Data Governance Procedures and Standards

To support its mission of teaching, research, and public service, the University of California, Riverside (UCR) must ensure its institutional data is governed effectively. Data governance provides the structure for managing data as a valuable asset, promoting its understandability, trustworthiness, accessibility, and privacy.

The following standards augment systemwide policies by establishing detailed procedures for classifying, documenting, and managing UCR's institutional data. These standards cover critical areas including data classification, documentation, definition approval, quality management, privacy, access and review, and data integration. They also establish requirements for the creation of Institutional Data Products and the retention and destruction of data, ensuring that all data is handled appropriately throughout its entire lifecycle.

The systemwide policies and guidelines that apply and that these standards help implement are:

Regents Policy 1111

Electronic Information Security Policy (IS-3)

University Records Management Program (RMP-1)

Records Retention and Disposition: Principles, Processes, and Guidelines (RMP-2)

Vital Records Protection (RMP-4)

Protection of Administrative Records Containing Personally Identifiable Information (RMP-7)|

PACAOS 130.00: Policies Applying to the Disclosure of Information from Student Records

UC Statement of Privacy Values

I. Data Governance Roles and Responsibilities

Data Governance Advisory Board

The Data Governance Advisory Board is a cross-campus collaboration of leaders representing various data domains. The advisory board is accountable for championing strategic data governance and architecture direction with Campus partners. The board's responsibilities include:

- Develop strategies, standards, and policies to make trusted data available in a secure manner.
- Develop the standards for when data is considered trustworthy.
- Define data domains and assign data owners for each.
- Monitor adherence to data definition standards and data quality standards.
- Review data governance and reporting project requests and roadmaps.
- Serve as the final escalation point for appeals to data access decisions made by a Data Owner.
- Provide a forum for Data Owners and campus representatives to balance data availability with privacy, compliance, and security.

Data Owner

Every institutional data domain will be assigned a Data Owner. A data domain is a logical grouping of data that pertains to a common purpose, object, or concept. Data Owners are accountable for the strategic management of the data domain and for ensuring the compliance of their data domain with data governance policy, practices, and all applicable laws. Key responsibilities of a Data Owner include:

- Appointing data steward(s) for the data entrusted in their care.
- Establishing data classification based on recommendations from data stewards.
- Setting access guidelines for critical data in their domain.
- Supporting initiatives to improve the confidentiality, integrity, availability, and effectiveness of University information.
- Work to improve data literacy of users of the data they manage.
- Provide strategic oversight for the use of their domain's data in Institutional Data Products, including AI products, to ensure alignment with university policies and strategic goals.

Data Steward

A Data Steward is responsible for the day-to-day management of a specific campus data asset. Data Stewards are assigned to the role by a Data Owner. The Data Steward is accountable for managing the availability, usability, integrity, and security of campus data. A Data Steward's responsibilities include:

- Create and document clear and concise data definitions.

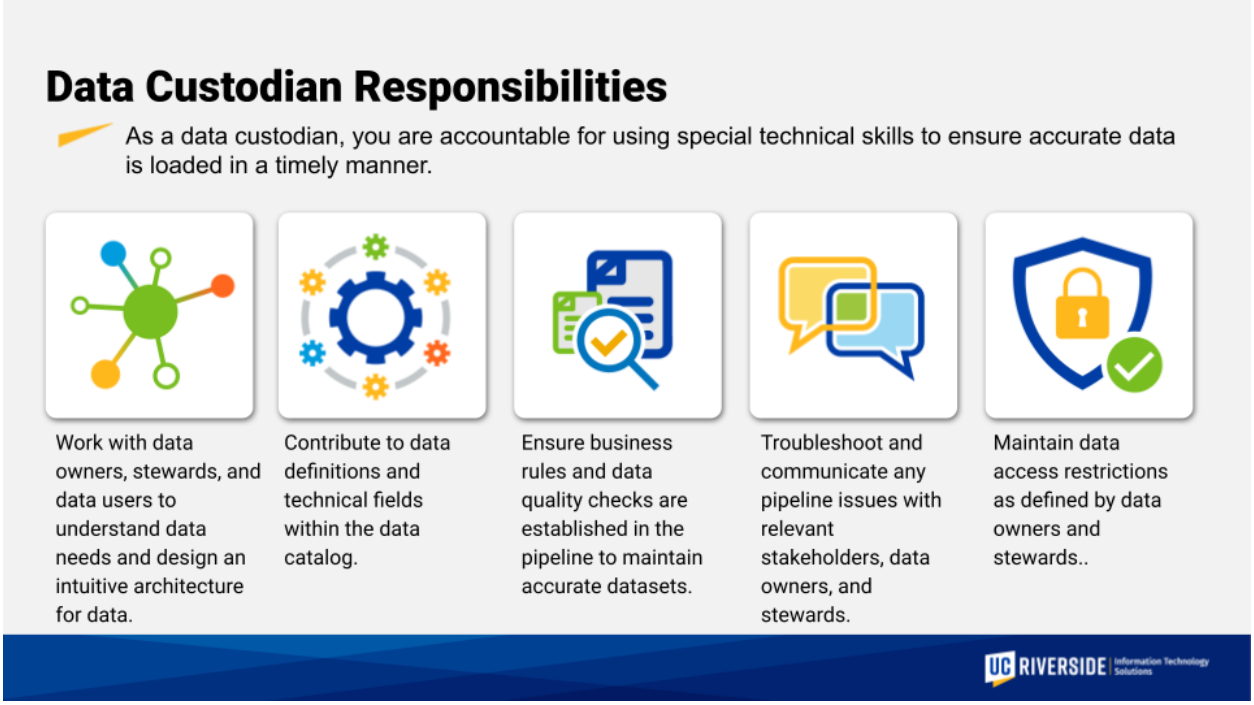
- Define dataset access permissions based on user roles available, working to define roles based on job codes or job responsibility alignment for ease of maintenance of permissions.
- Review, approve, or deny exception-based access requests that fall outside of the standard role-level permissions.
- Define data quality and business rules for the data.
- Correct any errors or inconsistencies in the data in a timely manner.
- Communicate concerns, issues, or problems with data to appropriate channels, such as data governance committee, data owners, ITS, or other relevant stakeholders.
- Set data retention timelines. Approve or deny data destruction recommendations from the Data Custodian.
- Review and approve the use of their data in Institutional Data Products, including AI products, to ensure compliance with data quality, privacy, ethics, and use standards.

