IRIS Data Management & Information Security Plan

Purpose of Document

This Data Management and Information Security Plan is a comprehensive statement of the various principles and procedures that the Institute for Research on Innovation and Science (IRIS) requires all staff, research partners, and projects to follow to maintain the security of IRIS and client data and information. The plan outlines a wide range of protections, security rules and responsibilities that establish the framework of data management and information security. IRIS is committed to protecting the confidentiality, integrity, and availability of information that is collected, processed, transmitted, stored, or disseminated for external contract work, grant research, and internal IRIS business. To support this IRIS follows all federal and other governmental and industry standard requirements in securing its data and information.

Contents

IRIS Information Security Plan

Introduction

This policy is designed to provide a framework for how IRIS can meet Federal, State, and industry information security requirements that apply as a result of project work or internal business requirements. Below is a list of the key laws, standards and regulations that impact how IRIS must secure data and information technology systems:

- Federal Information Security Management Act (FISMA)
- Family Educational Rights and Privacy Act (FERPA)

IRIS is part of the larger Institute for Social Research (ISR) on the University of Michigan, Ann Arbor campus. ISR is the world's largest academic social science survey and research organization. Established in 1949, ISR has a long history of gathering, managing, and disseminating valuable research data across a wide array of both public and private sector areas. As such, ISR provides a strong foundation for IRIS to build upon with robust and established internal organizations that directly benefit the mission of IRIS. With the involvement of ISR from inception and into the future the strength of IRIS is guaranteed to be a success for all participants.

ISR and IRIS also have a long history in supporting the data security requirements involving Personally Identifiable Information (PII) of project participants for multiple government as well as non-government organizations.

IRIS Enterprise Application/System Environment

The IRIS local area network (LAN), wide area network (WAN), and data infrastructure is managed centrally from within ISR, under the direction of IRIS personnel. Select ISR security and hardware personnel actively participate in the overall manage of the system.

The safeguarding and protections of project 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.

IRIS IT Web Hosting Services Application/System Environment

IRIS maintains a professional-grade web services hosting center that is supported by a team of ISR engineers monitoring the continuous operations of the network, including servers, security, and hosted applications. The IT Web Hosting Services group has a track record of securing sensitive data that meet a variety of client requirement that include websites and database servers that have undergone federal agency Security Authorization.

The ISR IT Web Hosting Services group employs a defense-in-depth approach utilizing four concentric layers of security to maintain access control to client data.

Layer 1: Enclaves

We identify and group systems that have similar protection requirements, increasing protection. We have multiple networks. Our internal security enclaves are based on the sensitivity of the information resources resident in each and the assessed threats to those resources.

Layer 2: Border Firewalls and Intrusion Prevention Systems

We use commercial-grade application-layer firewalls and intrusion prevention systems to manage access on the Internet perimeter and between intranet enclaves. The intrusion prevention systems can identify and block advanced hacking techniques before they reach the intended target.

Layer 3: Strong Authentication

Following the recommendations of the National Institute of Standards and Technology, IRIS requires a minimum of eight characters, using mixed cases plus a numeric or special character, for all passwords. User passwords are changed at least every 90 days, privileged access passwords more frequently.

IRIS has also implemented two factor authentication via the Duo security system. The two factor authentication system requires that all employees, researchers, and administrators use both a strong password and a smartphone based notification and authorization system to log in and access any IRIS infrastructure.

Layer 4: Configuration, Patch Management

The importance of effective configuration and patch management of all devices on our network is fundamental, from border routers to data center servers and networked devices. We enforce the concept of adopting “least-user privilege” policies to reduce the risk of users introducing security flaws, and we continually monitor the network for vulnerabilities.

Data Management Plan for the UMETRICS Projects at IRIS

UMETRICS Background

IRIS works with organizations to build a scientifically grounded conceptual and empirical framework that enables them to better describe and manage their scientific investments. IRIS work informs the regional, national and international debate on research measurement and accountability by describing research investments to better identify research strengths, gaps, and changes over time; by describing researcher activity to better identify promising and productive individuals and networks; and by describing the results of research to better document the results of science investments. This work is accomplished by using new open source tools and technologies to leverage and link existing data on scientific activities; by developing theoretically and empirically sensible measures to describe the links between science investments and scientific, economic and social results; and by working with national and international organizations to build an open community of practice.

