The University of Iowa
IT Security Plan Requirements for Restricted Data

System Name: _____ Date: _____

Description & Special Resource/Equipment Requirements:

Business Owner:_____ Phone: _____

E-mail address: _____Office Address: _____

Technical Support/Custodian: _____ Phone: _____

E-mail address: _____Office Address: _____

System Launch Timeline & End Date (if applicable):

Data Description/Classification Level:

Describe the data elements that are accessed, created, altered, viewed, derived, or deleted in this system. The highest (most restrictive) data element's classification level should determine the system level data classification.

Level 1 - **PUBLIC**	No existing local, national, or international legal restrictions on access apply. Access is granted upon request.
Level 2 - **INTERNAL**	Material for which the terms and conditions of the contract specify that the data is licensed on the basis of institutional affiliation, or, data which may be accessed by persons as part of their job responsibilities (role-based access).
Level 3a - **RESTRICTED**	Data sensitive due to intellectual or proprietary value or ethical considerations, or that could be used to invade institutional privacy, and for which there may or may not be regulation, civil statute, or other restrictions requiring its protection, or where data or software disclosure is contractually restricted and/or disclosure consequences include significant financial, homeland security, or other legal risk for the University. Access is controlled from creation to destruction, and is granted on a need-to-know basis or as permitted by law.
Level 3b - **RESTRICTED-HEALTH**	Restricted Data that could be used to invade personal privacy if accessed and used inappropriately. "Personally identifiable health information" and other federally regulated, protected health information.

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

SYSTEM-LEVEL DATA CLASSIFICATION _____

The University of Iowa
IT Security Plan Requirements for Restricted Data

Security Protections Checklist:

All controls up to and including those for the system level data classification must be addressed. **Implementation details may be a document name/location, URL, software tool, person responsible, timeline/interval, compensating/alternative control, or other clarifying data.**

ADMINISTRATIVE CONTROLS	**Level**	**Implementation Details**
A documented contingency plan including data recovery procedures exists	1	
System/audit logs are routinely analyzed for security vulnerabilities or intrusions, and all problems discovered must be resolved. The process used, including the interval between reviews and responsible party is documented.	1	
All suspicious activity and/or security incidents must be reported to the IT Security Officer	1	
Regular security/risk evaluations will be performed by a third party (e.g., Department or Collegiate IT Manager, IT Security Officer, Internal Auditor)	1	
IT Confidentiality and Non-Disclosure Statements are signed by all persons with access to confidential information	2	
Routine scanning for known security holes and or faulty configurations will be performed	2	
A system or unit-level Disaster Recovery Plan is available, which includes • contact information (with after hours) for business owners and system custodians; • prioritization of recovery for systems, processes, and data; • emergency operations procedures (alternative systems, manual procedures, etc) with metrics describing how long normal sysem may be inoperable before emergency processes are invoked; • system recovery procedures (steps, necessary resources)	3	
Legal Counsel approval has been obtained for all non-US citizens' permission to use export-controlled software and information	3	
Background checks will be performed on individuals with privileged (sysadmin) system-level access	3	
OPERATIONAL CONTROLS	**Level**	**Implementation Details**
A process for backup and recovery of data and applications exists, with a minimum of 3 versions, 30 day life, and 1 backup copy stored off-site	1	
The operating system and all applications are kept up to date with appropriate security and service patches (describe process, frequency)	1	
Equipment is housed in restricted access room, with backup power source	2	
At least two persons have privileged (sysadmin) access to the system	2	

Process is documented for user accounts and access lists to be routinely reviewed and kept up to date, including the interval between reviews and responsible party.	2	
User accounts are automatically disabled/locked given a set number of authentication violations since last successful login	2	
Criteria used for account eligibility, account access/duration, and account expiration is documented, including the process for notification of employee terminations and how they are handled (use checklist if applicable)	3	
Procedures for emergency access to the system (criteria, approval, follow-up, oversight) are documented.	3	
Procedures are documented for the systematic control of changes to hardware and software of the system, (request, approval, testing, QA, implementation, and reporting), including the process for periodic audit review of changes, and the responsible party.	3	
Backup media is not shared with other systems, data, or applications. . The method or type of backups, frequency of backups, and the procedure for recovery/restoration of data is fully documented and tested regularly, for a limited failure and a full system failure situation.	3	
Decommissioned data media is sanitized (degaussed, destroyed, etc)	3	
TECHNICAL CONTROLS	**Level**	**Implementation Details**
Guest, public or anonymous access is allowed	1	
All computers, including those connecting/accessing the system must have current anti-virus software	1	
Individual account/logins are defined for every user of the system, using UI-assigned login identifiers (i.e., "HawkID"), using Enterprise Authentication when possible, and guest/anonymous access is prohibited	2	
Use Enterprise Authentication to manage logins, or local strong password practices (complex long (6-15 char) passwords, changed every 90-180 days, and not reused), for all accounts including default/shipped accounts, and generic process/application accounts, or employ two-factor authentication	2	
All unnecessary services, communications ports, and system-level accounts must be disabled	2	
Security relevant user activities must be actively recorded/audited, and the logs must be stored in restricted access files	2	
Authentication data must be encrypted on the network	2	
Privileged (sysadmin level) account sessions must be encrypted	2	
Employ least privilege principles by granting users only the minimum necessary authorization level to do their work.	3	
All (non-privileged and privileged) account sessions must be encrypted	3	
Employ 15 minute inactivity timeouts (or password screen savers) on all machines with access to sensitive data, which are in open areas or shared offices	3	

Database system/server and Web server must run on separate systems	3	
Employ system facilities to restrict logins to a defined set of IP addresses (e.g., tcpwrappers, TCP/IP filters) or consider using a host based firewall program	3	

Review Information: Next Review Date: _____

Agreement has been reached on the implementation details:

Business Owner:_____ Date: _____

Technical Support/Custodian: _____ Date: _____

IT Security Officer: _____ Date: _____

A site visit to review/verify the implementation details has been completed:

3rd Party IT Official:_____ Date: _____

Final Approval:

University Official: _____ Date: _____