Data Custodian

A Data Custodian is accountable for using special technical skills to ensure data access permissions are maintained, data is secure, and that accurate data is available in a timely manner.

- Maintain data access restrictions as defined by data owners and stewards.
- Work with data owners, stewards, and data users to understand data needs and design an intuitive architecture for data.
- Contribute to data definitions and technical fields within the data catalog.
- Document all data pipelines and integrations to or from the data source.

- Ensure business rules and data quality checks are established to maintain accurate datasets.
- Troubleshoot and communicate any pipeline issues with relevant stakeholders, data owners, and stewards.
- Recommend data for destruction when its retention period has expired.
- Perform the data destruction on all relevant data sources.



Data Consumer

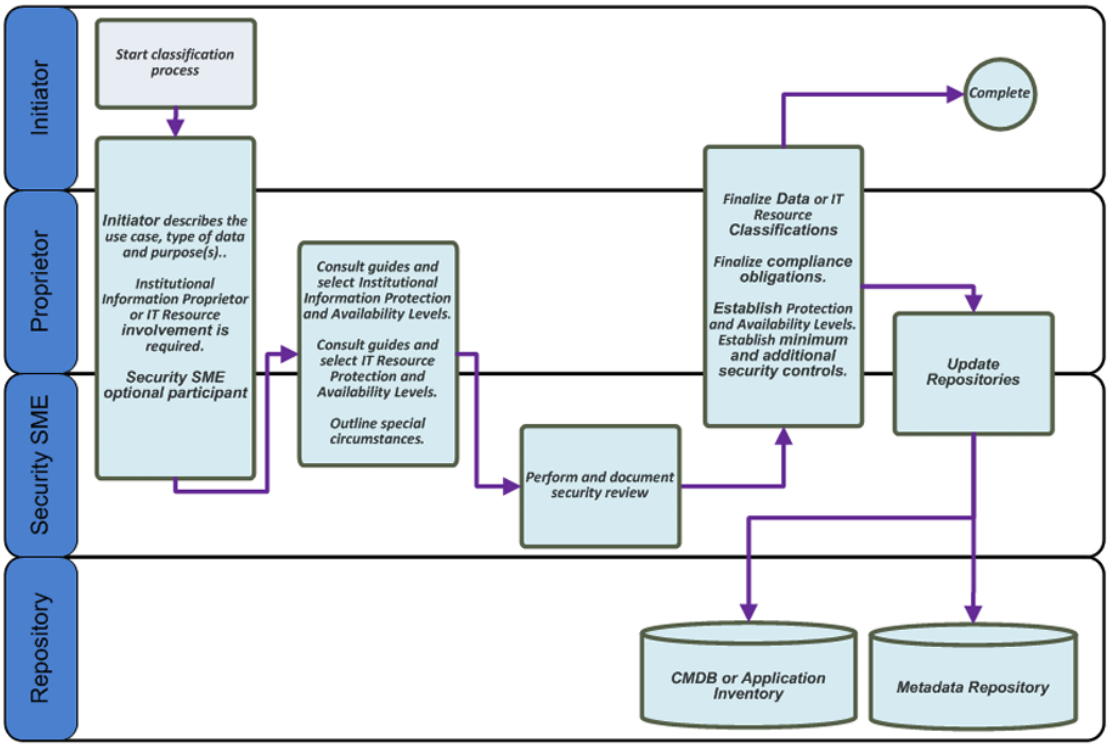
A Data Consumer is someone who has access to institutional data for operational, analytical, research, or other purposes.

- Comply with all access, privacy, and security policies defined by Data Owners and Stewards.
- Seek to understand the definitions, metadata, and "source of truth" for data to ensure accurate interpretation and reporting.
- Promptly notify Data Stewards of any suspected data quality issues, anomalies, or security breaches.
- Ensure that any derived reports, visualizations, or redistributed datasets maintain the same level of protection as the source data.
- Perform secure data destruction on local copies or temporary storage once the specific business purpose is fulfilled.