IRIS implements these objectives through the development and enhancement of the UMETRICS program. This program provides data infrastructure for IRIS and external research partners to provide independent evidence of the results of public and private investments in research and training. The data submitted by contributing universities will be used in conjunction with data from other partners for statistical and research purposes to (1) conduct frontier analyses that estimate the economic and social returns to scientific discovery and training by using (2) new data and organizational infrastructure to support (3) the responsible, non-partisan application of world-class research to develop a mature, evidence-based science policy.

Outputs from IRIS projects will consist of aggregate statistical products, reports, and tools that will not directly identify contributing universities without written permission. Tabulations and visualizations released through this research have the potential to enhance knowledge of the interactions between research, entrepreneurship, and innovation, which ultimately allows the Bureau to create better statistical measures of the nation's people and economy.

Policies for Access and Sharing and Provisions for Appropriate Protection/Privacy

In order to be a responsible trustee of contributed university data, the data is 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.

The IRIS Project Team will reconcile requirements from these sources:

- Stakeholder Concerns: Stakeholders are the ultimate owners of their own data. The concerns are mostly around protecting the privacy and integrity of stakeholders, i.e. researchers, students, etc.

- Government Regulations: For example the Family Educational Rights and Privacy Act (FERPA).
- Legitimate Access Needs: In order for the project to proceed, access to confidential data is required.

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 itself is 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.

Appendix A: Description of IRIS Information Security Procedures and Controls

IRIS employs a defense-in-depth security architecture to reduce risk associated with cyber attacks that can impact the confidentiality, availability, and integrity of IRIS systems. Below is a description of the IRIS procedures and controls that are in place to address data security requirement with respect to sensitive but unclassified data maintained on IRIS systems. The procedures are organized into the three classes of controls used in NIST FIPS 200 and the suite of NIST Special Publications that make up the FISMA risk management framework.

A. Management Controls

A.1 Risk Assessment and Management

Risk Assessments of systems are performed periodically or after a major organizational change to address changing threats and organizational priorities. IRIS risk management processes are based on the FISMA requirements as defined in NIST SP 800-30 and the more recent NIST SP 800-39. Internal technical risk assessments of IT network and systems are based on the *Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines* (CAG).

Threat and vulnerability assessments are performed as part of the risk management program to continually assess the effectiveness of the IRIS management, operational, and technical controls. System audits are performed to verify how the system is being accessed, and unusual activity is investigated and addressed.

IRIS's uses expert inputs from a variety of sources, including hardware and software vendors, and virus and security software vendors. System patches and hot fixes are applied to on an as needed basis. Virus definitions are automatically updated, and can be manually updated on an as-needed basis. As information becomes available about potential security threats, the system is checked to ensure that issues are addressed as they are made known.

A.2 Information Sensitivity and Security Categorization

As part of the risk management framework, IRIS will ensure project data is categorized to ensure employed security controls are commensurate with the impact and risks associated with potential *data* exposures. IRIS security categories of data and information systems are consistent with FISMA compliance requirements (e.g., FIPS 199) and are based on three potential impact levels, *High*, *Moderate* and *Low*.

A.3 Protection of Sensitive Identifiable Information

The IRIS Information Security Policy states that all sensitive identifiable information that is accessed, stored, or transmitted on IRIS managed networks/computers is protected in accordance with a written project-level information security plan. Sensitive identifiable information includes personally identifiable information (PII), and personal information. In addition, information that is used to gain access to sensitive identifiable information (e.g., password, passphrase to a security token, security code, etc) are secured to at least the same level as the information it is protecting. This information security plan state applicable laws and regulations, define the boundaries and security category of the information that requires protection, and a description of the appropriate security measures and procedures that are commensurate with the sensitivity of the data in both the electronic and hard copy domains (e.g., administrative controls, authentication, access controls, use of encryption, and sanitization and retention). The IRIS Technical Director works with the other IRIS leadership and in coordination with ISR Information Technology in the preparation of these plans so all known compliance requirements are met.

