Project Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| Description & Special Resource/Equipment Requirements:  |

Principal Investigator:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-mail address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Office Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Technical Leader: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Phone: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

E-mail address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Office Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |
| --- |
| Research Timeline & End Date:  |

Data Description/Classification Level:

Describe the data elements that are accessed, created, altered, viewed, derived, or deleted in this project. The highest (most restrictive) data element’s classification level above should determine the project level data classification. Please refer to the [Institutional Data Policy](https://itsecurity.uiowa.edu/policy-institutionaldataaccess) and [Data Classification Guidelines](https://itsecurity.uiowa.edu/classifying-institutional-data) for additional information. All classification levels other than public are collectively referred to as “non-public.”

|  |  |
| --- | --- |
| **Public – Low Sensitivity**  | No existing local, national, or international legal restrictions on access apply. May be granted to any requester, or it is published with no restrictions. |
| **University-Internal – Moderate Sensitivity**  | Non-Public Protected or Internal data. Material for which the terms and conditions of the contract specify that the data is licensed on the basis of institutional affiliation. Data may be accessed by persons as part of their job responsibilities (role-based), or participation in a research project. |
| **Restricted – High Sensitivity**  | Data sensitive due to intellectual value or ethical considerations, or that could be used to invade institutional privacy, or for which there may be regulation, civil statute, or other restrictions requiring its protection. May have personal privacy considerations, or may be specifically restricted by federal or state law such as FERPA. |
| **Critical – Very High Sensitivity** | Data sensitive due to intellectual value or ethical considerations, or that could be used to invade institutional privacy, or for which there may be regulation, civil statute, or other restrictions requiring its protection. May have personal privacy considerations, or may be specifically restricted by federal or state law such as HIPAA, GDPR, ITAR, or export controls. |

|  |  |  |
| --- | --- | --- |
| Data Element Description | Data owner and where data will reside | Classification Level  |
|  |  |  |
|  |  |  |
|  |  |  |

PROJECT-LEVEL DATA CLASSIFICATION \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Security Protections Checklist:

***All controls up to and including those for the project level data classification must be addressed***. Implementation details may be a document name/location, URL, software tool, person responsible, timeline/interval, or other clarifying data. Controls and standards described below are specified by legal, policy and contractual requirements. For more information see the applicable regulation(s), the [University IT Policy](http://itsecurity.uiowa.edu/policy/) digest, and/or the relevant/applicable [Iowa Department of Administrative Services IT Standards](http://das.ite.iowa.gov/standards/enterprise_it/index.html).