II. Data Classification

- Systems or applications level
  - Stewards and custodians are required to classify data systems using classifications defined by UCOP
  - P4 - High, P3 - Moderate, P2 - Low, P1 - Minimal
- Data fields in systems or applications level
  - Sensitive data fields need to be classified using the same classification definitions

Classifying Institutional Information and IT Resources



III. Data Privacy

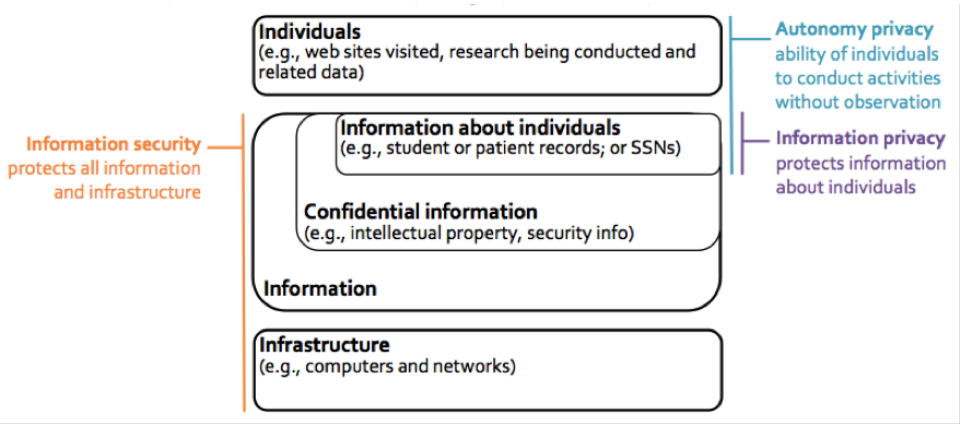
All individuals have a responsibility to protect the privacy of our institutional data as required, and to manage it appropriately throughout the whole data lifecycle. The ITS Data Governance Advisory Board provides a forum for Data Owners and campus representatives to pursue strategies to balance institutional data availability with privacy, compliance, and security.

Data collected from individuals must follow all applicable data privacy laws and UC and UCR policies, procedures, and standards.

As defined by the University of California Privacy and Information Security Initiative:

- Autonomy privacy: An individual's ability to conduct activities without concern of or actual observation.

- Information privacy: The appropriate protection, use, and dissemination of information about individuals.
- Information security: The protection of information resources from unauthorized access, which could compromise their confidentiality, integrity, and availability.



IV. Data Access and Review

This standard establishes the principles and processes for granting, managing, reviewing, and revoking access to UCR's institutional data through any tool, including AI products, ensuring its protection, confidentiality, integrity, and availability.

Authorization Principles and Decision-Making

- **Role-Based Access is the Default:** Access to data and systems will be standardized according to a user's defined role and job function. This approach ensures consistent access permissions for all individuals within a specific role, significantly streamlining the new employee onboarding process and reducing time-to-productivity.
- **Exception-Based Access:** Any requests for access that fall outside of the defined role-based standards must be justified and will be processed according to decision criteria and approval workflow.
- **Access Management Tool:** All exception-based data access authorization requests must be formally submitted and comprehensively documented through a designated and approved access management tool (e.g., ServiceNow, identity and access management system).
- **Stewardship Authority:** The Data Steward of the requested data domain is the authoritative decision-maker for granting or denying access. The Data Steward may grant designees to review data requests on their behalf.
- **Least Privilege:** Authorization for access will be based on the principle of "least privilege," granting access only to the minimum necessary data fields, functions, and classification levels (e.g., P3, P4 data) required to fulfill the clearly defined business need.
- **Exception-Based Access Decision Criteria:** Authorization decisions are primarily based on:

    - The institutional data risk classification of the data requested (P1-P4).
    - The clearly articulated stated business purpose justifying the need for access.
    - Compliance with all applicable UCR policies, federal, state, and local laws, including FERPA, HIPAA, and other privacy regulations. This review is critical for all requests, especially external.

  Data requests will be evaluated to ensure they are in the best interest of UCR, protecting its reputation, assets, and the privacy and security of its constituents (students, faculty, staff, patients, etc.). Consideration will also be given to (1) the value versus time and effort to collect the data and (2) the ethical implications of the data use, potential for misuse, and alignment with UCR's mission and values.

- **Restriction on Export of Data to Countries of Concern and Covered Persons:** To comply with the Department of Justice's Bulk Data Rule, implementing Executive Order 14117, data shall not be released to entities organized in or individuals residing in countries of concern, or other entities meeting the definition of "Covered Persons" under the Rule. Countries of concern currently are the People's Republic of China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela. In addition, persons receiving data may be required to attest that they will not transfer the data to Covered Persons.
- **Additional Approvals for Sensitive Data:** For internal requests involving sensitive (P3) or restricted (P4) data classifications, mandatory approval from the requester's direct supervisor is required, in addition to the Data Steward's decision, with optional consultation with the Data Owner.
- **Acknowledgement of Responsibilities:** Prior to gaining access to sensitive or restricted data, all authorized individuals must formally acknowledge and agree to adhere to the responsibilities and obligations associated with handling such data, as defined by UCR policies and relevant regulations.

Appeals Process

- Decisions regarding data access authorization may be appealed directly to the **Data Owner** of the relevant data domain. Appeals of the Data Owner's decision may be escalated to the **Data Governance Advisory Board**. The Advisory Board's decision is final.

User Responsibilities and Training

- **Adherence to Policy:** Authorized users are responsible for strict adherence to all UCR data governance policies, including those pertaining to data use, security, privacy, and confidentiality.
- **Prohibition on Unauthorized Data Sharing:** Users granted access to institutional data are strictly prohibited from sharing that data with any other individual or entity (whether within UCR or external), or publishing publicly or within the UCR network, unless explicitly authorized by the Data Steward for the specific dataset in question and

documented through the proper access request channels. Data sharing restrictions apply to the data in any format, even when summarized or calculated in a manner that the data was not initially received.
- **Mandatory Training: Required training** on data privacy, security awareness, and specific data handling and sharing protocols may be a prerequisite for initial authorization and may be required periodically to maintain access to certain institutional datasets.
- **Reporting Misuse:** Authorized users have a responsibility to promptly report any suspected or actual misuse, unauthorized access, or breach of UCR data to the UCR Campus Privacy Officer.