IRIS protects submitted PII in a variety of ways to ensure maximum protection of client university data.

- All data files uploaded to IRIS are immediately and automatically encrypted. These data files are immediately and automatically moved into a secure data locker on a server that is not connected to an open port to the outside world. The 'Keys' to this locker are stored on an air gaped drive that is physically maintained away from the locker.
- All PII data is immediately and automatically hashed (encrypted) at the field and record level within the database where it is stored. The hashing key is stored on an air gaped drive that is physically maintained away from the database server.
- A special encrypted database is used to house all PII and it is maintained separately from other data.
- Identifiable micro level (record level) data never leaves the secure enclave for any reason other than to merge it with federal data at the Census Bureau.
- Data that is merged with federal data is transmitted in encrypted SAS files from inside the secure enclave using the federal government's Census secure portal. Additionally, PII fields remain hashed throughout the process so no PII micro data is ever sent in an unsecure fashion.

- Micro data is protected inside the Census Bureau systems by Title 13 and Title 26 federal laws. It remains encrypted and hashed until used for matching and then the PII is destroyed within the Census system.

A.4 Review of Security Controls

Internal IRIS security assessment/audits that involve both compliance and substantive testing (e.g., test validity of the control itself) are performed on IT infrastructure systems as well as selected major applications. The scope of these assessments includes an inventory of authorized devices and software, security configurations, servers, and network devices (e.g., firewalls, routers, and switches), boundary defense, monitoring and analysis of audit logs, access control, vulnerability management, and malicious software defenses.

IRIS and ISR IT complete, on an annual basis, FISMA "Self Assessments" based on NIST Special Publication 800-53 to match the federal regulatory requirements.

A.5 Rules of Behavior

Rules governing the use of the company's network and communication tools are outlined in the *Use of Information and Communications Technologies Policy*. This policy outlines responsibilities and expectations for all IRIS employees, including end-user network access and administrative privileged user access. All employees are briefed on this policy during new employee orientation where they subsequently sign that they have read and understand the rules as terms of employment before they are provided user accounts.

A.6 Application/System Interconnection/Information Sharing

IRIS IT policy prohibits connections to external networks (networks other than those supported by IRIS).

B. Operational Controls

B.1 Personnel Security

All IRIS employees undergo a criminal background check and verification of employment and educational background.

IRIS employees are trusted users and, upon acceptance of the *Use of Information and Communications Technologies Policy*, are granted access to IRIS data as required performing their job functions. Access authorization is granted with the understanding that needs may change over time, depending on job requirements.

IRIS implements procedures that ensure consultants/contractors and temporary workers sign Confidentiality and Nondisclosure Agreements before being granted access to sensitive IRIS information systems or proprietary information in accordance with internal published guidance.

Accounts are created through a process that is initiated by the IRIS Technical Director upon hire. Rights and permissions to the system are based on the employee's need to complete specific projects. Once the default set of rights has been applied, the employee's manager can request changes to the user's access permissions. Employees receive an orientation to the system and the rules and responsibilities related to accessing the system prior to being issued account credentials.

Employees are held personally and individually responsible for all actions performed using the IRIS network and the Internet. Violations of any guideline listed below will be subject to immediate disciplinary action to include suspension of employment or discharge, in addition to possible criminal and civil penalties. If necessary, the company will advise appropriate officials of any illegal activity.

B.2 Physical and Environmental Protection

IRIS locations are physically secured by electronic locks. Employees and contractors need security badges for access to their assigned work site. Visitors are escorted at all times by an IRIS or ISR employee. Equipment rooms have either a cipher or electronic lock with a secured code.

Emergency hardware is installed on all Emergency Exit Only doors. Emergency exits are appropriately marked with illuminated Exit signs in to guide staff to the exits in the event of an emergency. IRIS has undergone, and passed, inspections by the governing Fire Marshall's Code.

The building management team has published and distributed an emergency evacuation program in addition to an emergency evacuation plan specific to ISR. ISR has conducted several evacuation drills, some of which have involved the local fire department.

B.3 Contingency Planning

IRIS's present disaster recovery and business continuity capability is based on both replication and synchronization of key applications/servers and data recovery from tape media and/or backup data/image files. The IRIS alternate data facility that hosts the critical servers is located in a different US power grid that the primary data facility.

