provisions**

    a. **Capitalized Terms**: All capitalized terms used in this DSCP and its attachments shall have the meanings set forth in 28 CFR Part 202, Subpart B unless specified otherwise. If a definition below does not appear in 28 CFR Part 202, Subpart B, then the definition given below applies. Note: The definitions in 28 CFR Part 202 Subpart B must be consulted; the definitions below are generalizations or summaries of the detailed definitions in the regulations.

        i. **Bulk U.S. Sensitive Personal Data**: A collection or set of Sensitive Personal Data relating to U.S. persons or U.S. devices, regardless of whether anonymized, pseudonymized, de-identified, or encrypted, where such data

meets or exceeds specific bulk thresholds (i.e., 100+ human genomic data on U.S. persons, 1,000 epigenomic, proteomic or transcriptomic human data on U.S. persons; 1,000+ biometric identifiers on U.S. persons; 1,000+ precise geolocation data on U.S. devices; 10,000+ personal health data on U.S. persons; 10,000+ personal financial data on U.S. persons; and 100,000+ covered personal identifiers on U.S. persons).

ii. **CISA Security Requirements**: those security requirements set forth in the Cybersecurity and Infrastructure Agency ("CISA") Security Requirements for Restricted Transactions E.O. 14117 Implementation, January 2025, as incorporated in 28 CFR 202.248.

iii. **Country of Concern**: One or more of those countries identified by the United States Department of Justice ("DOJ") as a "Country of Concern," which currently includes: China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela.

iv. **Covered Data Transaction or Covered Transaction**: Shall refer to "Prohibited Transactions" involving data brokerage and "Restricted Transactions" involving certain vendor, employment, or investment agreements, as described in the University's DSCP.

v. **Covered Person**: Any person controlled by or subject to the jurisdiction or direction of a Country of Concern or primarily residing in a Country of Concern, including foreign entities headquartered in, organized under the laws of, or significantly owned by a Country of Concern or other Covered Persons and their employees.

vi. **Critical Vendor:** A Vendor whose goods or services, if disrupted, compromised, or failed, would have a significant material impact on the University's operations, reputation, financial stability, legal obligations, or compliance posture. DSPs handling sensitive data are, for purposes of this Policy and the University's DSCP, almost always considered Critical Vendors.

vii. **Data Brokerage**: The sale or licensing of access to data, or similar commercial transactions, involving the transfer of data where the recipient did not collect or process the data directly from the U.S. person.

viii. **Due Diligence**: The methodical process of conducting thorough research and investigation on a prospective or existing vendor to assess their capabilities, financial stability, reputation, security posture, compliance, and potential risks before entering into or renewing a contractual agreement.

ix. **Data Service Provider** ("DSP"): A Vendor that processes, stores, transmits, or otherwise accesses the University's data, including cloud service providers, managed information technology ("IT") service providers, data analytics firms, payroll processors, and any other Vendor handling data on behalf of the University.

x. **Government-Related Data**: Precise geolocation data for any location within specific government-related areas, or certain categories of data related to U.S. government personnel or operations, including precise geolocation data collected from within areas identified on the Government-Related Location Data List ("GRLD List") as set forth in 28 C.F.R. § 202.1401.

xi. **Prohibited Transaction**: A "Covered Data Transaction" involving data brokerage with a Country of Concern or Covered Person, which is generally prohibited unless an exemption or specific license applies. This generally

includes transactions involving the sale or licensing of access to Covered Data to a Country of Concern or Covered Person, especially bulk human 'omic data or human biospecimens.

xii. **Restricted Transaction:** A "Covered Data Transaction" involving a Vendor agreement, employment agreement, or investment agreement with a Country of Concern or Covered Person, which is permissible only if specific security, due diligence, audit, and recordkeeping requirements (as outlined by CISA, the DOJDSP, and the University's DSCP) are met.

xiii. **Sensitive Personal Data**: Includes covered personal identifiers, precise geolocation data, biometric identifiers, human `omic data, personal health data, personal financial data, or any combination thereof. This term excludes public or nonpublic data that does not relate to an individual; data that is, at the time of the transaction, lawfully available from a federal, state or local government record or in widely distributed media; personal communications; and information or informational materials and ordinarily associated metadata or metadata reasonably necessary to enable the transmission or dissemination of such information and informational materials. See 28 CFR § 202.249.

xiv. **U.S. Person**: Any United States citizen, national, or lawful permanent resident; any individual admitted to the United States as a refugee under 8 U.S.C. 1157 or granted asylum under 8 U.S.C. 1158; any entity organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any person in the United States. A human being who is a U.S. Person would not be a Covered Person unless they are residing in a Country of Concern.

xv. **Vendor:** Any external person or entity (individual, company, organization, or governmental entity) providing goods or services to the University.

xvi. **Vendor Management**: The comprehensive process of selecting, onboarding, monitoring, evaluating, and offboarding Vendors to ensure optimal performance, value delivery, and risk mitigation throughout the entire Vendor lifecycle in accordance with this Policy.

xvii. **Vendor Risk Assessment:** The systematic process of identifying, analyzing, evaluating, and prioritizing the potential risks associated with engaging a particular Vendor, with specific focus on data security and regulatory compliance for DSPs.

b. Implementation

i. **Responsible Operating Unit**: Although this DSCP applies to the entire University and its operations, the Office of Corporate Compliance shall be administratively responsible for the implementation of the DSCP.

ii. **Responsible Person**: The Data Security Compliance Officer ("DSCO") shall be responsible for the day-to-day implementation of the DSCP and shall report to the individual serving as both the Executive Vice President for Finance and Administration and Co-Executive Vice President for Health Affairs ("EVPFA/Co-EVPHA"). The DSCO's duties shall include:

1. Coordination of other sub-policies and education and training programs necessary to achieve compliant conduct.
2. Reporting regularly to the President and the EVPFA/Co-EVPHA and at their direction and assistance to the University trustee(s) as to the

current state of (A) the University's compliance efforts and (B) the implementation of the DSCP.

3. Other duties as set forth below.

iii. **Standards and Procedures to Prevent and Detect Conduct Not in Compliance with 28 CFR 202:** To prevent and detect non-compliant conduct, the DSCO shall identify each requirement set forth in 28 CFR 202 and develop, monitor and maintain a list detailing the following:

1. The person primarily responsible for assuring compliance with each regulatory obligation.
2. The specific compliance obligations imposed on the University as a result of each regulation.
3. When applicable, the dates on which those compliance obligations must be implemented.
4. A list of human, financial, or other resources necessary to achieve compliance.
5. A list of any current impediments to achieving full compliance which need to be addressed by the institution.
6. Recommendations for alleviating any such impediments.

c. University Oversight

i. **Board Oversight**: The President, EVPFA/Co-EVPHA, or DSCO shall routinely report to applicable members of the University's Board of Trustees as to the status of ongoing compliance efforts, the resources necessary to achieve compliance, and any current impediments to achieving full compliance and recommendations for alleviating those impediments.

ii. **Senior-Level Administrative Oversight**: The President and the EVPFA/Co-EVPHA shall have primary administrative oversight of the DSCP. It shall be the responsibility of the President and the EVPFA/Co-EVPHA to ensure the effectiveness of the DSCP.

d. Exclusion of Individuals with a History of Non-Compliant Conduct: The President, EVPFA/Co-EVPHA and Vice President for Human Resources shall ensure that individuals with a history of non-compliant behavior in a particular area of the DSCP not be hired to perform any duties in that area; individuals with a history of non-compliant behavior in two or more areas of the DSCP will not be hired by the University in any capacity.

e. Monitoring, Evaluating, and Reporting Mechanisms: The University shall maintain its Comply-Line, which allows for confidential reporting mechanisms which are detailed at https://ukhealthcare.uky.edu/staff/corporate-compliance and it may offer other reporting mechanisms. When the University receives inquiries concerning methods for compliance with 28 CFR 202 or reports of non-compliant behavior, the DSCO shall coordinate the response to such inquiries to provide instruction and the investigation of such reports to ascertain whether non-compliant has occurred and to determine what remedial steps may be appropriate to address such conduct. Each year, the DSCO shall take reasonable steps to evaluate the effectiveness of the DSCP on a regular basis, whether members of the University community are following the DSCP, whether the DSCP is effectively monitoring and auditing to detect non-compliant

behavior, and whether the DSCP is, overall, effectively achieving the University's stated policies of compliant conduct.

f. **Incentives and Disciplinary Measures**: The President, Provost, Executive Vice Presidents for Finance and Administration and for Health Affairs, Vice President for Student Success, and the Vice President for Research shall take such steps as are appropriate to include compliance with University policies and standards as a part of the annual employee review and compensation process. In addition, a failure to adhere to the DSCP and its related policies shall be subject to the University's regulations and policies on faculty, staff and student conduct, due process, and discipline, and removal.

g. **Responding to and Prevention of Future Non-Compliant Conduct**: The President, Provost, Executive Vice Presidents for Finance and Administration and for Health Affairs, Vice President for Student Success, and the Vice President for Research shall cause the University to promptly respond to non-compliance by taking appropriate steps to eliminate the non-compliance and to prevent its recurrence in the future.