Access Review and Revocation

- **Periodic Review:** Authorizations for access to **sensitive (P3) and restricted (P4) data** will be formally reviewed by the respective Data Steward on a **yearly basis** to ensure ongoing business need and compliance. Reviews for less sensitive data will occur as deemed appropriate by the Data Steward or UCR policy.
- **Data Steward-Initiated Termination:** A Data Steward retains the explicit right to **immediately terminate access** to a dataset or data feed at any time, without prior notice, if concerns arise regarding data misuse, security risks, policy violations, or a change in institutional best interest.
    - Upon termination, an **ITS ticket must be filed promptly** to revoke technical access.
    - The Data Steward may also **mandate the deletion of any UCR data saved locally** by the terminated party and require certification of such deletion.
- **Timely Revocation:** Authorization to institutional data **must be terminated in a timely manner** upon an individual's separation from the university (e.g., resignation, termination, retirement) or upon a significant change in job responsibilities that no longer requires the granted data access. This process should be automated where feasible.

Shared Accounts and Service Accounts

- **Prohibition of Shared Accounts:** The use of generic or shared user accounts for accessing sensitive (P3 & P4) institutional data is **strictly prohibited**, except where explicit, documented, and highly controlled exceptions are approved by the Data Owner and Information Security. These exceptions will be reviewed by the Information Security Office annually.
- **Service Account Management:** Service accounts utilized for automated data access or system-to-system integrations must be:
    - Justified by a clear business purpose.
    - Managed with the principle of least privilege.
    - Documented with their specific access rights and associated systems.
    - Subject to regular review and password rotation in accordance with UCR's IT Security policies.

    - Owned and overseen by a designated UCR department or individual responsible for its security and use.

Documentation and Auditability

- All data access requests, authorization decisions, associated agreements, reviews, and revocations will be thoroughly **documented and maintained** within the designated access management tool. This documentation will serve as a complete audit trail.
- The Data Governance Advisory Board will conduct an annual review of a sample of access requests and provisioned access to ensure its protection, confidentiality, integrity, and availability.

Research Data Requests

The standards established by the Research and Economic Development Office apply to data requests from researchers, either internal to UCR or external.

1. Researcher fills out Unfunded Agreement Request
2. Researcher submits IRB Application
3. IRB reviews and approves/denies research
4. Researcher signs Data Security Agreement
5. Researcher submits Data Request

External Data Requests

These standards apply to all requests for UCR data originating from parties external to the University of California, Riverside, including public record requests, vendors, individual researchers, external organizations, or government entities. This does not apply to a student's request for their own data or the exceptions listed below. All provisions within the 'Data Access and Review' section above apply to external data access requests, except where explicitly modified or augmented by the specific requirements outlined in this section.

Exceptions to this are for:

- UCOP, audit, or benchmarking requests, which will come through the Data Steward directly, or the Unfunded Agreement Request through the Research, Innovation, and Economic Development Office (RED).
- Requests from federal or state regulatory agencies conducting reviews, audits or investigations of UCR, such as the EEOC, U.S. Department of Education, U.S. Department of Justice, California Civil Rights Department, U.S. Department of Health & Human Services, which typically will be handled or coordinated by the Chief Compliance Office or the Office of Legal Affairs. Additionally, financial audits and reviews coordinated by UCR's Accounting: Internal Revenue Service (IRS), US Department of Agriculture, US Department of Energy, etc., California Franchise Tax Board, California Department

California Department of Tax and Fee Administration, and Agency Research sponsors for Contracts and Grants administration, and UC hired external audtiors.
- Requests under the California Higher Education Employer-Employee Relations Act (HEERA), which are handled by Central Human Resources.
- Data requests or disclosures as part of a claim, lawsuit/litigation, subpoena, or as required by state or federal law.

1. Formal Request Submission

- All external data requests need to be submitted through the UCR Records Request form.
- The request form must require clear articulation of the purpose of the data request, the specific data elements required, the intended use, and the duration of access.
- If a request comes to a UCR employee through another method, the requestor should be directed to this form or in the case of exceptions, the employee must submit a request to the UCR Records Request form on behalf of the requestor prior to processing the request.
- All external data requests must be documented through a designated, standardized formal channel.

2. Processing of External Data Requests

- An automated process will determine the sensitivity of the request and route the records request to the appropriate individual for review and processing.
- If solely P1 data, the legal team will fulfill the request.
- If P2 to P4 data and the requestor is a researcher, external grant evaluator, or institutional collaborator for research purposes, the request will be sent to the RED Office.
- If P2 to P4 data and not a use case specified above, the request will be sent to the Office of Data & Analytics who will then share with the appropriate Data Stewards.
    - For directory information requests, per FERPA 34 CFR Part 99, the requestor will be required to pay a fee before the request will be fulfilled.
    - A formal risk assessment will be conducted by the Data Steward or Designee for requests involving sensitive data or complex integrations to identify and mitigate potential vulnerabilities and threats.
- For ongoing audits or investigations, a single 'umbrella' entry may be submitted in the request management tool to document the scope of the audit and the responsible campus office, in lieu of documenting every individual data exchange occurring throughout the audit lifecycle. Any audit or investigation that carries a formal "Confidential" designation or legal privilege is excluded from this documentation process.

Standards for Non-Public External Data Access (P2-P4)

1. Data Use Agreements & Contracts

- A formal data use agreement is required for any non-public data (P2-P4) that will be shared outside of UCR.
    - For vendors: Appendix DS (third party with procurement contracts)
    - For other parties: Data Use Agreements
    - For researchers: Data Security Agreement (sensitive data)
- The data use agreement will specify:
    - Permitted uses and users of the data. Use is restricted solely to the purpose stated in the request.
    - No sharing of the data other than intent specified.
    - Must follow UCR's encryption standards.
    - Data destruction requirements upon completion of the project or expiration of the agreement.
    - UCR's audit rights to ensure compliance.
    - Incident response procedures in case of a data breach.
    - Indemnification clause.