IRIS performs daily, weekly, and monthly backups. Backup media is stored off-site at a secure location, and can be recalled within four hours. Backup media recalls are tested quarterly to ensure a timely retrieval process. Restores are made from backup data on a monthly basis to ensure integrity of the media.

Included both on the IRIS website and in the technical welcome packet is a complete disaster recovery plan.

B.4 Information Controls

Data, and associated work products, that contain restricted or sensitive information (e.g., data categorized as *High* impact) are annotated with the appropriate security label. Media that contains restricted or sensitive information is locked in a container commensurate with the risk and transported in a manner consistent with security requirements.

Electronic media is appropriately sanitized before being retired or reissued for other uses. These methods will include degaussing, destructive overwrite, or shredding, depending on security requirements.

B.5 Application/System Hardware and Software Maintenance Controls

Hardware and software maintenance is performed by the IT staff. Most hardware is covered under maintenance agreements that provide on-site support for repair and maintenance activities. In these cases, service vendor staff is escorted by IT staff while on-site. Most maintenance activity is scheduled for off hours, with at least 48 hours of advanced written notice, to minimize disruption to staff.

Support contracts are purchased with hardware and software vendors to ensure continuity of operations. Whenever possible, the terms of coverage are managed in a master agreement to ensure that vendor contracts include all hardware/software from a particular vendor. This keeps all equipment covered and prevents IT needing to manage multiple contracts for a single vendor.

The majority of the software in use by this system is commercial off-the-shelf software purchased by IRIS. If purchased with contract funds, assets are tracked to ensure that they revert to the contracting agency at the end of the contract term. Software inventories are tracked online and kept up-to-date with installation moves/adds/changes to keep IRIS in compliance with licensing and usage restrictions.

B.6 Data Integrity/Validation Controls

Anti-virus and malware protection software are used on all employee computers and servers. Virus signature files are updated automatically, and manually as needed. Machines are set to run automated weekly scans. Incoming data transmissions are scanned for malware, spam and other threats through a variety of checks, including firewalls, intrusion detection and other monitoring software.

B.7 Incident Response and Reporting

Information security incident response is an important component of the IRIS information security program. IRIS's incident response capability outlined it the IRIS *Incident Response Plan* that is largely

based on the NIST Special Publications 800-61 that addresses: preparation, detection and analysis, containment, eradication, recovery, and post-incident activities.

Training and security awareness is critical component of incident response as well as incident prevention. Each IRIS employee and contractor is responsible for reporting suspicious or adverse events. ISR IT operational staff and incident handlers shall be trained on incident identification, reporting and escalation, response, and where needed forensics analysis. As part of the incident preparation phase, IT and security staff will monitor notification of alerts and advisories about vendor patches and vulnerabilities.

Incident detection will be performed by multiple sources. Network management software is in use to detect status of system components and communications links. Logs for firewalls are sent to a logging server where they can be used for reporting and analysis. Intrusion detection and prevention technologies are deployed in depth to detect, prevent, and alert when external client hosted sites are attacked.

B.8 Security Awareness and Training

All employees and contractors receive an IT orientation to alert them to appropriate uses of the system, and of consequences for inappropriate use. Once this orientation has been provided, the user is required to sign documentation that this training has been received.

Continuous security awareness is facilitated by the Technical Director as well as security bulletins and alerts disseminated by the IT Department or Chief Security Officer when needed.

IRIS also performs additional security training for personnel associated with specific roles related to information security. System administrators are required to undergo annual refresher as part of an internal IRIS control related to personnel with escalated privileges. Members of the IRIS Computer Security Incident Response Team receive specialized training quarterly in order to effectively response to a security incident.

C. Technical Controls

C.1 Identification and Authentication

Access to the system is controlled by accounts. Each user is required to have their own account, and sharing accounts is specifically prohibited by IRIS policy. Each account is created by specific request. Employee accounts are disabled at close of business on the employees' last day, or immediately at the request of Human Resources or appropriate IRIS Director.