3. **Due Diligence for Restricted Transactions per 28 CFR 202.1001**

a. **Risk-Based Procedures Verifying Data Flows Involved in Any Restricted Transaction:** The University shall utilize various procedures to assess and mitigate its risks in any Restricted Transaction as described in 28 CFR 202, Subpart D.

i. **Annual Risk Assessment:** At the direction of the DSCO, on an annual basis, the University shall undertake on a routine (at least annual) and ongoing basis a robust risk assessment of the compliance risks which it is likely to encounter. The risk assessment shall identify the potential areas of risk for the University, including how and when the University may engage in data transactions with Covered Persons or Countries of Concern. The risk assessment shall also examine the University's (a) current security measures, (b) Vendors, employees, and any other stakeholders, (c) offered activities, products and services, (d) coverage under existing general or specific licenses or exemptions, (e) any geographic considerations associated with any stakeholder, and (f) the location of and the individuals in control of Sensitive Personal Data and Government-Related Data in possession of the University. Following each risk assessment or audit, and any detected violations, the University shall re-evaluate this DSCP and make appropriate changes as needed to ensure ongoing compliance with 28 CFR 202.

ii. **Transaction Specific Procedures:** For each contemplated Restricted Transaction, the University employee or student wishing to undertake a Restricted Transaction shall provide the DSCO with the following information:

1. Types and volumes of Government-Related Data and Sensitive Personal Data which will be a part of the proposed Restricted Transaction;
2. Identity of proposed Restricted Transaction parties; and
3. End-use of data and method of data transfer.

Upon receipt of the foregoing information pertaining to the Restricted Transaction, the DSCO shall evaluate the proposed Restricted Transaction to determine if the proposed Restricted Transaction is fully compliant with 28 CFR 202. The proposed Restricted Transaction may not proceed until such time as the DSCO advises the employee in writing that the proposed Restricted Transaction complies with 28 CFR 202.

b. Vendor Management and Validation: For Restricted Transactions involving Vendors, the Vendor Due Diligence Policy attached as Attachment 1 identifies the risk-based procedures for, among other things, verifying the identity of Vendors. The University adopts and incorporates by reference that policy into the DSCP.

c. Written Data Security Compliance Program Policy: This document constitutes the University's written data security compliance policy as required by 28 CFR 202.1001.

d. Written Policy Describing the Implementation of Security Requirements: The University adopts and incorporates by reference the Security Requirements which are set forth in Attachment 2. The DSCO and the EVPFA/Co-EVPHA shall be primarily responsible for implementing the Security Requirements. The DSCO and the EVPFA/Co-EVPHA shall collaborate with the University Research enterprise, UK HealthCare, University Information Technology Services, and others across the University to ensure that the University remains compliant with all Security Requirements.

e. Written Policy Describing the Compliance in Research Activities: The University's policy on compliance with the DOJDSP and this DSCP in research activities is attached as Attachment 3 and adopted and incorporated by reference into the DSCP.

f. Regarding activities which implicate review/vetting under the DOJDSP or this DSCP but which are **not** activities covered by the procedures in Attachments 1 (concerning vendor relationships) and 3 (concerning research relationships) of this DSCP, the DSCO will apply the following expectations for review of those activities:

i. Phase 1 - Prior to initiating activities involving a data transaction covered by or to which the DOJDSP and the University's DSCP applies:

1. Data Assessment and Classification: When a proposed Covered Data Transaction is proposed:
    a. The DSCO or their designee must conduct a thorough review of all data types and volumes involved in the proposed activity to determine if they constitute Covered Data under the DOJDSP and the University's DSCP. This includes assessing if any data will meet "bulk" thresholds.
    b. Special attention must be paid to the potential collection or use of precise geolocation data from within areas on the Government-Related Location Data List ("GRLD List") as set forth in 28 C.F.R. § 202.1401.
    c. The classification process must proceed even if the data is anonymized, pseudonymized, de-identified, or encrypted, as

these measures do not exempt data from DOJDSP regulations and the University's DSCP applications if it meets "bulk" thresholds or constitutes government-related data.

2. Partner and Covered Person Screening:
    a. When presented with activities potentially subject to the DOJDSP or the University DSCP, the DSCO or designee must conduct due diligence to screen all potential collaborators and other parties, including individuals and entities, against the list(s) of Countries of Concern and Covered Persons. This includes using vendor-screening software that incorporates updates to any published Covered Persons List and accounts for alternative spellings or also-known-as designations.
    b. If a potential collaborator or other party is identified as a Covered Person or is associated with a Country of Concern, the activities must undergo heightened scrutiny.

3. Prohibited Transaction Review: Any proposed activity that involves a Prohibited Transaction (e.g., but without limitation, Data Brokerage of Covered Data to a Country of Concern or Covered Person, or any access to bulk human 'omic data by a Country of Concern or Covered Person) is strictly forbidden unless an explicit license from the DOJ National Security Division (NSD) is obtained. Requests for such licenses will be reviewed by the NSD under a "presumption of denial." Any license application contemplated by a Researcher must first be approved for submission by both DSCO and the Office of Legal Counsel ("General Counsel").

4. Restricted Transaction Compliance Plan:
    a. If a proposed activity involves a Restricted Transaction (e.g., employment or investment agreements providing access to a Country of Concern or Covered Person), a detailed compliance plan must be developed and approved by the DSCO in advance of the Restricted Transaction proceeding.
    b. This plan must demonstrate how the activity will adhere to the CISA Security Requirements and the University's DSCP, including:

        i. Organizational and System-Level Requirements:
            1. Identifying, prioritizing, and documenting all assets of a covered system.
            2. Designating an individual accountable for cybersecurity and compliance.
            3. Documenting all vendor and supplier agreements.
            4. Developing and implementing incident response plans.

5. Implementing access controls to prevent unauthorized access by Covered Persons or Countries of Concern.
6. Conducting internal risk assessments to guide data-level requirements.
7. Remediating all known exploited vulnerabilities within forty-five (45) calendar days, starting with critical assets.

ii. Data-Level Requirements: Implementing a combination of mitigations, such as:
1. Data minimization and data masking strategies.
2. Comprehensive encryption techniques.
3. Privacy-enhancing technologies.
4. Identity and access management techniques to deny unauthorized access to Covered Data.

5. Contractual Agreements:
   a. All activity agreements (and/or the University's standard terms and conditions applicable to vendors) in which Covered Data will or could be shared to a Covered Person or Country of Concern must include specific clauses as directed by General Counsel, including without limitation representations of applicable parties and prohibiting any transactions that violate the DOJDSP.
   b. For Restricted Transactions, research agreements must stipulate compliance with CISA's Security Requirements and incorporate provisions for onward-transfer clauses for any data shared with foreign persons who are not Covered Persons, along with reporting of known or suspected violations of those clauses.
   c. These agreements must clearly define data ownership, access rights, data handling protocols, and termination clauses in the event of DOJDSP non-compliance.

ii. Phase 2 - During Activities:

1. Continuous Monitoring and Due Diligence:
   a. University individuals and units with the relationships with the outside parties or collaborators ("Internal Requestors") are responsible for continuous monitoring of data flows and collaborator and other party activities to ensure ongoing DOJDSP and University DSCP compliance.
   b. Any changes in collaborator or other party status (e.g., a collaborator or other party becoming a Covered Person or associated with a Country of Concern) must be immediately reported to the DSCO.

c. Periodic screening of collaborators and other parties by Internal Requestors in consultation with the DSCO should be conducted to verify their status in accordance with the DOJDSP, the University's DSCP, and, where applicable, the University's Vendor Management and Due Diligence and Research Policies concerning DOJDSP compliance (Attachments 1 and 3 to this DSCP).

2. Data Security Measures:
    a. Strict adherence to the CISA Security Requirements is mandatory for all Restricted Transactions. This includes maintaining robust cybersecurity infrastructure, access controls, encryption, and data minimization practices.
    b. All data collected, processed, or stored as part of an activity involving Covered Data must be protected against unauthorized access, disclosure, alteration, and destruction.

3. Recordkeeping:
    a. Internal Requestors, the DSCO, and other University employees and students must maintain detailed and auditable records of all Covered Data Transactions, including:
        i. Types and volumes of data involved.
        ii. Identity of all parties to the transaction.
        iii. Security measures implemented.
        iv. Due diligence performed.
        v. Any rejected transactions.
    b. Records must be maintained for a minimum of ten (10) years.