2. Security and Encryption Standards

- External requestors must explicitly agree to and demonstrate adherence to UCR's mandated security and encryption standards for all data received, stored, and transmitted. This includes:
    - Data encryption at rest and in transit, commensurate with the data's P-level classification.
    - Use of secure data transfer protocols (e.g., SFTP, secure APIs, secure cloud environments).
    - Implementation of robust access controls within the requestor's environment.
    - Regular security audits and vulnerability assessments, as required by the Data Use Agreement.

3. Data Retention, Termination of Access, and Destruction of Data

- The Data Use Agreement will specify a clear retention period for the data. Upon expiration or completion of the project, the external party must certify the secure destruction of all UCR data received.
- A Data Steward retains the right to terminate a data integration to an external entity at any time if deemed necessary to protect UCR's interests, ensure compliance, or respond to changing circumstances or identified risks.

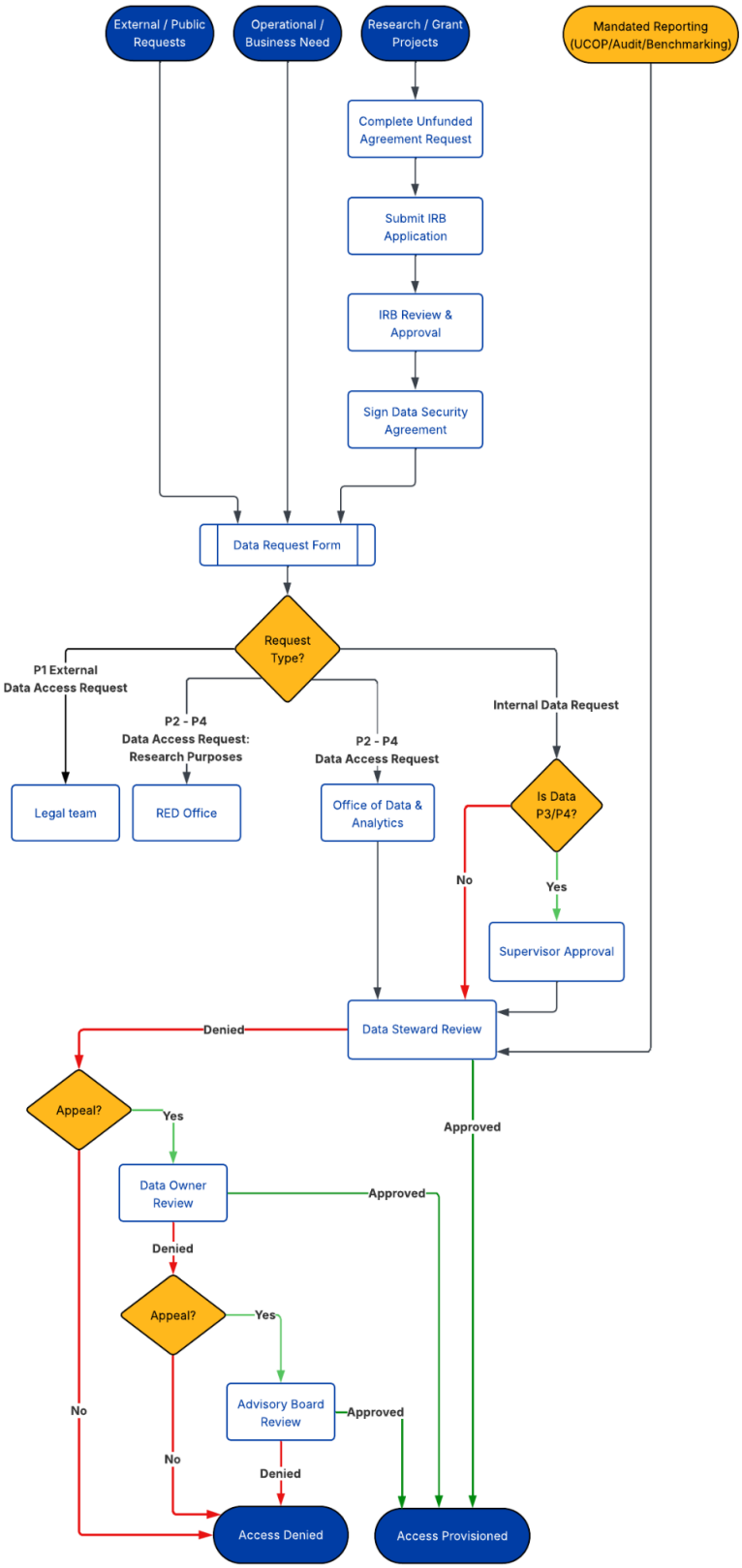
4. Logging and Audit Trail

- All external data requests, approvals, denials, and data provisioning actions will be thoroughly logged and maintained as part of an auditable trail.
- For ongoing integrations, periodic reviews and audits of the external party's compliance will be conducted.

5. Incident Response

- External parties must agree to immediately notify UCR in the event of a suspected or actual data breach involving UCR data and cooperate fully with UCR's incident response procedures.

Data Access Flow



V. Data Documentation

Data Stewards and Data Custodians are required to provide data documentation in the data catalog tool. Data Consumers must confirm that they are using the correct source of truth and following acceptable uses defined for the dataset within the data catalog.