|  |  |  |
| --- | --- | --- |
| **ADMINISTRATIVE CONTROLS** | Required for Classification Level: |   Implementation Details |
| A documented contingency plan including data recovery procedures exists | All |  |
| Register all servers with the Information Security & Policy Office so that the systems can be monitored for potential security problems. In addition this supplies name and contact information for the systems, as well as the services, criticality and sensitivity of the data. All other computers must be inventoried locally with identification of the assigned user.  | All |  |
| All suspicious activity and/or security incidents must be reported to the Information Security & Policy Office (it-security@uiowa.edu or 335-6332) prior to taking action to investigate. Loss or theft of any mobile computer shall be reported to the Information Security & Policy Office within 24 hours. The notification shall include contact information, date of theft/loss, description of the theft/loss, whether sensitive information was stored on the device, whether the storage was encrypted, and whether the password or token was stored with the laptop.  | All |  |
| Regular security/risk evaluations are performed by a third party (e.g., Collegiate IT Manager, Security Office, Internal Audit, HCIS Security) at least annually. | All |  |
| System/audit logs are maintained for a minimum of 90 days, and regularly analyzed for security vulnerabilities or intrusions. All problems that are discovered must be resolved. Devices will synchronize their time with a campus NTP server. | Non-public |  |
| Criminal background checks will be performed on individuals with system-level access  | Non-public |  |
| IT Confidentiality and/or Non-Disclosure Statements are signed by all persons with access to confidential information. | Non-public |  |
| Routine scanning for known security vulnerabilities and/or faulty configurations must be performed on a regular basis. | Non-public |  |
| Annual training is required and must be tracked. All users must complete security awareness training that includes protection of confidential information; system administrators must complete technical security standards training.  | Non-public |  |
| Legal Counsel approval has been obtained for all non-US citizens’ permission to use export-controlled software and information | Restricted or critical |  |
| Any additional controls specifically required by law, regulation or contract. | All |  |
| **OPERATIONAL CONTROLS** | Required for Classification Level |   Implementation Details |
| A process for backup and recovery of data and applications exists, with three versions of backups, kept for a minimum of 30 days. One fully recoverable backup version must be stored in a secure off-site location. The restore process must be documented and tested. | All |  |
| All computers, including those connecting to the system from off-campus, are kept up to date with current operating system and application updates/patches by reviewing, testing, and installing them at least monthly. Install critical security patches for active exploits within five (5) business days of release. Successful patch installation should be verified manually or use a management service such as System Center Configuration Manager (SCCM) for Windows. If patches can’t be installed, consult the vendor for compensating protections.  | All |  |
| Equipment is housed in an environmentally sound, restricted access server room or data center location which is monitored. Use a backup power source if availability of the system is critical | Non-public  |  |
| At least two persons must have privileged (system administrator level) access to the system.  | Non-public |  |
| User accounts and access lists are reviewed at least quarterly, and kept up to date by deactivating invalid/terminated users, and removing unnecessary access rights. | Non-public |  |
| Devices and media containing confidential data shall be erased with a DoD approved method prior to disposal. Paper documents containing confidential data shall be shredded. | Non-public |  |
| Implement a change management procedure for deployment of web applications. Separation of duties shall be implemented to prevent developers from publishing their own applications to the production environment. | Non-public |  |
| User accounts are automatically disabled/locked given a maximum of five authentication violations since the last successful login.  | Non-public |  |
| Backup media is not shared with other systems, data, or applications, and is transmitted, stored, and disposed of securely. | Non-public |  |
| **TECHNICAL CONTROLS** | Required for Classification Level |   Implementation Details |
| All eligible computers, including those connecting/accessing the system must have current anti-virus software installed and signatures updated daily  | All |  |
| Privileged access account sessions must be encrypted. Use industry standard “strong” encryption algorithms and key lengths: a minimum of 256 bit symmetric or 2048 bit asymmetric for: remote connections; administration tasks; and file transfers containing confidential data. | All |  |
| Authentication data (e.g., passwords) must be encrypted on the network and in storage | All |  |
| Implement full disk encryption on portable devices such as laptops, tablet computers, and external (such as USB flash) storage devices.  | All |  |
| Employ system facilities to restrict logins to a defined/limited set of IP addresses and communication ports using an appropriately configured firewall. The following requirements must be met for network firewalls: 1. Default passwords and SNMP Community strings are changed 2. Software/device is kept up to date, and updates tested before being applied 3. Firewalls shall do ingress and egress filtering, use default deny policy, and fail closed, as well as logically segregating critical systems 4. Firewall configurations are reviewed, and updated quarterly by network/security administrators | Non-public |  |
| The UI Wireless Network Service should be used for all wireless connections, or a comparable WPA2 enterprise authenticated protocol/service must be used | Non-public |  |
| Individual account/logins are defined for every user of the system, using the Hawk ID format, and guest/anonymous access is prohibited for all other than public access data.  | Non-public |  |
| Integrate the system with University Hawk ID authentication to automatically manage user accounts and passwords, or use local strong password practices if Hawk ID authentication is not possible (Set complex 9-15 character passwords on all accounts consisting of a combination of alpha, numeric, and/or special characters, and change all passwords every 60-90 days.) This applies to all accounts including default/shipped accounts, and generic process/application accounts. Alternatively, employ two-factor authentication.  | Non-public |  |
| All unnecessary services, communications ports, and system-level accounts must be disabled. Document the services (programs) running on the system, and the communications ports left open, and review them quarterly for changes.  | Non-public |  |
| Security relevant user activities must be actively recorded/audited, and the logs must be stored in restricted access files for a minimum of 60 days  | Non-public |  |
| Employ the “least privilege” principle by granting users only the minimum necessary authorization level to do their work. | Non-public |  |
| Employ 20 minute inactivity timeouts on all computers with access to sensitive data. Screen savers with passwords may be used as an alternative.  | Non-public |  |
| Implement a host based intrusion detection/prevention system such as Tripwire or OSSEC to monitor the system (i.e., for log analysis, file integrity checking, rootkit detection, time-based alerting, and active monitoring). | Restricted or critical |  |
| Collection and use of social security numbers shall be limited and based on a strong business need. Social Security numbers shall not be used as a unique customer number, used as the primary key in databases except where required by law, or displayed in full on external web-based applications beyond the initial data entry screen.  | Restricted or critical |  |

Review Information: Next Review Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Agreement has been reached on the implementation details:*

Principal Investigator:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Technical Leader: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

University IT Security Officer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*A site visit to review/verify the implementation details have been completed, if applicable:*

3rd Party IT Official:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Final Approval:*

VPR Officer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_