4. Reporting Obligations:
    a. Rejected Transactions: Any person who receives and rejects a Prohibited Transaction involving Data Brokerage must report it the DSCO within three (3) days of the rejection, even if automatically rejected by software or other means, and the University, via the DSCO, must report it to the DOJ National Security Division within fourteen (14) days of the rejection, even if automatically rejected by software or otherwise.
    b. Annual Reports (if applicable): With the assistance of applicable Internal Requestors and other University employees and students, for Restricted Transactions associated with non-research activities involving cloud-computing services where twenty-five percent (25%) or more of the U.S. person's equity interests are owned by a Country of Concern or Covered Person, the DSCO will submit annual reports to the DOJ.
    c. On-Demand Reporting: All University employees and students will be prepared, and where directed, to do so via the DSCO, to furnish reports and information to the DOJ under oath at any time, before, during, or after a transaction.

d. Known or Suspected Violations: Any known or suspected violations of the DOJDSP or contractual clauses related to disallowed onward transfers must be immediately reported to the DSCO for onward reporting to the DOJ.

4. **Other Data Security Compliance Program Requirements Required by the United States' Attorney General:** The University will modify its DSCP if the U.S. Attorney General requires that additional information be included in the DSCP.

5. **Educating and Training Employees and Students:** The University shall conduct and make education and training available for all employees and students to make them generally aware of the DSCP and the underlying reasons for the Data Security Program. The University will conduct more detailed training for employees who are involved with Covered Data Transactions ("CDT Employees") according to the roles of the employees being trained. The training program for CDT Employees shall consist of training on the following:

   a. DSCP;
   b. Security Requirements;
   c. The reasons why the DSCP is necessary to protect national security; and
   d. The responsibilities of each employee and the consequences of noncompliance.

   The education and training program shall provide employees and students with the information they need to effectively participate in the University's compliance efforts. Using appropriate assessment tools, coupled with this Policy, the education and training program will hold individuals accountable for their compliance. The education and training program will be tailored for the risks of noncompliance which affect the individuals being trained. Examples from 28 CFR 202 and other sources will be used as a part of the training where relevant. The education and training materials will be maintained as easily accessible internal resources for employees and students. If the same types of violations recur after initial education and training has been provided or if deficiencies are identified in the periodic assessments or audits, the University will reassess its education and training program to determine if additional education or training is warranted or if the existing program should be modified to address and to prevent similar violations or eliminate deficiencies in the future.

6. **Annual Data Compliance Program and Auditing for Restricted Transactions:**

   a. **Written Data Compliance Program**: The University acknowledges that the DOJDSP requires that by October 6, 2025, for Restricted Transactions, a written, individualized, risk-based data compliance program must be established and annually certified by a designated officer, executive, or employee responsible for compliance. This program must:
      i. Reflect the organization's day-to-day operations.
      ii. Be easy to comply with and make verification of compliance straightforward.
      iii. Be designed to prevent employees from engaging in misconduct.
      iv. Include internal reporting procedures and a formal escalation process.
      v. Establish and implement risk-based procedures for verifying data flows.

   This Policy and its attached related policies are intended to address these requirements.

b. Annual Audits: Pursuant to the terms of this DSCP and in conformity with the DOJDSP, at the direction and oversight of the DSCO, who shall oversee and receive input from others within the University community, the University will conduct regular audits of the DSCP, records required to be maintained under 28 CFR 202.1101, Security Requirements, and its Restricted Transactions once for each calendar year that a Restricted Transaction is made, which audit must cover the preceding twelve (12) months. Audit results and related records must be retained for at least ten (10) years. The DSCO and all other applicable University employees and students will assist in fulfilling these requirements.

7. **Supplemental Policies:** The University may adopt policies to supplement the DSCP, to provide members of the University community with rules which will apply to specific situations, to provide internal controls to enhance the likelihood of compliance and that will identify, escalate, and report activity in violation of the DSCP, to minimize risk identified in the University's risk assessment, to assure that high-risk transactions are appropriately reviewed by compliance personnel, and to determine whether a specific license under 28 CFR 202.802 or an advisory opinion under 28 CFR 202.901 should be obtained.

8. **Annual Certification:** Each year, as coordinated by the DCSO, a University officer, executive, or other compliance officer shall certify to the U.S. Attorney General or other DOJ official that the DSCP is operative and is in compliance with applicable requirements under 28 CFR 202.1001(b).

9. **Non-Compliance and Penalties**

a. Failure to comply with this Policy, including its attached policies and standards, and the DOJDSP can result in severe consequences, including:

i. Disciplinary Actions: Subject to such other processes and expectations as may apply to the applicable individual or entity, up to and including termination of employment, enrollment, or affiliation with the University.

ii. Civil Penalties: Up to $368,136 or twice the amount of the transaction, whichever is greater, per violation.

iii. Criminal Penalties: Willful violations may result in fines up to $1,000,000 and up to twenty (20) years imprisonment.

b. Any known or suspected violations of this Policy, included its incorporated policies and standards, or the DOJDSP must be immediately reported to DSCO.

Attachment 1

University of Kentucky
Vendor Management and Due Diligence Policy
For U.S. Department of Justice's Data Security Program

1. Statement of Purpose: The purpose of this Vendor Management and Due Diligence Policy ("Policy") is to establish a comprehensive framework for the effective management of all third-party Vendor relationships and the rigorous conduct of due diligence on these Vendors who provide goods or services to the University of Kentucky and its affiliated corporations ("University") in conformity with compliance with the United States Department of Justice's Data Security Program ("DOJDSP") as well as the University's Data Security Compliance Program Policy ("DSCP").

a. This Policy aims to:
   i. Mitigate and manage risks across the entire Vendor lifecycle, encompassing operational, financial, legal, regulatory, reputational, and cybersecurity risks.
   ii. Ensure compliance with all applicable laws, regulations, and evolving standards associated with the DOJDSP.
   iii. Protect the confidentiality, integrity, and availability of the University of Kentucky's data and assets, particularly Bulk U.S. Sensitive Personal Data or Government-Related Data as defined by the DOJDSP and in Section 2, below.
   iv. Promote transparency, accountability, and consistency in Vendor selection, engagement, monitoring, and termination processes.
   v. Establish clear responsibilities and lines of authority for all aspects of Vendor management and due diligence obligations related thereto.

2. Definitions: All capitalized terms used in this Policy shall have the meanings set forth in the DSCP.

3. <u>General Provisions</u>

a. **<u>Policy Application</u>**: This Policy applies to all departments, employees, contractors, and agents of the University involved in any aspect of third-party Vendor relationships, from initial need identification and engagement through contract termination. This includes, but is not limited to:
   i. All new Vendor engagements.
   ii. Renewal or extension of existing Vendor contracts.
   iii. Significant changes to existing Vendor relationships (*e.g.*, increased scope of services, changes in data handling, changes in data processing locations, changes in Vendor ownership).
   iv. All Vendors providing goods or services, regardless of criticality, though the depth of application will be risk-based.
   v. Specifically, this Policy applies with heightened scrutiny to DSPs that process, store, transmit, or otherwise access the University's data, especially Bulk U.S. Sensitive Personal Data or Government-Related Data, and their direct or indirect interactions with Countries of Concern or Covered Persons, including those designated by the National Security Division under 28 CFR § 202.211(a)(5).

vi. All sub-contractors and downstream Vendors within a Vendor's supply chain where the University has direct or indirect oversight, especially concerning data access and processing.

b. General Policy Requirements:

i. Risk-Based Approach: The depth and frequency of both Due Diligence and ongoing Vendor management activities will be directly proportional to the criticality of the Vendor, the nature of services provided, the level of access to the University's data (especially sensitive data), and the overall risk profile of the engagement. For DSPs, particularly those handling Bulk U.S. Sensitive Personal Data or Government-Related Data, this means a significantly higher level of scrutiny and continuous monitoring.

ii. Proportionality: Resources allocated to Vendor management and Due Diligence will be commensurate with the identified risks and strategic importance of the Vendor relationship.

iii. Transparency and Documentation: All Vendor management and Due Diligence activities, findings, decisions, and communications must be thoroughly documented, securely stored, and readily retrievable for audit purposes to demonstrate compliance with the DOJDSP and the University's DSCP.

iv. Continuous Monitoring: Vendor Due Diligence is not a one-time event. Vendors, especially Critical Vendors and DSPs, will be subject to ongoing performance monitoring, security assessments, and periodic re-assessments throughout the entire contract lifecycle.

v. Collaboration and Accountability: Effective Vendor management and Due Diligence require cross-functional collaboration. Clear roles, responsibilities, and accountability will be established for all parties involved, including third-party Vendors, procurement, legal, IT, information security, compliance, and finance.

vi. "Know Your Data" and "Know Your DSP": In association with this Policy, the University commits to understanding the types, volumes, and sensitivity of data it collects, processes, and shares with third parties. For DSPs, this includes understanding their data handling practices, infrastructure, sub-processors, and any direct or indirect connections to "Countries of Concern" or "Covered Persons."

vii. Compliance First: All Vendor engagements must adhere to applicable laws, regulations, and internal policies, with strict adherence to data protection and national security requirements under the DOJDSP and the University's DSCP, as well as applicable contracts, and where applicable, the University's Terms & Conditions.