- Definitions
    - Institutional data product - A dashboard, report, or visualization that is published for widespread use across campus as a trusted, validated, and approved data product
    - Dataset - A collection of data, typically for one area of the campus, a role within the campus, or for a data domain
    - Data element - one part of a dataset and often synonymous with a data field
- Data element documentation required
    - Name
    - Long name
    - Format
    - Description
    - Domain
    - Example data
    - Acceptable uses
- Dataset documentation required
    - Name
    - Type (table, view, API, etc.)
    - Description
    - Load frequency & schedule
    - Risk classification
    - Domain
    - Dataset platform
    - Physical name
    - Data owner & steward
    - Source information
    - Primary key
    - Data retention schedule
    - Acceptable uses
- Institutional data product documentation required
    - Name
    - Description
    - Audience
    - Load frequency & schedule
    - Risk classification
    - Domain(s)
    - Data owner & steward
    - Development team

- Platform & link
- Lineage & calculations (optional)

VI. Data Definition Approval Process

- Institutional data elements will be documented and communicated to ensure transparency, clarity, consistency, shared understanding, ease of use, and replicability.
- Data custodians and data stewards will contribute to the data definition process. The data steward will review proposed definitions for accuracy. They will ensure that the pending definition sufficiently avoids overlap with existing terms, even in other data domains. Once accepted by the data steward, the definition will be published in the data catalog.
- Data definitions are available for open review and comment by the broader institutional data community. Comments will be reviewed by the advisory board and brought to the appropriate data owner for resolution.
- Changes to data definitions will be communicated with relevant stakeholders.

VII. Data Quality

Data quality is the foundation of effective data governance and is absolutely critical for establishing trust in data. Without high-quality data—meaning data that is accurate, complete, consistent, timely, and valid—governance is undermined, and decisions become unreliable. Critically, data quality impacts *every step* of the data lifecycle: from its initial capture in transactional/operational systems to its refinement for analytics and its consumption by AI/Machine Learning models. To ensure this trust, robust data quality checks—such as completeness validation, format consistency, referential integrity, and timeliness verification—must be rigorously performed and enforced across the pipeline. Poor quality at any point cascades downstream, leading to flawed insights, compliance risks, and a loss of stakeholder confidence. Therefore, a core function of data governance is to implement and enforce the standards necessary to ensure reliable, trustworthy data throughout the entire data ecosystem.

- Data stewards will be encouraged to define quality checks that should be performed against their data sets. Data custodians should provide reporting to data stewards to see the outcomes of the checks.
- Any issues raised through automatic data quality checks will be sent to the data steward. Preference for resolution of data quality issues will be to resolve the issue within the transactional or source system. Occasionally, a transformation to resolve an issue may be done in the pipeline to the data warehouse but this is not preferred because it could lead to discrepancies between the source system and the data warehouse.
- Any data consumer who discovers a data quality issue should report it through Service Now to the data team. The data team will work with the data steward to identify the root cause and prioritize the resolution of the issue.

VIII. Data Integration

These standards govern the secure, compliant, and effective integration of institutional data (P2-P4) across UCR systems (including custom applications, third-party hosted applications, and AI products and systems) and with external entities. An integration is defined as data moving between systems on a regular or recurring basis. A one-time data share or audit request is not considered an integration for these purposes.

- **Purpose-Driven Integrations:**
  - All data integrations must serve approved business purposes that align with UCR's strategic objectives and operational needs.
  - Any new or significantly modified use of an existing integration requires additional review and approval, ensuring its continued alignment with institutional goals and data governance principles.
- **Authoritative Data Sourcing:**
  - Data integrations for institutional data products must primarily source data from official systems of record (SORs) or the enterprise data warehouse. This approach minimizes unnecessary data duplication, reduces storage overhead, and ensures consistency and accuracy across UCR.
  - All integrations will adhere to established university data standards for format, quality, and naming conventions.
- **Data Stewardship Authority:**
  - For integrations between UCR systems, the Data Steward of the originating data system retains stewardship for that data throughout its lifecycle, regardless of where the data resides downstream.
  - Stewardship does not transfer to a receiving system simply because data is replicated or integrated there. The Data Steward of a downstream system cannot unilaterally determine access or other governing policies for data originating from another system. Their role is to manage and utilize the data within the parameters set by the originating Data Steward.
- **External Integration Requirements:**
  - Any data integration involving an external software system or third-party entity must strictly adhere to UCR's "External Data Access Request Standards" (as outlined above).
  - This includes, but is not limited to, requirements for data classification, legal agreements (e.g., DUAs), security protocols, and data destruction.
  - The appropriate Data Steward(s) must approve any data integration to external parties, as defined in the “External Data Access Request Standards.”
- **Security Vetting for External Integrations:**
  - Prior to establishing any new data integration with an external, non-UCR source, a mandatory Information Security Consultation must be conducted by the Information Security Office. This consultation is critical to thoroughly vet the external system's security posture, ensuring it meets UCR's standards for data protection, encryption, and appropriate data sharing practices.

- **Documentation and Transparency:**
    - All data integrations, whether internal or external, will be comprehensively documented within a centralized repository.
    - This documentation will be readily available for Data Steward visibility and include details such as data flow, purpose, data elements involved, security controls, and associated agreements.
- **Standardized Request Process:**
    - Requests for new data integrations (both internal and external) must be initiated through the designated institutional request system, such as ServiceNow. This ensures a standardized intake process, proper routing for approvals, and a clear audit trail.

IX. Institutional Data Products

This standard establishes the requirements for the creation, validation, publication, and lifecycle management of Institutional Data Products at the University of California, Riverside. It ensures that all official data products are accurate, consistent, secure, and contribute effectively to UCR's decision-making and operational excellence.