To protect IRIS user accounts, the IRIS Password Policy is implemented using system controls based on the below parameters a minimum eight (8) character complex password schema. IRIS institutes

standards associated with password expiration, uniqueness, minimum age, and bad login attempts, and account lock outs. All passwords used to access sensitive systems are encrypted in transit and at rest using a level encryption that is commensurate with the level of risk. Passwords are changed immediately if there is suspicion that it has been compromised. Users must contact the IT Service Desk to have a lost or forgotten password changed

The network operating system and certain applications on the system help manage user access. For example, restricted use data is only accessible from the site where its use is licensed; the network is configured to manage this requirement. Data and applications on the system have rights restricted to certain groups or users.

C.2 Access Control

Logical access controls are deployed as part of a defense-in-depth architecture beginning with controls at the IRIS perimeter with interior controls layered within the IRIS domain of control. Access controls addresses security of systems - both hardware components and software components. These systems include not only computers, desktops and servers but also laptops, USB memory/drives, and rotational media.

Access controls are in place to restrict activities of users and system personnel to authorized transactions and functions. Access to IT resources and records is limited to authorized individuals following the principle of least privilege and separation of duties.

C.3 Encryption

IRIS Project Directors in coordination with Information Technology will determine the need for encryption using a risk-based approach. Encryption can be applied to communications channels, discrete files, USB drives, removable media, email, or entire hard drives or volumes (applicable to mobile laptops). In general, data categorized as “HIGH” impact (e.g., sensitive identifiable information, credit card information, sensitive federal agency information, IRIS proprietary information, etc) will be encrypted using SSL and secure SSH when in transit over an untrusted security domain/network (e.g., Internet).

Only authorized encryption shall be employed on IRIS systems. Currently AES 256-bit Bitlocker encryption is used on all servers. Users are prohibited from employing encryption to hide information for non-business purposes or to intentionally mask communications from local system monitoring or network intrusion detection systems.

C.4 Systems and Communications Protection

Network Security Architecture

The safeguarding and protections of contributed data are based on a defense-in-depth architecture. Firewalls, VPN's, IPS, and 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.

For interior authentication and authorization controls, IRIS employs and LDAP-based directory service. Distribution lists and security group permissions are assigned at the time of account creation based on user's position. Other permissions are assigned as required or with Technical Director's permission. Group or individual permissions are set either by security policies or group memberships. By setting system/application logging, or system security auditing to the desired levels, a number of transactions or functions can be followed, including unauthorized access.

Network Security Monitoring

All activities taking place on IRIS IT systems are subject to monitoring in order to protect the confidentiality, availability, and integrity of IRIS systems as well as to respond to either internal or external security incidents or even criminal activity. Network monitoring may include collection of email, Internet browsing, and network discovery for the detection of unauthorized/rogue devices. IRIS resources and data, user account and directories, user files, user e-mail, or other data may also be subject to review.

Security Testing and Vulnerability Scans

Security testing and evaluation of systems connected to high-threat environments, or that process or store sensitive data, occurs prior to staging to the production environment. Procedures and test plans shall be updated to reflect lessons learned and newly identified vulnerabilities. Vulnerabilities identified through security testing must be documented and disseminated to the IRIS Technical Director. All vulnerability reports shall be properly classified and access limited on a need-to-know basis.

As a methodology, IRIS uses a combination of manual and automated techniques to assess management, operational, and technical controls. ISR security staff are trained and have received certifications in security testing such as GWAPT (GIAC Web Application Penetration Tester) certification.

Virus/Malware Protection

To protect IRIS systems/data IRIS IT ensures that anti-virus protection mechanisms are installed on all IRIS-owned desktops, personally-owned computers, file servers, and mail servers and that these mechanisms are updated regularly. Anti-virus systems are configured to update automatically, reliably, and through a centrally controlled management framework, where feasible.

C.5 Audit Trails and Security Logs

IRIS implements security logging on information systems such as computers, network devices, firewalls/VPNs, and application commensurate with the risk associated with the loss of confidentiality, integrity and availability of the system/data. Data and systems processing/storing sensitive data should as a minimum be configured to log and track attempted breaches that include the time of incident, source information (e.g., IP address or user-ID), access attempts, and failures. All security logs shall be maintained in a manner that ensures confidentiality and integrity of data (e.g., audit trails and system logs are accessible only to administrative users).