4. Roles and Responsibilities

a. University Oversight:

i. Board and Senior-Level Administrative Oversight: This Policy is subject to the University's DSCP and the Board and Senior-Level Administrative Oversight provisions set forth therein.

b. Vendor Management Committee ("VMC"):

i. The VMC shall consist of the Executive Director for Procurement Compliance, the UKHC System Privacy Officer, the Chief Information Security Officer and the University's Data Security Compliance Officer ("DSCO"), the latter of whom is responsible for the day-to-day implementation of the University's DSCP.

ii. The VMC shall:

A. Review and approve high-risk Vendor engagements, including all DSPs handling Bulk U.S. Sensitive Personal Data or Government-Related Data;
B. Oversee the overall effectiveness of this Policy; and
C. Review and approve significant changes to Critical Vendor relationships.

c. Procurement:

i. Lead the Vendor sourcing and selection process.
ii. Coordinate and facilitate all Due Diligence activities.
iii. Manage the Request for Proposal ("RFP") or Request for Information ("RFI") and contract negotiation processes.
iv. Maintain a centralized Vendor management system/database.
v. Ensure that contractual agreements include all necessary clauses related to Due Diligence, risk management, performance, data protection, and DSP compliance.

d. Office of Legal Counsel ("General Counsel"):

i. Upon the request of other internal parties, review and approve all Vendor contracts and Data Processing Addendums (DPAs).
ii. Advise on legal and regulatory compliance aspects of Vendor relationships that involve the DOJDSP or the University's DSCP.
iii. Assist in the determination of Prohibited or Restricted Transactions under the DOJDSP and provide advice on reporting, licensing, and specific contractual requirements.
iv. Manage any litigation or regulatory inquiries related to Vendor conduct.

e. Information Technology Services Security Department (IT Security) shall, where relevant to the Vendor's access and activities:

i. Lead the security assessment portion of Due Diligence for all Vendors involved in a Covered Data Transaction, particularly DSPs.
ii. Develop and maintain robust security questionnaires, standards, and assessment methodologies.
iii. Conduct risk assessments and review independent security assessments of DSPs.
iv. Require that DSPs' relevant security frameworks comply with the CISA Security Requirements for Restricted Transactions.
v. Review and approve DSP incident response plans and capabilities.
vi. Provide continuous security posture monitoring for critical DSPs.
vii. Validate DSP compliance with CISA Security Requirements for Restricted Transactions.

f. Information Technology Services Department (IT):

i. Assess Vendor's IT infrastructure, system architecture, integration compatibility, and operational resilience.
ii. Where applicable and feasible, IT will evaluate Vendor's disaster recovery and business continuity plans.
iii. Review and validate Vendor's data flow diagrams, data storage locations, and data processing environments.

g. DCSO:

i. Lead the assessment of Vendor compliance with the DOJDSP.
ii. Review Vendor's policies and procedures related to data privacy, data access, data retention, and data destruction.
iii. Advise on risk mitigation strategies to address identified compliance gaps, especially for DSPs.

iv. For Restricted Transactions with DSPs, oversee the implementation and verification of the required written Data Compliance Program, including risk-based procedures for verifying data flows and Vendor identity.
v. Ensure proper reporting to relevant authorities as required by regulations (e.g., DOJDSP).

h. Requesting Department:

i. Identify the business need for a Vendor and define clear service and product requirements.
ii. Participate actively in the Vendor selection and the Due Diligence process.
iii. Serve as the primary point of contact and manager of the Vendor relationship post-contracting.
iv. Monitor day-to-day Vendor performance against service level agreements ("SLAs"), including contractual obligations and key performance indicators ("KPIs").
v. Report any performance issues, security concerns, or compliance breaches in accordance with this Policy and the University's DSCP.

i. University Financial Services:

i. Where applicable, assess Vendor's financial stability, solvency, and creditworthiness.
ii. Where not managed via Requesting Department activities, process Vendor payment and manage financial aspects of contract.

j. Risk Management:

i. Where applicable, review Vendor's insurance coverage, ensuring adequate and appropriate limits, especially cyber liability insurance for DSPs.

5. Vendor Management and Due Diligence Process Throughout Vendor Lifecycle

a. Phase 1: Planning and Initial Assessment (Pre-Engagement Due Diligence)

i. **Initial Vendor Sourcing:** Procurement identifies potential vendors through market research, existing relationships, or an RFP/RFI process, or the Department/Division engages with a vendor.
ii. **Preliminary Vendor Risk Categorization:**
    1. Based on the nature of the service, potential access to the University's data or the data of others the University maintains and manages (type and volume), criticality to operations, and any potential involvement of Countries of Concern or Covered Persons, an initial risk category is assigned (e.g., Low, Medium, High, or DSP-specific categories like "DSP - Restricted Transaction Potential," "DSP - Prohibited Transaction Potential").
    2. This initial assessment triggers the depth of subsequent due diligence.
iii. **DSP Initial Screening:**
    1. For any potential DSP, an initial screening will be conducted to identify if the service involves Bulk U.S. Sensitive Personal Data or Government-Related Data, in accordance with this Policy and the University's DSCP.
    2. Simultaneously, a preliminary check will be made by Procurement regarding the DSP's (and its major sub-processors') connection to Countries of Concern or Covered Persons (e.g., based on headquarters, significant ownership, or primary operations) via a check of the DSP and associated entities and persons against any U.S. restricted lists.

3. If a Prohibited Transaction is identified, the engagement will generally not proceed without explicit legal guidance and, if applicable, an approved license from the DOJ.
4. If a Restricted Transaction is identified or the DSP or associated entities or persons appear on a U.S. restricted list, heightened due diligence requirements will be triggered.

b. Phase 2: Due Diligence and Vendor Selection

i. **Tailored Due Diligence Information Request:**

1. Based on the preliminary risk categorization, a comprehensive due diligence questionnaire and request for supporting documentation may be prepared and sent to the Vendor(s).
2. For DSPs, the questionnaire will be significantly expanded, with critical focus areas including, where applicable and required:
    (a) Company Information: Legal structure, ownership, management team, financial stability (audited financials, credit reports), and details of any mergers, acquisitions, or significant changes in control.
    (b) Operational Capabilities: Service delivery model, capacity, staffing, quality control, certifications (*e.g.,* ISO 9001), and a robust business continuity and disaster recovery plan.
    (c) Information Security:
        (1) Detailed information security program documentation (policies, standards, procedures).
        (2) Data classification, handling, and retention policies.
        (3) Specific controls for Bulk U.S. Sensitive Personal Data or Government-Related Data (including data flow diagrams).
        (4) Encryption mechanisms (in transit and at rest) and key data management practices.
        (5) Access control mechanisms (*e.g.,* Principle of Least Privilege, Multi-Factor Authentication, etc.), privileged access management, and comprehensive logging.
        (6) Network security controls (*e.g.,* firewalls, Intrusion Detection Systems/Intrusion Prevention Systems, segmentation, Distributed Denial of Service protection, etc.).
        (7) Vulnerability management, patch management, and secure coding practices.
        (8) Incident response plan, breach notification procedures, and defined SLAs for breach reporting, except where time periods for breach reporting are governed by KRS 61.932(2)(b).
        (9) Evidence of independent security assessments (*e.g.*, SOC 2 Type 2 reports, ISO 27001 certification, penetration test reports, security ratings from third-party services).
        (10) Personnel security practices (*e.g.,* background checks, security awareness training, etc.).
        (11) Capacity to comply with CISA Security Requirements.
    (d) Compliance & Legal:

(1) Confirmation of a written Data Compliance Program covering risk-based procedures for verifying data flows and Vendor identity.
(2) Require verification of compliance with CISA Security Requirements for Restricted Transactions.
(3) Identification of any direct or indirect connections to Countries of Concern or Covered Persons within the DSP's entire supply chain, including sub-processors and ownership structures.
(4) Detailed information on data residency, data sovereignty considerations, and mechanisms for lawful international data transfers.
(5) Litigation history, regulatory enforcement actions, and privacy-related complaints.
(6) Anti-bribery and corruption policies, and general code of conduct.

