IRIS New Member Onboarding

We are delighted that your institution is considering IRIS membership! IRIS is a national source of credible data and rigorous findings about the productivity and public value of higher education. For more information, please visit our website: iris.isr.umich.edu.

This new member onboarding packet is intended to help your institution think through common questions and issues about IRIS membership. It will streamline and facilitate the process of becoming an IRIS member by identifying more clearly how to engage in the process and how to identify the key individuals on your campus and at IRIS who are central to making membership successful. Our goal is to add value and reduce burden to our member institutions.

After several years of bringing new members into IRIS we believe we have learned a few things that may be of help to you. To make the most of your IRIS membership, we strongly recommend designating a champion on your campus who can bring the right people together and who will also disseminate the reports you will receive from IRIS to the appropriate units. To get started, that person should identify and convene key stakeholders who are responsible for the relevant datasets. The IRIS Managing Director and Technical Director will schedule a conference call with this group to discuss process and technical questions in preparation for the first data submission.

IRIS INSTITUTE FOR RESEARCH ON INNOVATION & SCIENCE

Common questions related to IRIS membership

The following topics seem to come up with some regularity for institutions considering IRIS membership. This document addresses these questions and provides contact information for IRIS staff who can provide more information and answer your questions. You may have questions we haven't yet considered, so please reach out to us if that is the case.

- Cost and details of membership
- Institutional capacity to manage data transmission to IRIS
- FERPA
- Private universities and FOIA
- How to effectively utilize IRIS data products
- Protection of privacy and confidentiality
- Data security

Cost and Details of Membership

Membership for a single institution (or for a university system that provides a single data stream) is $25,000 per year. This fee covers the infrastructure costs at IRIS, which include staff salaries, new data product development, computer software and hardware, overhead, and the like.

Please note: A significant benefit of IRIS membership is that researchers on your campus will have free access to the de-identified IRIS dataset that is released each year for research, a value of $1,250 per person per year. For more information about research using IRIS data, see iris.isr.umich.edu/research-data/. Be sure to alert the researchers on your campus of this opportunity.

The membership period is August – July, so if your institution signs an IRIS Member Agreement after August, we prorate the fees for the first year as described in the Agreement. The following August, your institution will be billed for the coming year. Each contract thus covers the first, prorated year, plus three additional years and is renewable.

Once you have reviewed the Agreement with your Office of General Counsel (or the appropriate legal/contract representative on your campus), send your signed or redlined Agreement to Nancy Calvin-Naylor (nbirk@umich.edu) and Karen Woollams (woollams@umich.edu).

Once the Agreement has been submitted to IRIS, the IRIS managing director will contact the person you designate as the decision-maker to talk with you about getting started. We strongly recommend you convene a group of key stakeholders who are responsible for the relevant datasets. The managing director and technical director will schedule a call with your team to discuss process and technical questions in preparation for the initial submission of data.

When the Agreement is fully executed, your membership period will begin, and we will initiate the process by sending an invoice to the person you designate to handle payment.

Data transmission to IRIS

The task of compiling and transmitting administrative data from your HR, procurement, and research systems may feel daunting. Some institutions have systems operating on very different platforms and are challenged at the thought of integrating disparate data sets, while others express concern about having to commit significant resources to compiling data.

At IRIS, we have worked with institutions that are quite diverse in how they manage data and we will walk through all of these issues with your data point of contact. Our technical director, Kevin Bjorne, has an outstanding record of helping institutions manage this process effectively. Kevin estimates the initial data transmission may take about 40 hours of institutional effort, and considerably less time for subsequent data transmissions. For institutions that participated in the federal STARMETRICS program this time can be much reduced by adapting existing scripts, as IRIS data are based on STARMETRICS data formats.

Questions about FERPA

Universities often ask us about FERPA. We leave the determination of whether your data are protected by FERPA up to you and your Office of General Counsel. If you decide your data are protected by FERPA, IRIS will protect them as outlined in the Member Agreement, consistent with FERPA requirements under the study exception.

Questions about FOIA

Private institutions often have concerns about FOIA. In 1994, the State of Michigan passed the Confidential Research and Investment Information Act (CRIIA) to protect confidential research, intellectual property, and trade secret records maintained by any public university or college in Michigan. Under CRIIA, data provided to a public university in Michigan by a private external source may be withheld from disclosure if all the following conditions are met:

(a) The information is used exclusively for research, testing, evaluation, and related activities;

(b) The information is designated as confidential by the external source before or at the time it is received;

(c) The University has entered into an authorized agreement to keep the information confidential; and

(d) A document containing a general description of the information to be received under the confidentiality agreement, the term of the agreement, the name of the external entity with whom the agreement was made, and a general description of the nature of the intended use for the information, is recorded by the University within 20 regular working days after it is received.