Definition and Purpose

An Institutional Data Product is any application, report, dashboard, visualization, data extract, analytic model, AI/machine learning model, data science, skill, agent, or other structured data output that:

- Derives from UCR's official systems of record (SORs) or the enterprise data warehouse.
- Is designed for widespread, recurring use. Typically has a method of data integration involved to refresh the data.
- Is used for official university business, strategic decision-making, operational management, or external reporting.
- Is intended for recurring use or broad dissemination across departments, to external entities, or for public consumption.
- Contain data that are formally governed by an assigned Data Steward.

An Institutional Data Product is not:

- A one-time data share or audit request.
- A document, written report, or presentation file not intended for recurring use or broad dissemination across departments, to external entities, or for public consumption.

For the purpose of this standard, a data product is considered "published" when it is shared with or made accessible to any individual or entity beyond its immediate creator(s), regardless of the method of dissemination (e.g., direct email, shared drive, web portal, system integration).

The purpose of this standard is to ensure that all UCR Institutional Data Products are reliable, secure, and consistently presented, serving as trusted sources of information for the UCR community and authorized external parties.

Publication Requirements for Non-Public Data

- **Mandatory Use of Approved Tools:** Any Institutional Data Product containing non-public data (classified as P2, P3, or P4) must be published and disseminated solely through UCR ITS-supported and approved tools or platforms.
- **Safeguarding Data:** These approved tools are specifically selected and configured to:
    - Restrict access to appropriate individuals based on the "need-to-know" principle and UCR's Data Access and Review Standard.
    - Safeguard the data through technical controls such as encryption, robust authentication, and access logging.
    - Ensure compliance with UCR's security policies and all applicable legal and regulatory requirements (e.g., FERPA, HIPAA).

Publisher Responsibilities

Individuals or teams creating and intending to publish Institutional Data Products are responsible for adhering to the following:

- **Policy Compliance:** Comply with all relevant UCR data governance policies and standards, including Data Classification, Data Access and Review, and Data Integration standards.
- **Approved Publication Channels:** Ensure the data product is published exclusively through a UCR ITS-approved tool or platform that meets the requirements outlined in Section 2 above. Any platform hosting P2-P4 data must be reviewed and approved by the ITS Security team.
- **Access Control (Need-to-Know):** For data products containing sensitive (P3) and restricted (P4/P5) data, publishers must implement and verify stringent access controls within the publishing tool to ensure that access is granted strictly on a "need-to-know" basis, in accordance with the Data Steward's authorization. Auditing of access must be tracked for compliance purposes.
- **Data Catalog Documentation:** Prior to publication, the author/publisher must accurately input and maintain all required metadata about the data product within the designated UCR Data Catalog. This includes, but is not limited to:
    - A clear and concise description of the data product's purpose and content.
    - Identification of the primary audience for the data product.
    - Mapping to data fields present in the Data Catalog, explicitly linking the product's elements to their authoritative definitions.
    - Detailed descriptions of calculations or derivations not already defined in the Data Catalog.

    - Information on the data source(s), data refresh frequency, ownership, and IS-3 Availability Level (optional).

Certification of Institutional Data Products

- **Certified Status:** A Data Steward or Designee may officially label an Institutional Data Product as "Certified" after a thorough review and vetting process ensuring that each of the Data Product Standards listed below are met.
- **Meaning of Certification:** A "Certified" data product is considered:
    - **Trusted:** It has been formally validated by the Data Steward as an accurate, reliable, and authoritative use of the underlying data.
    - **Accurate:** Its data sources, methodologies, and calculations have been verified for correctness and consistency with official UCR data definitions.
    - **Governed:** It fully complies with all UCR data governance policies and standards, including security, privacy, and quality.
- **Benefits of Certification:** Certified products will be prominently identified within UCR's data catalog and reporting environments, signifying their status as the preferred and most reliable sources for official decision-making and reporting.

Data Product Standards

All Institutional Data Products must adhere to the following standards:

- **Data Quality:** Data presented must be accurate, complete, timely, and consistent with the underlying source data. Any data quality limitations should be clearly noted.
- **Data Definitions and Consistency:** All metrics, dimensions, and data elements used must align with UCR's official data definitions as documented in the UCR Data Catalog.
- **Security and Privacy:** Strict adherence to UCR's Data Classification Policy and Data Access and Review Standard, ensuring appropriate safeguarding, de-identification, or aggregation for sensitive data.
- **Presentation and Usability:**
    - **Clarity and Readability:** Products should be easy to understand, navigate, and interpret.
    - **Consistency:** Adhere to UCR's visual branding guidelines and internal presentation best practices for charts, graphs, and layout.
    - **Context:** Include necessary titles, labels, legends, and explanatory text to provide context and prevent misinterpretation.
    - **Actionable Insights:** Designed to support informed decision-making by presenting data in a meaningful and relevant way.
- **Accessibility:** Products must conform to UCR's digital accessibility standards (e.g., WCAG 2.1 AA) to ensure usability for all individuals.
- **Performance:** Products should be designed to load and operate efficiently, providing timely access to information without undue delays.

- **Change Management:** All significant changes to a published data product (e.g., data sources, methodologies, calculations, audience) must follow a documented change management process, which may require re-approval from the Data Steward.
- **Lifecycle Management:** Institutional Data Products must have a defined lifecycle, including procedures for periodic review, updates, and eventual decommissioning or archiving when no longer needed or accurate. Data retention schedules and the retention standards below apply to institutional data products.