(e) Insurance: Proof of adequate insurance coverage, including robust cyber liability insurance with sufficient limits commensurate with the data handled and potential risks.
(f) Sub-contracting/Sub-processing: Comprehensive list of all sub-contractors and sub-processors who will access or process the data that the University will provide the Vendor access to, along with evidence of these third parties' own DOJDSP due diligence process.
(g) Reputation: Collection of references, media checks, and public record searches.

ii. **Vendor Response and Review:** Vendors provide the requested information. As distributed by Procurement to designated internal departments (VMC, General Counsel, IT, Compliance, Finance, Requesting Department, etc.) review the submitted documentation against the DOJSCP, the University's DSCP and other internal standards and policies.

iii. **Risk Analysis and Assessment:**
1. A comprehensive risk analysis is collected from other designated internal departments and performed by Procurement, identifying potential risks, assessing their likelihood and impact (quantitatively where possible), and evaluating the effectiveness of the Vendor's proposed controls.
2. For DSPs, this includes a deep dive into data breach potential, regulatory fine exposure, and national security implications under the DOJDSP and the University's DSCP.
3. For "Restricted Transactions," rigorous verification of the DSP's Data Compliance Program and CISA Security Requirements is mandatory.

iv. **Audits or On-Site Visits (for High-Risk Vendors/DSPs):** For high-risk or Critical Vendors, especially DSPs, on-site visits, independent security audits (*e.g.*, review of SOC 2 Type 2 reports, penetration testing reports), or direct technical assessments may be conducted.

v. **Reference Checks:** Where relevant and as directed by Procurement, contacting references provided by the Vendor, with specific questions regarding data security, compliance, and overall performance.

vi. **Consolidated Due Diligence Report:** Procurement, in collaboration with all reviewing departments, compiles a consolidated Due Diligence report summarizing findings, identified risks, and recommended mitigation strategies. This report includes a clear recommendation for engagement or rejection which shall comply with all requirements set forth in 28 CFR § 202.1104.

c. <u>Phase 3: Contract Negotiation and Approval</u>

i. **Risk Mitigation Plan Development:** If risks are identified, a detailed risk mitigation plan is developed jointly with the proposed Vendor, outlining specific actions and timelines to reduce risks to an acceptable level. For DSPs, this plan must specifically address any identified gaps in security controls, data handling practices, or compliance with DOJDSP and the University's DSCP.

ii. **Contract Negotiation:** As General Counsel, Procurement, and the prospective Vendor negotiate the contractual terms, the contract must incorporate:

1. Clearly defined scope of services and, where applicable, SLAs.
2. Robust data protection clauses (data breach notification requirements, audit rights, data deletion/return at termination, limitations on sub-processing, data ownership).
3. Specific clauses addressing DOJDSP requirements for Restricted Transactions, including adherence to the University's DSCP, CISA Security Requirements, audit rights, and recordkeeping obligations.
4. Indemnification, liability, and insurance requirements.
5. Right to audit and perform security assessments.
6. Termination clauses and exit strategy.
7. Confidentiality and intellectual property provisions.
8. Express representations and warranty by Vendor that all information provided by Vendor has been true and accurate, and as applicable, that Vendor is not a Covered Person and/or not subject to the Country of Concern jurisdiction requirements.

iii. **Final Approval:** The consolidated Due Diligence report, risk mitigation plan, and proposed contract are presented to the relevant approving authority or authorities (e.g., Enterprise Data Governance, Procurement). Approval is granted via signature to contracts by authorized University signers under applicable signature delegation procedures after consideration by those units required by University policies to provide prior review and commentary, and only if all risks are deemed acceptable or adequately mitigated. For "Restricted Transactions," explicit approval from the DSCO (with advice from General Counsel) is required.

d. <u>Phase 4: Ongoing Vendor Management and Monitoring</u>

i. **Vendor Onboarding:** New Vendors are formally onboarded, including system access provisioning, training (if necessary), and introduction to relevant University personnel.

ii. **Risk Monitoring and Review:**

1. <u>Continuous security monitoring</u>: Information Security will leverage security ratings services and other tools to continuously monitor the external security posture of critical DSPs using a risk-based approach.
2. <u>Financial monitoring</u>: Where determined relevant to the situation, University Financial Services will periodically review the financial health of Critical Vendors.

3. Compliance monitoring: The DSCO will track regulatory changes affecting DOJSCP compliance.
4. Change Management: Any significant changes in the Vendor's services, ownership, security posture, or sub-processors must be reported by the Vendor and the Requesting Department and will trigger a reassessment of risks.

iii. **Issue Resolution:** A clear process for logging, tracking, and resolving Vendor performance issues, disputes, or security incidents will be maintained by the Requesting Department and Procurement.

iv. **DSP-Specific Ongoing Obligations (for Restricted Transactions):**
1. Annual Audits: For DSPs involved in Restricted Transactions, the University, in coordination with the DSCO will ensure annual audits are conducted by an independent third party to verify compliance with the University's DSCP and CISA Security Requirements.
2. Recordkeeping: All records related to the Restricted Transaction, including the University's DSCP, audit reports, and security assessments, will be maintained for at least 10 years.
3. Reporting: the DSCO will ensure timely reporting to the DOJ as required by the DSP (e.g., annual reports for cloud-computing services based on equity interests).

e. Phase 5: Re-assessment and Contract Renewal/Termination

i. **Periodic Re-assessment & Recurring Due Diligence:** All Vendors are subject to periodic re-assessment based on their risk categorization:
1. High-Risk Vendors (including most DSPs): Annually or as significant changes occur.
2. Medium-Risk Vendors: Every 1-3 years or as significant changes occur.
3. Low-Risk Vendors: Every 3-5 years or as significant changes occur.
4. The re-assessment process mirrors the initial Due Diligence, but with a focus on changes since the last review.

ii. **Triggered Re-assessment:** Re-assessment may also be triggered by specific events:
1. Significant changes in the Vendor's ownership, management, or financial health, especially if it involves a "Country of Concern" or "Covered Person."
2. Changes in the scope of services or types of data accessed.
3. Security incidents, data breaches, or major vulnerabilities involving the Vendor or any of its sub-processors.
4. Negative publicity, regulatory actions, or compliance failures related to the Vendor.
5. Persistent poor performance or non-compliance with contractual terms.
6. Updates in relevant data protection laws or national security regulations (e.g., updates to the DOJDSP, CISA guidance).

iii. **Contract Renewal:** Prior to contract extension or renewal, a review of Vendor performance, risk profile, and continued business need will be conducted. Due Diligence re-assessment will inform the renewal or extension decision and any renegotiation of terms.

iv. **Contract Termination and Offboarding:**
1. When a contract is terminated (due to non-renewal, breach, or change in business need), a formal offboarding process is initiated.

2. This includes ensuring secure return or destruction of all University data and other data managed by the University held or accessed by the Vendor, revocation of access, retrieval of assets, and final financial reconciliation.
3. For DSPs, verification of data destruction/return through audit or certification is mandatory.

6. Documentation and Record Keeping

All documentation related to Vendor management and Due Diligence must be maintained in a centralized, secure, and auditable Vendor management systems or designated repositories. This includes, but is not limited to:

- Vendor contracts, DPAs, and all amendments.
- All Due Diligence questionnaires, responses, and supporting documentation.
- Internal risk assessment reports, findings, and mitigation plans.
- Approval records for Vendor engagements.
- Performance monitoring reports, SLAs, and KPIs.
- Issue logs and resolution documentation.
- For DSPs, specifically**:**
    - Data flow diagrams and data inventory.
    - Detailed security assessment reports (initial and ongoing).
    - Evidence of DSP's Data Compliance Program (for Restricted Transactions).
    - Audit reports verifying DSP compliance (for Restricted Transactions).
    - Records of any communication with the DOJ regarding DSP transactions (e.g., license applications, reporting).
    - Confirmation of data destruction/return at termination.

Records must be retained in accordance with the University's record retention policy and all applicable legal and regulatory requirements, including the DOJDSP's requirement to maintain records for at least 10 years for Covered Data Transactions.

7. Training and Awareness

All employees involved in Vendor management or Due Diligence activities will receive training on this Policy, related procedures, and the specific implications of the DOJDSP. Training will emphasize the importance of identifying and escalating potential risks, particularly those related to "Countries of Concern" and "Covered Persons."

8. Non-Compliance and Penalties

The non-compliance and penalty commentary included in the DCSP and as implemented via the DOJDSP are incorporated into this Policy.

9. Policy Review

This Policy will be reviewed by the DSCO at least annually, or more frequently if there are significant changes in:

- Applicable laws and regulations (e.g., updates to the DOJDSP, CISA guidance, etc.).
- Industry best practices for Vendor management and overall due diligence.
- the University's business operations, risk appetite, or strategic direction.
- The global geopolitical landscape impacting supply chain and data security risks.

Attachment 2

University of Kentucky
Security Requirements Policy
For U.S. Department of Justice's Data Security Program

SECURITY REQUIREMENTS FOR RESTRICTED TRANSACTIONS
E.O. 14117 Implementation

JANUARY 2025

SECURITY REQUIREMENTS FOR RESTRICTED TRANSACTIONS
Pursuant To Exec. Order 14117, *Preventing Access To Americans' Bulk Sensitive Personal Data And United States Government-Related Data By Countries Of Concern*

On February 28, 2024, President Biden signed Executive Order (E.O.) 14117, *Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern*, to address national-security and foreign-policy threats that arise when countries of concern and covered persons can access bulk U.S. sensitive personal data or government-related data that may be implicated by the categories of restricted transactions.

As directed by E.O. 14117, CISA has developed the following security requirements to apply to classes of restricted transactions identified in regulations issued by the Department of Justice (DOJ). *See generally* 28 C.F.R. part 202 (identifying classes of restricted transactions at 28 C.F.R. § 202.401).