The University of Michigan's General Counsel and FOIA Office have determined that your data submission meets the requirements for an exception to FOIA requests under CRIIA. Our Agreement specifies that all FOIA requests will be reviewed accordant to any applicable FOIA exceptions, including, to the extent the institution depositing data with IRIS is a private entity and the materials have been clearly designated as confidential, the Confidential Research and Investment Information Act (CRIIA).

Utilizing IRIS data products

Developing a plan to utilize reports and products derived from IRIS data will enable your institution to maximize its investment. Experience at other institutions has indicated that an active plan is required to ensure that these reports won't languish in someone's inbox. Most institutions find it useful to empower a team that meets regularly to manage its relationship with IRIS and to deploy IRIS products. IRIS maintains a Technical Advisory Group (TAG), and each member institution has an opportunity to participate in the governance of IRIS.

While there is no single correct way to use the data products generated by IRIS, we encourage institutions to share their successful approaches. Here are some examples from organizations that have benefited from IRIS data:

Internal uses:

- Acquire better understanding of suborganizational units (e.g., schools, colleges, institutes, etc.)
- Generate knowledge of how research funds are expended, e.g., what staff, what equipment, which vendors
- Understand movement of faculty, staff, and students supported by research funds and the networks they form, etc.
- Generate analytic decision-making tool for research management, e.g., growth areas, start-up resource requirements, staffing needs, graduate student program development, etc.

External uses:

- Tools for conversations with external stakeholders, e.g., legislators, boards of regents, donors, public, etc.
- Institutional promotion for development, recruitment, student admissions
- Benchmarking institutional growth and development

Working with your university's government relations office is often an excellent approach. Liaison with unit and institutional development officers is also useful, and your public relations office and speechwriters will want to have access to information to include in talks, institutional publications, press releases, and even in tweets about your campus.

From time to time, IRIS will share examples of successful use of IRIS data and products.

Protection of privacy and confidentiality at IRIS

IRIS is committed to the responsible use of restricted data. We do not share your identifiable data with anyone other than our partner, the Census Bureau, and IRIS Nodes (see IRIS Member Agreement for more details).

Once your data are sent to the Census Bureau and matches with their datasets have been made, results generated from matched data are rigorously screened by the Census Bureau in a process called "disclosure proofing." Disclosure proofing procedures are designed to prevent re-identification of an individual or organization from the reports you receive. Disclosure proofing of results from analyses of restricted Census data is required by federal law. Some specific details of the disclosure proofing process are also protected by law and cannot be shared. With that said, the disclosure process influences the reports you receive in several ways.

1. ***Individual Data.*** Information on individual employees can only be released if it is based on a sufficient number of cases to insure that no single person can be identified in the data. Low match rates combined with fine categories in some panels of your reports mean data points cannot be disclosed.
2. ***Vendor and Subaward Data.*** Information on business establishments can only be released when it is based on a large enough number of establishments and when the concentration rate is low. In the kinds of spending data we report, a concentration rate would be high if a small number of vendors accounted for a large percentage of spending in a particular category. Hypothetically, if your institution has a contract with an airline that means most travel expenses are charged to that vendor, then even if your employees use many airlines, we may not be able to disclose spending information because of high concentration rates. Spending in some NAICS codes cannot be reported because of these issues.
3. ***Secondary Disclosure and Implicit Samples.*** Effective disclosure proofing requires attention to the possibility that data in a single report, or data disclosed in more than one report can be used to infer information about individuals or organizations. For instance, if we were to issue an updated report that differed from the data in your prior reports by only one or two data points, comparing reports would allow you to identify information about those data points, compromising privacy and confidentiality.

We continue to work with our University partners and with the Census Bureau to produce the most detailed and valuable reports that conscientious attention to privacy and confidentiality concerns will allow.

Data security at IRIS

IRIS has a robust data management and security plan. The IRIS data infrastructure is managed centrally from within the Institute for Social Research (ISR) at the University of Michigan. The ISR is the world's largest academic social science survey and research organization. Established in 1949, ISR has a long history of gathering, managing, disseminating, and protecting valuable research data, including personally identifiable information.