Data Product Review and Depublication

- The Data Steward(s) and Data Owner(s) of the source dataset(s) have the right to request the de-publication of any Institutional Data Product that does not align with their standards for compliance, privacy, ethics, or appropriate use of the data. Upon such a request, the data product must be taken offline until the identified issues are remediated to the satisfaction of the Data Steward and/or Data Owner.

X. Data Retention

Data retention schedules are a critical component of sound data governance, establishing mandatory timeframes for how long specific types of data must be kept and when they must be securely disposed of. Their primary importance lies in risk mitigation. Retaining data—especially personally identifiable information (PII) or sensitive corporate records—longer than legally or operationally required significantly increases the organization's exposure across multiple fronts. Shorter retention periods could increase compliance risk.

- **Cybersecurity Risk:** Excessive data retention directly expands the organization's attack surface. Each obsolete or unnecessary record kept is an additional liability that must be defended. Old, unclassified data often resides in legacy systems or forgotten locations, making it a prime, high-value target for cybercriminals seeking PII, financial data, or intellectual property. The secure, timely disposal of redundant data is thus a proactive and essential step in minimizing the potential scope and impact of a data breach. For further guidance, please review both Security: Data Lifecycle Management: Retention and Sanitization and Security: Data Lifecycle Management: Protection
- **Regulatory Risk:** Prolonged retention can lead to non-compliance with data privacy laws, attracting substantial fines and damaging public trust. Our institution is specifically governed by requirements like the Family Educational Rights and Privacy Act (FERPA), and may also be subject to HIPAA for health records, GLBA for financial information, and global or state laws like GDPR and CCPA depending on the individuals whose data we process.
- **Legal Risk:** Excess data acts as an organizational liability, significantly expanding the scope and cost of e-discovery in litigation and increasing the potential for adverse findings.

Therefore, a strict, enforced data retention schedule, coupled with a commitment to minimizing data proliferation, is essential for minimizing the data footprint, ensuring compliance, and actively reducing the organizational risk profile associated with data ownership.

Data Retention Schedules

- Data Stewards are required to document a data retention period for each dataset within the Data Catalog.
- Data retention periods must follow UCOP guidelines for data retention schedules as specified in the UC RMP-1 University Record Management Policies.
- Data Stewards should determine how long the data is needed for business operations, analysis, and historical reporting. This includes specifying a period for active use (e.g. for student support) and a period for archival use (e.g. for historical research or trend analysis). This helps prevent the unnecessary long-term storage of data that no longer provides value, reducing storage costs and complexity.
- All Data Steward defined retention periods for a data set that go beyond the UCOP defined retention schedule will be treated as a Cybersecurity Exemption. The request must follow the normal CISO Security Exemption process.

Data Destruction and Disposal

- When a dataset's retention period has expired, it must be securely disposed of. The Data Custodian is responsible for performing the data destruction according to the schedule set by the Data Steward. The Custodian will recommend data for destruction, the Data Steward will approve, then the Custodian will perform the destruction on all relevant data sources.
- Data destruction may need to happen in transactional (or source) data systems, integrations, and in the data warehouse.
- The data destruction method must be appropriate for the data's sensitivity. For example, sensitive data may require secure overwriting or cryptographic shedding, while non-sensitive data may be handled with standard deletion.
- When data is destructed or disposed of, a destruction log should be maintained, documenting when data was destroyed, by whom, and using what method, for auditing purposes.

XI. Best Practices for Data Consumers

Recognize that you are responsible for the security and compliance of any institutional data you choose to store on your device.

Minimize Local Data Footprint

The most secure way to manage sensitive data, including FERPA data, is to avoid storing it locally whenever possible.

Best Practice	Description
Data Minimization	Critically evaluate if you truly need the full, sensitive dataset on your local device. If a summary, aggregate, or truncated set of data will suffice for your work, use that instead.
De-Identification First	When feasible, proactively de-identify or remove sensitive fields (e.g., PII) before downloading data for analysis, testing, or reporting.
Use Approved Network Storage	Favor storing active, non-de-identified data on approved, secure network drives or cloud services over your local hard drive.
No Sensitive Data on Personal Devices	Avoid storing P3 or P4 organizational data on personal or non-managed devices.

Protect Data at Rest

Data stored on your device should be protected by layers of security, primarily through encryption.

Best Practice	Description
Encrypt Your Device	Ensure your entire hard drive utilizes Full Disk Encryption (FDE) (e.g., BitLocker, FileVault). This is the best defense against data theft if your device is lost. If you do not encrypt your entire hard drive, at a minimum, encrypt files with institutional non-public data (P2-P4).
Encrypt Removable Media	When using external hard drives or USB sticks for organizational data, always use encryption on that media.

Data Cleanup and Lifecycle Management

Proactive cleanup of unnecessary files is essential to reduce risk exposure.

Best Practice	Description

Prompt Disposal	Delete data as soon as you are done with it. Storing it "just in case" creates unnecessary risk.
Adhere to Retention Schedules	If data must be kept either locally, on a network drive, cloud storage, or in a database not maintained by ITS, familiarize yourself with the UCOP Data Retention Schedule and delete the data when the required time period is met and the data qualifies for destruction.
Ensure Secure Deletion	Regularly empty your Recycle Bin or Trash to finalize the disposal of unencrypted files. Deleting files without emptying the trash leaves them recoverable.

XII. Approval, Amendment and Revision History

This standards document was issued [____], 2026. It is a living framework managed by the Data Governance Advisory Board. The Advisory Board will conduct a formal review of these procedures and standards on a 12-month cadence to ensure continuous alignment with systemwide UC policies, evolving data privacy regulations, and institutional needs. Any amendments or revisions approved during this annual review will be documented in the version control history and communicated to campus stakeholders.