BACKGROUND

The security requirements are designed to mitigate the risk of sharing U.S. government-related data or bulk U.S. sensitive personal data with countries of concern or covered persons through restricted transactions.[1] They do this by imposing conditions specifically on the covered data, as defined below, that may be accessed as part of a restricted transaction; on the covered systems, as defined below, more broadly; and on the organization as a whole. While the requirements on covered systems and on an organization's governance of those systems apply more broadly than to the data at issue and the restricted transaction itself, CISA assesses that implementation of these requirements is necessary to validate that the organization has the technical capability and sufficient governance structure to appropriately select, successfully implement, and continue to apply the covered data-level security requirements in a way that addresses the risks identified by DOJ for the restricted transactions. For example, to ensure and validate that a covered system denies covered persons access to covered data, it is necessary to maintain audit logs of such accesses as well as organizational processes to utilize those logs. Similarly, it is necessary for an organization to develop identity management processes and systems to establish an understanding of what persons may have access to different data sets.

In addition to requirements on covered systems, applying security requirements on the covered data itself that may be accessed in a restricted transaction is also necessary to address the risks. The specific requirements that are most technologically and logistically appropriate for different types of restricted transactions may vary. For example, some transactions may be amenable to approaches that minimize data or process it in such a way that does not reveal covered data to covered persons. In other cases, techniques such as access control and encryption may be more appropriate to deny any access by covered persons to covered data. The security requirements contemplate multiple options to minimize the risk to covered data, though all of the options build upon the foundation of the requirements imposed on covered systems and the organization as a whole. While U.S. persons engaging in restricted transactions must implement all of the organizational- and covered-system level requirements, such persons will have some flexibility in determining which

[1] CISA notes that these security requirements are, as required by the E.O., designed to "address the unacceptable risk posed by restricted transactions, as identified by the Attorney General." E.O. 14117 Sec. 2(d). They are not intended to reflect a comprehensive cybersecurity program. For example, several areas addressed in CISA's Cross-Sector Cybersecurity Performance Goals (CPGs), available at https://www.cisa.gov/cross-sector-cybersecurity-performance-goals, are not reflected in the data security requirements, even though the CPGs themselves are a common set of protections that CISA recommends all critical infrastructure entities voluntarily implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques. As the operational lead for federal cybersecurity and national coordinator for critical infrastructure security and resilience, CISA recommends that all U.S. persons implement cybersecurity best practices in light of the risk and potential consequence of cyber incidents.

combination of data-level requirements is sufficient to address the risks posed, based on the nature of the transaction, so long as the combination of security mechanisms deployed fully and effectively prevents access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern. If a combination of security mechanisms proves to be insufficient to prevent such access, that combination of security mechanisms will be considered invalid in protecting future access to covered data by covered persons.

IN GENERAL

The security requirements provide the organizational- and covered system-level requirements (Section I) and covered data-level requirements (Section II) which U.S. persons engaging in restricted transactions must meet. These security requirements are in addition to any compliance-related conditions imposed in applicable DOJ regulations. See 28 C.F.R. § 202.1001–202.1201. References below to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF),[2] NIST Privacy Framework (PF),[3] and CISA's Cross-Sector Cybersecurity Performance Goals (CPGs)[4] are intended to help the reader understand which aspects of existing frameworks, guidance, or other resources these security requirements are based upon, consistent with the requirements of the E.O. Understanding and applying these security requirements does not require a reader to also understand and apply the referenced resources.

DEFINITIONS

To the extent these security requirements use a term already defined in DOJ's regulation, see 28 C.F.R. § 202.201-202.259, CISA's use of that term below carries the same meaning.

For the purpose of these security requirements:

- *Asset* means data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes.
- *Covered data* means government-related data bulk U.S. sensitive personal data.
- *Covered system:*
    - means an information system used to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, view, receive, collect, process, maintain, use, share, disseminate, or dispose of (collectively, "interact with") covered data as part of a restricted transaction, regardless of whether the data is encrypted, anonymized, pseudonymized, or de-identified; and
    - does not include an information system (e.g., an end user workstation) that has the ability to view or read sensitive personal data (other than sensitive personal data that constitutes government-related data) but does not ordinarily interact with such data in bulk form.[5]
- *Information system* means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- *Network* means a system of interconnected components, which may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

[2] NIST, Cybersecurity Framework ver. 2.0, available at https://www.nist.gov/cyberframework.
[3] NIST, Privacy Framework ver. 1.0, available at https://www.nist.gov/privacy-framework.
[4] CISA, Cross-Sector Cybersecurity Performance Goals, available at https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.
[5] For example, if an end user workstation only interacts with individual records of U.S. sensitive personal data, although it may have the ability to "read" or "view" bulk U.S. sensitive personal data, it is not deemed on its own to be a covered system unless it takes further actions outlined in the definition of covered system (e.g., maintaining or processing data in excess of the bulk thresholds) with respect to such data. Note that there are no bulk thresholds for government-related data and individual records would be considered covered data. Thus, end user workstations that interact with government related data are covered systems.

SECURITY REQUIREMENTS

I. ***Organizational- and System-Level Requirements.*** For any covered system:

A. Ensure basic organizational cybersecurity policies, practices, and requirements, including all of the following, are in place:

1. Identify, prioritize, document all assets of the covered system.

a. Maintain, to the maximum extent practicable, an updated inventory of covered system assets with each system's respective internet protocol (IP) address (including IPv6).[6] (*NIST CSF 2.0 ID.AM-01, CISA CPGs 1.A*)

b. Ensure inventory is updated on a recurring basis, no less than monthly for Information Technology (IT) assets. (*NIST CSF 2.0 ID.AM-08, CISA CPGs 1.A*)

2. Designate, at an organizational level, an individual (*e.g.,* a Chief Information Security Officer) responsible and accountable for (1) cybersecurity and (2) governance, risk, and compliance functions (GRC). This could be one individual responsible and accountable for both areas, or one individual for each of these two areas. (*NIST CSF 2.0 GV.RR-02, CISA CPGs 1.B*)

3. Remediate known exploited vulnerabilities (KEVs) in internet-facing systems within a risk-informed span of time, prioritizing the most critical assets first and completing remediation for all such vulnerabilities within 45 calendar days. (*NIST CSF 2.0 ID.RA-01 and 08 CISA CPGs 1.E*)

a. Implement alternative compensating requirements, should patching not be feasible.

b. Establish a process to evaluate, after patching, whether internet-facing covered systems with KEVs were compromised prior to patching.

4. Document and maintain all vendor/supplier agreements for covered systems (*e.g.*, third-party network connection agreements), including contractual IT and cybersecurity requirements. (*NIST CSF 2.0 GV.SC-05, 06, 07, 10, CISA CPGs 1.G, 1.H, 1.I*)

5. Develop and maintain an accurate network topology of the covered system and, to the extent technically feasible, any network interfacing with a covered system to facilitate visibility into connections between assets, and aid in timely identification of and response to incidents. (*NIST CSF 2.0 ID.AM-03, CISA CPGs 2.P*)

6. Adopt and implement an administrative policy that requires approval before new hardware or software is deployed in/on a covered system. U.S. persons engaging in restricted transactions must maintain a risk-informed allowlist of approved hardware and software for covered systems. (*NIST CSF 2.0 GV.PO-02, ID.RA-09, ID.AM-08, PR.PS-01, 02, 03, CISA CPGs 2.Q*)

7. Develop and maintain incident response plan(s) applicable to covered systems, which should be reviewed annually and updated as appropriate. (*NIST CSF 2.0 ID.IM-04, CISA CPGs 2.S, 5.A*)

B. Implement logical and physical access controls to prevent covered persons or countries of concern from gaining access to covered data that that does not comply with the data-level requirements (Section II) including through information systems, cloud-computing platforms, networks, security systems, equipment, or software. (*NIST CSF 2.0 PR.AA-01 through PR.AA-06*) Specifically, U.S. persons engaging

[6] This list may be maintained in an automated fashion that tracks dynamic changes in the covered system (*e.g.*, automatic provisioning of virtual machines or containers in a cloud environment) and may consist of several constituent parts for discrete subsystems.

in restricted transactions must:

1. Enforce multifactor authentication (MFA) on all covered systems (*e.g.*, by requiring an Authentication Assurance Level (AAL) AAL2 or AAL3 authenticator as defined in the most recent version of NIST Special Publication 800-63B and/or its supplements), or in instances where MFA is not technically feasible and/or not enforced, require passwords have sufficient strength, including sufficient length of 15 or more characters. (*NIST CSF 2.0 PR.AA-03, PR.AA-04, CISA CPGs 2.B, 2.H*)

2. Promptly revoke (*e.g.*, on day of departure or within a risk-informed timeframe) any individual credentials, shared credentials, and/or authorized access to covered systems upon termination or change in roles for any individual with access to covered system(s). (*NIST CSF 2.0 GV.RR-04, PR.AA-01, & PR.AA-04, CISA CPGs 2.D*)

3. Collect logs for covered systems pertaining to access- and security-focused events (*e.g.*, intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network, and detection of unsuccessful login events), and store such logs for use in both detection and incident response activities (*e.g.*, forensics to assist in detection, response, and recovery). Implement a process to notify cybersecurity personnel when a critical log source, such as an operating system event logging tool, is not producing and retaining logs as expected. (*NIST CSF 2.0 PR.PS-04, & DE.CM-03, and 09, CISA CPGs 2.T, 2.U*)

    a. Securely store collected logs in a central system, such as a security information and event management tool or central database, for at a minimum 12 months. In the event of a data breach or a violation of these security requirements, logs should be maintained until final resolution of the matter by the U.S. Government.

    b. Ensure that collected logs may only be accessed or modified by authorized and authenticated users.