Tab A – System and Application Controls (For Reference Only)

Below are the system controls generally in place for any IRIS managed system:

<table>
<tr><td>Control Type</td><td>Security Protective Measure Description</td></tr>
<tr><td>Network/System Access (stored on servers)</td><td>- Access to project information on shared network drives, Microsoft SharePoint, databases, and other information systems are generally controlled using Active Directory role-based access control (e.g., network access to Microsoft resources) or local file/folder permissions (e.g., across all operating systems).
- Coordination between data owner/system manager and IT will be made to ensure user and Group level permissions are controlled based on principle of least privilege access model.</td></tr>
<tr><td>Password and PIN Standard</td><td>Password/Pass Phrases:

- Access to project data will require "unique" user IDs in accordance with IRIS Password strength standards summarized below (reference IRIS Password Policy):

<table><tr><td>Minimum Length</td><td>8 characters</td></tr><tr><td>Character requirements

(3 of 4 required)</td><td>- Min. 1 upper case character

- Min. 1 lower case character

- Min. 1 number

- Min. 1 special character (@, #, %, etc.)</td></tr></table>
- All desktop are configured with automatic screen savers configured with password protection.
- Group logins or shared passwords are prohibited.</td></tr>
<tr><td>Encryption</td><td>The following applications are supported by IRIS for encrypting data:

File encryption applications and supported algorithms)</td></tr>
</table>

	- Microsoft Office 2007 (or newer) applications (128-bit AES encryption) - WinZip versions 10.x or newer (128-bit or 256-bit AES encryption) - Adobe Acrobat versions 9x or newer (256-bit AES encryption); versions 7 and 8 (128-bit AES encryption) - PGP Zip on IRIS computers (256-bit AES encryption) File, device, disk encryption - PGP encryption applications: Desktop Home, Endpoint Device Control, Desktop Email, Whole Disk Encryption (better suited for higher volume of data). Other File Protections: - File-level password protection mechanisms found in Microsoft Office applications are suitable for when some form of confidentiality is needed, however, is not as strong a measure as encryption and should not be used for security of sensitive individual identifiers. - Worksheet level password protections found in Excel are not designed to be secure and should not be used to provide confidentiality (e.g., hidden columns in Excel can be readily seen using other word processing applications).
Remote Access	- Network access from external users: -- IPSec VPN (restricted to IRIS provided laptop) -- Web SSL VPN (from any web browser) -- Windows Terminal Server (from RDC or web browser)
Physical Access Controls to IRIS Data Centers	- Physical access to network file servers and database servers that store project data are in the ISR data center is restricted to only IT personnel and key facility managers using ID badge access controls where badge use is electronically logged to a central system. - The physical space inside the ISR data center/server rooms are monitored with video surveillance - A visitor access log is maintained to manually log all personnel who do not have badge access
Perimeter	- All business/project data is protected by at least one commercial-grade firewall

Security	- IRIS IT/Web Services employs a commercial-grade intrusion prevention system in addition to commercial-grade firewall
Malware Protection	- All servers that store data employ malware protection - Automated updating of virus signatures
Data Backup and Replication	- At least once per 24 hours - Disk-to-disk or disk-to tape - Tapes (for long term storage) are picked up be secure courier once per week and stored at secure offsite location
Security Logging	- Security logging is performed on the file server. As a minimum, event logs audit unsuccessful logins.
Sanitization and Destruction	- Physical Destruction: All IT managed storage hardware designated for disposal (e.g., hard drives, printers, magnetic media) is physically destroyed by IRIS's recycling vendor by shredding the hardware to guaranty 100% destruction of all data. Smaller bulk sensitive optical media (e.g., CD/DVD) can also be physically destroyed via document cross-cut shredding devices. - Sanitization: Hard drives that include sensitive data that are designated for re-use by IT are sanitized using disk duplicator hardware (KCLONE12HD) that includes a disk sanitization feature using the DoD 5220.22 standard (7 pass version). - A "Certificate of Data Destruction" will be provided to the project or client upon request

Tab B – IRIS Security Diagram

Below is a diagram of how IRIS handles security and encryption.