The safeguarding and protections of data are based on a defense-in-depth architecture. Firewalls, secure remote application access platforms, and other boundary controls are implemented based on a risk-based approach that adheres to a least privilege access control model. Specific configuration controls are safeguarded on a strict "need-to-know" basis.

The IRIS client-server environment is protected from intrusions, malicious software, denial-of-service attacks, and insider misuse using a combination of administrative, physical, and technical controls. Access to server resources once inside the network is based on a role-based directory service architecture. Host-level security includes antivirus and malware protection software that is centrally managed to allow for rapid incident response. Access to all data storage and management systems is restricted to only 4 personnel.

All IRIS enterprise servers are located in separate, secured rooms with access limited to authorized administration staff. Server rooms are locked at all times with access restricted to only IT personnel utilizing electronic proximity access badges to gain entry. Licensed restricted-use dataset access is tightly controlled in accordance with security requirements. Access to the general systems is limited to IRIS employees. Visitors are accompanied by IRIS staff throughout their visit and not allowed access to the internal network.

In order to be a responsible trustee of contributed university data, the data are stored and accessed in a manner consistent with stakeholder concerns and follows evolving data management practices in the United States and within Data Management Association (DAMA International) standards, as well as relevant government regulations and laws (for example, the Family Educational Rights and Privacy Act, or FERPA).

A core aspect of IRIS is making de-identified data available for research purposes. There is a balance between protecting the privacy of stakeholders while also granting access to this information (all while abiding by legal guidelines). We use the four A's to meet these requirements: authenticate the user's source, understand what they're authorized to do, create an account and audit their activities.

Authorization

In allowing access for researchers, IRIS will weigh the merits of each research project and determine whether there is a valid need for access to the data. Each researcher will have an approved area of focus and his/her permissions will reflect defined, appropriate views of the data.

Access

Access to the full data repository is restricted to the participating NODE institutions, the Census Bureau, IRIS Technical Director, and ISR Data Security personnel. Access to the de-identified data set is restricted to qualified research individuals that have been vetted and approved through IRIS research data use application process. All individuals will be required to sign affidavits of non-disclosure before given access to the data. User access will be revoked upon termination of employment or at the end of the approved research timeframe. Additionally, research access will be reviewed every 90 days to determine if continued access is appropriate and necessary.

Access will be monitored to compile data about who is accessing information for compliance auditing, and to detect unusual or suspicious behavior. Confidential information will be more strictly monitored. The data are secured onsite within the IRIS enclave at the ISR facility on the University of Michigan campus.

Authentication

Each member has been effectively verified as being who they say they are.

Audit

Auditors must be independent of the data and/or the process involved. In addition to any external auditors required, we will provide internal auditing to keep quality standards high. Responsibilities include reporting on the "State of Data Security," by verifying that activities are in compliance with regulations, and comparing our procedures against best practices. Auditing is not a substitute for data security management; rather it is a support process that will occur regularly.

Destruction of Data Post-Project

Upon the date of expiration or termination of this Agreement, the parties mutually agree that Michigan shall, at Michigan's expense, remove any identifying elements from the Materials in Michigan's possession (the "De-identified Materials"). Michigan agrees to send a statement certifying the de-identification of the Materials to the Depositor within 30 days of their de-identification. Michigan agrees that no data from the Materials, or any parts thereof, except in the form of the De-identified Materials, shall be retained unless written authorization from Depositor for the retention of such files has been received and confirmed.

Let us know if you still have questions about data security. We're happy to share the IRIS Data Management Plan, the IRIS Business Continuity Plan, and the IRIS Incident Response Plan.

University Contacts

Communication is critical to making membership work. Knowing who to reach out to is very important.

Identify the name, title, and contact information of the following people at your institution:

- the **ultimate decision-maker** about whether to join IRIS. Also include contact information for an **assistant or chief of staff**
- the person who will be responsible for actually **transmitting your institution's data** to IRIS
- the person who will be responsible for **managing the payment** of IRIS invoices
- anyone else at your institution who should receive **communications and IRIS data products/reports**

Please complete the form at https://tinyurl.com/IRIScontacts

Still have questions?

Not a problem! We understand that you will want to learn as much as you can about the benefits of joining IRIS and how to maximize this investment. Feel free to contact us.

Jason Owen-Smith, Executive Director
jdos@umich.edu

Nancy Calvin-Naylor, Managing Director
nbirk@umich.edu

Kevin Bjorne, Technical Director
kbjorne@umich.edu

We are very much looking forward to working with your institution and welcome you to the IRIS family!