4. Implement configurations to deny by default (*e.g.*, by requiring authentication) all connections to covered systems and any network on which covered systems reside, unless connections are explicitly allowed for specific system functionality. (*NIST CSF 2.0 PR.PS-01*)

5. Issue and manage, at an organizational level, identities and credentials for authorized users, services, and hardware, with sufficient attributes available to prevent access by covered persons or countries of concern to covered data that that does not comply with the data-level requirements (Section II). Limit system access to the types of transactions and functions that authorized users are permitted to execute. (*NIST CSF 2.0 PR.AA-05, CISA CPGs 2.C*)

C. Conduct an internal data risk assessment that evaluates whether and how the overall approach selected and implemented pursuant to Section II sufficiently prevents access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern, taking into consideration the likelihood of disclosure and the likelihood of harm based on the nature of the transaction and the data at issue, to include potential data misuse and associated consequences. The risk assessment must include a mitigation strategy outlining how implementation will prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern. The risk assessment should be reviewed annually by the organization and updated as appropriate. (*NIST Privacy Framework ID.RA-P1, NIST Privacy Framework ID.RA-P3, NIST Privacy Framework ID.RA-P4, NIST Privacy Framework ID.RA-P5*)

II. ***Data-Level Requirements.*** For any restricted transaction, implement a combination of the following mitigations that, taken together, is sufficient to fully and effectively prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern, consistent with the data risk assessment described in Section I.C.:

A. Apply data minimization and data masking strategies to reduce the need to collect, or sufficiently obfuscate, respectively, covered data to prevent visibility into that data, without precluding the U.S. persons engaging in restricted transactions from conducting operations with the data. These strategies must include:

1. Maintaining and implementing a written data retention and deletion policy, to be reviewed annually and updated as appropriate. (*NIST Privacy Framework GV.PO-P1, CT.PO-P2*)

2. Processing data in such a way to either render it no longer covered data or minimize the linkability to U.S. person entities before it is subject to access by a covered person or country of concern. (*NIST Privacy Framework CT.DP-P2*)

    a. This may be achieved through application of techniques such as aggregation, pseudonymization, de-identification, or anonymization.

    b. When implemented, observability and linkability of data must be minimized to ensure U.S. person identities cannot be inferred or extrapolated from the individual data set at issue or in combination with other data sets the recipient or recipient-linked organizations are known to hold.

    c. Aggregations of covered data must be based on at least the number of records required to render the data "bulk" under the regulations found at 28 C.F.R. § 202.205.

3. Treating information systems that implement such processing as covered systems subject to the requirements of Section I. (*NIST Privacy Framework CT.DP-P4, CM.AW-P3, GV.PO-P2*)

B. Apply encryption techniques to protect covered data during the course of restricted transactions. These techniques must include:

1. Comprehensive Encryption: Encrypt covered data in a restricted transaction, regardless of type, during transit and storage.[7] (*NIST Privacy Framework CT.DP-P1, PR.DS-P1, PR.DS-P2, CISA CPGs 2.K*)

2. Key Management: Generate and securely manage cryptographic keys used to encrypt covered data, including the following practices: (*NIST Privacy Framework CT.DP-P1 & PR.DS-P2, CISA CPGs 2.L*)

    a. Do not co-locate encryption keys with covered data.

    b. Do not store encryption keys, via any mechanism (physically or virtually), in a country of concern.

    c. Covered persons must not be authorized to have access to encryption keys.

[7]For the purposes of this requirement, CISA considers comprehensive encryption to mean cryptographic algorithms, ciphers, and protocols that are ordinarily accepted by U.S. persons with significant expertise in cryptography as being sufficient to provide confidentiality and integrity protections to sensitive data against compromise by currently known techniques and a level of computing power that is reasonably foreseeable to be available to any person, organization, or country in the near future. CISA considers U.S. Government approved encryption algorithms, ciphers, and protocols to meet this standard, but organizations may determine that other algorithms, ciphers, and protocols also qualify. For connections made using Transport Layer Security (TLS), only version 1.2 or higher is considered comprehensive encryption.

d. All information systems responsible for the storage of and access to encryption keys must be considered covered systems subject to the requirements of Section I.

C. Apply privacy enhancing technologies, such as privacy preserving computation (*e.g.*, homomorphic encryption), or differential privacy techniques (*e.g.*, inject sufficient noise into processing of data to preclude the reconstruction of covered data from the processed data), to process covered data. Use of such techniques are subject to the following:

1. The application of privacy enhancing technologies must not reveal to covered persons participating in the restricted transaction covered data or information that could reasonably likely be used to reconstruct covered data, including by linking processed data with other data sets (*e.g.*, allowing a covered person to participate in a privacy preserving computation that requires trusted parties would not be permissible).

2. For the avoidance of doubt, information systems that implement such processing are covered systems subject to the requirements of Section I. (*NIST Privacy Framework CT.DP-P1*)

D. Configure the previously outlined identity and access management techniques to deny authorized access to covered data by covered persons and countries of concern within all covered systems. (*NIST Privacy Framework PR.AC-P4*)

Attachment 3
University of Kentucky
Research Policy
For U.S. Department of Justice's Data Security Program

1. Statement of Purpose: This Research Policy ("Policy") outlines the principles and procedures governing University of Kentucky and its affiliated corporations' ("University") research activities in which access is granted to certain types and volumes of data to individuals and entities that are subject to the restrictions and prohibitions of the U.S. Department of Justice Data Security Program ("DOJDSP") in order to achieve compliance with the DOJSCP, the University's Data Security Compliance Program ("DSCP") and related policies and procedures.

a. This Policy aims to:

i. Establish a framework for identifying, assessing, and mitigating risks associated with research activities that may involve "Covered Data" including "Bulk U.S. Sensitive Personal Data" or "Government-Related Data" as each term is defined by the DOJDSP and in Section 2 of this Policy.
ii. Ensure compliance with requirements to protect national security by preventing unauthorized access to bulk Covered Data by "Countries of Concern" and "Covered Persons" as each term is defined by the DOJDSP and in Section 2 of this Policy.
iii. Ensure that all research adheres to the prohibitions, restrictions, and security requirements set forth by the DOJDSP and the DSCP.
iv. Define roles and responsibilities for compliance, due diligence, recordkeeping, and reporting related to DOJDSP and DSCP requirements.
v. Safeguard sensitive data involved in research, protecting the privacy of U.S. persons and national security interests.
vi. Mitigate the risk of civil and criminal penalties for non-compliance with the DOJDSP.

2. Definitions: All capitalized terms used in this Policy shall have the meanings set forth in the DSCP.

3. General Provisions:

a. Policy Application: This Policy applies to all faculty, staff, students, contractors, and any other individuals affiliated with the University who engage in, propose, or manage research, whether domestic or international (for purposes of this Policy, "Researcher(s)") that involve Covered Data as defined by the DOJDSP and the University's DSCP. This includes, but is not limited to the following data, whether or not the Covered Data is anonymized, pseudonymized, de-identified, or encrypted:

i. Research involving human 'omic data (genomic on more than 100 U.S. persons, or epigenomic, proteomic, or transcriptomic data on more than 1,000 U.S. persons).
ii. Research involving biometric identifiers on more than 1,000 U.S. persons.
iii. Research involving precise geolocation data on more than 1,000 U.S. devices.
iv. Research involving personal health data on more than 10,000 U.S. persons.
v. Research involving personal financial data on more than 10,000 U.S. persons.

vi. Research involving covered personal identifiers on more than 100,000 U.S. persons.
vii. Activities with foreign entities, individuals, or organizations involving any of items 3(a)(i)-(vi) above or item 3(a)(viii) below.
viii. Any activities that may involve Data Brokerage, vendor agreements, employment agreements, or investment agreements that grant access to Covered Data.

b. Policy Requirements and Phases: All Researchers who propose to engage in research for which the DOJDSP and the University's DSCP applies as described in section 3(a) of this Policy must comply with the following DOJDSP and University DSCP requirements:

i. <u>Phase 1 - Prior to initiating research activities involving a data transaction covered by or to which the DOJDSP and the University's DSCP applies:</u>

1. **Data Assessment and Classification:** When a proposed Covered Data Transaction is proposed:
   - **a.** The University's Security, Export, Compliance and University Research Engagement office ("SECURE") must conduct a thorough review of all data types and volumes involved in the proposed research to determine if they constitute Covered Data under the DOJDSP and the University's DSCP. This includes assessing if any data will meet "bulk" thresholds.
   - **b.** Special attention must be paid to the potential collection or use of precise geolocation data from within areas on the Government-Related Location Data List ("GRLD List") as set forth in 28 C.F.R. § 202.1401.
   - **c.** The classification process must proceed even if the data is anonymized, pseudonymized, de-identified, or encrypted, as these measures do not exempt data from DOJDSP regulations and the University's DSCP applications if it meets "bulk" thresholds or constitutes government-related data.

2. **Partner and Covered Person Screening:**
   - **a.** When presented with research activities potentially subject to the DOJDSP or the University DSCP, SECURE must conduct due diligence to screen all potential collaborators and other parties, including individuals and entities, against the list(s) of Countries of Concern and Covered Persons. This includes using vendor-screening software that incorporates updates to any published Covered Persons List and accounts for alternative spellings or also-known-as designations.
   - **b.** If a potential collaborator or other party is identified as a Covered Person or is associated with a Country of Concern, the research activities must undergo heightened scrutiny.

3. **Prohibited Transaction Review:** Any proposed research activity that involves a Prohibited Transaction (*e.g.*, but without limitation, Data Brokerage of Covered Data to a Country of Concern or Covered Person, or any access to bulk human 'omic data by a Country of Concern or Covered Person) is strictly forbidden unless an explicit license from the DOJ National Security Division (NSD) is obtained. Requests for such licenses will be reviewed by the NSD under a "presumption of denial." Any license application contemplated by a Researcher must first be approved for submission by both SECURE and the Office of Legal Counsel ("General Counsel").

4. **Restricted Transaction Compliance Plan:**
    - **a.** If a proposed research activity involves a Restricted Transaction (*e.g.,* an agreement providing access to a Country of Concern or Covered Person), a detailed compliance plan must be developed and approved by SECURE in advance of the Restricted Transaction proceeding.
    - **b.** This plan must demonstrate how the research activity will adhere to the CISA Security Requirements and the University's DSCP, including:
        - (i) **Organizational and System-Level Requirements:**
            - (1) Identifying, prioritizing, and documenting all assets of a covered system.
            - (2) Designating an individual accountable for cybersecurity and compliance.
            - (3) Documenting all vendor and supplier agreements.
            - (4) Developing and implementing incident response plans.
            - (5) Implementing access controls to prevent unauthorized access by Covered Persons or Countries of Concern.
            - (6) Conducting internal risk assessments to guide data-level requirements.
            - (7) Remediating all known exploited vulnerabilities within forty-five (45) calendar days, starting with critical assets.
        - (ii) **Data-Level Requirements:** Implementing a combination of mitigations, such as:
            - (1) Data minimization and data masking strategies.
            - (2) Comprehensive encryption techniques.
            - (3) Privacy-enhancing technologies.
            - (4) Identity and access management techniques to deny unauthorized access to Covered Data.

5. **Contractual Agreements:**
    - **a.** All research activity agreements (and/or the University's standard terms and conditions applicable to vendors) in which Covered Data will or could be shared to a Covered Person or Country of Concern must include specific clauses as directed by General Counsel, including without limitation representations of applicable parties and prohibiting any transactions that violate the DOJDSP.
    - **b.** For Restricted Transactions, research agreements must stipulate compliance with CISA's Security Requirements and incorporate provisions for onward-transfer clauses for any data shared with foreign persons who are not Covered Persons, along with reporting of known or suspected violations of those clauses.
    - **c.** These agreements must clearly define data ownership, access rights, data handling protocols, and termination clauses in the event of DOJDSP non-compliance.

ii. <u>Phase 2 - During Research Activities</u>:

1. **Continuous Monitoring and Due Diligence:**

(a) Researchers are responsible for continuous monitoring of data flows and collaborator and other party activities to ensure ongoing DOJDSP and University DSCP compliance.
(b) Any changes in collaborator or other party status (*e.g.,* a collaborator or other party becoming a Covered Person or associated with a Country of Concern) must be immediately reported to SECURE.
(c) Periodic screening of collaborators and other parties by Researchers in consultation with SECURE should be conducted to verify their status in accordance with the DOJDSP, the University's DSCP, the University's Vendor Management and Due Diligence Policy concerning DOJDSP compliance, and this Policy.

2. **Data Security Measures:**
   (a) Strict adherence to the CISA Security Requirements is mandatory for all Restricted Transactions. This includes maintaining robust cybersecurity infrastructure, access controls, encryption, and data minimization practices.
   (b) All data collected, processed, or stored as part of a research activity involving Covered Data must be protected against unauthorized access, disclosure, alteration, and destruction.

3. **Recordkeeping:**
   (a) Researchers, SECURE, and other University employees and students must maintain detailed and auditable records of all Covered Data Transactions, including:
      (i) Types and volumes of data involved.
      (ii) Identity of all parties to the transaction.
      (iii) Security measures implemented.
      (iv) Due diligence performed.
      (v) Any rejected transactions.
   (b) Records must be maintained for a minimum of ten (10) years.

4. **Reporting Obligations:**
   (a) **Rejected Transactions:** Any person who receives and rejects a Prohibited Transaction involving Data Brokerage must report it SECURE within three (3) days of the rejection, even if automatically rejected by software or other means, and the University, via SECURE, must report it to the DOJ National Security Division within fourteen (14) days of the rejection, even if automatically rejected by software or otherwise.
   (b) **Annual Reports (if applicable):** With the assistance of applicable Researchers and other University employees and students, for Restricted Transactions associated with research activities involving cloud-computing services where twenty-five percent (25%) or more of the U.S. person's equity interests are owned by a Country of Concern or Covered Person, SECURE will submit annual reports to the DOJ.
   (c) **On-Demand Reporting:** All University employees and students will be prepared, and where directed, to do so via SECURE, to furnish reports and information to the DOJ under oath at any time, before, during, or after a transaction.

(d) **Known or Suspected Violations:** Any known or suspected violations of the DOJDSP or contractual clauses related to disallowed onward transfers must be immediately reported to SECURE for onward reporting to the DOJ.

iii. **Phase 3 - Annual Data Compliance Program and Auditing:** Pursuant to the terms of the University's DSCP and in conformity with the DOJDSP, at the direction and oversight of the University's Data Security Compliance Officer (DSCO), who shall oversee and receive input from SECURE and others within the University community will provide input to the DSCO to enable the University will conduct those audits of the data compliance program and related software and systems as required by the DOJSCP and the DSCP. Audit results and related records must be retained for at least ten (10) years. Researchers, SECURE, and all other applicable University employees and students will assist in fulfilling these requirements.

4. Roles and Responsibilities: The following individuals and units have the identified roles and responsibilities:

a. **Board and Senior-Level Administrative Oversight** – This Policy is subject to the University's DSCP and the Board and Senior-Level Administrative Oversight provisions set forth therein.

b. **Researchers:**
   i. Responsible for understanding and complying with this Policy for all research activities.
   ii. Involved in conducting initial data assessment and collaborator and other party screening assessment.
   iii. Develop and implement the compliance plan for Restricted Transactions associated with the research activities.
   iv. Ensure ongoing adherence to all data security measures.
   v. Promptly report any potential DOJDSP violations, University DSCP violations, or changes in collaborator or other party status.

c. **SECURE:**
   i. Provide guidance and support to Researchers on DOJDSP requirements.
   ii. Review and approve research agreements for DOJDSP compliance.
   iii. Assist in collaborator and other party screening and due diligence.
   iv. Facilitate necessary reporting to the DOJ.
   v. Develop and deliver education and training on DOJDSP and DSCP requirements.
   vi. Liaise with the General Counsel, Procurement and Information Technology Services, as necessary.

d. **Information Technology Service's Security Offices and Personnel:**
   i. Implement and maintain technical security controls consistent with CISA Security Requirements.
   ii. Provide expertise on data minimization, encryption, and access management.
   iii. Assist in data flow mapping and vulnerability remediation.
   iv. Liaise with SECURE, General Counsel, and Procurement, as necessary.

e. **Individuals/Contractors:** All individuals, whether Researchers, vendors (pursuant to the University's Vendor Management and Due Diligence Policy on DOJDSP/DSCP matters) or contractors who are involved in research activities are responsible for understanding and adhering to the DOJDSP, the University's DSCP, and this Policy.

5. Education, Training and Awareness: The University will provide access to education and training and awareness programs to all relevant employees and students on DOJDSP and the University's DSCP requirements, this Policy, and other relevant University policies and procedures.

6. Non-Compliance and Penalties: The non-compliance and penalty commentary included in the DCSP and as implemented via the DOJDSP are incorporated into this Policy.

7. Policy Review: This Policy will be reviewed at least annually by the University's DSCO, who shall oversee and receive input from SECURE and others within the University community, or more frequently if there are significant changes in:

a. Applicable laws and regulations (*e.g.,* updates to the DOJDSP, CISA guidance, etc.).
b. Academic and medical research higher education institution best practices for research activities and overall due diligence.