Sample UCR PI Data Security Plan

Organization	
Organizational Unit	Chemistry
Department	Research
Data Proprietor(s)	Dr. Jonathan Doe
Date of Submission	November 1, 2007

Type of Protected Data	
Social Security Number	Yes
Driver's License Number	Yes
Financial Account or Credit Card number in combination with any password that would permit access to the individual's account.	No

Access Procedures and Controls			
Is there a defined procedure to control access to the computer?	Yes	Is a policy to control access to the computer implemented?	Yes
Are requests/approvals recorded and kept?	Yes	Are background checks required for systems with sensitive or protected data?	Yes
Are there periodic audits reviewing who has access?	Yes	Are there periodic audits reviewing privileges of users?	Yes
Are system logs kept?	Yes	Are system logs periodically reviewed?	Yes

List name of file, type log information contents, retention period, frequency of review and the contact information for the person responsible for the review.

Location/ File Name	Information	Retention Period	Review Frequency	Contact
/dev/sysmsg	err;kern.notice;auth.notice	6 months	Hourly/ weekly	Dr. Jane Doe

System Administration					
How many people have administrative rights to your systems?	3	Are logs kept of administrative access?	Yes	Are they reviewed periodically?	Yes

Please describe the logging procedure. Include access log location, retention period, frequency of review and the contact information for the person responsible for the review of whom and when the system was accessed.

Log files are written locally to /dev/sysmsg as well as written to the central SYSLOGing system. An automated script is run hourly to detect anomalous behavior such as login failures, etc. Nightly these logs are reviewed by the Operations staff. The log files are kept on tape for 6 months. Dr. Jane Doe reviews these logs weekly for incidents the script or Operations staff may have missed.

Primary System Administrators			
First/Last Name	Dr. Jane Doe	Email Address(es)	jane.doe@ucr.edu
Work Number	22222	Additional Numbers	Cell-222-2222
Secondary System Administrator			
First/Last Name	Dr. Jack Doe	Email Address(es)	jack.doe@ucr.edu

Work Number	22222	Additional Numbers	Cell-222-2222
Other System Administrator(s)			
First/Last Name	Lowe Doe	Email Address(es)	lowe.doe@ucr.edu
Work Number	22222	Additional Numbers	Cell-222-2222
List Additional contacts information	play.doe@ucr.edu, x-22222, cell 222-2222		
List Additional contact information	no.doe@ucr.edu, x-22222, cell 222-2222		

General System Information	
Enter IP address(es). Please include additional address if using multiple nic cards for the same physical system. *e.g. 138.23.225.13*	138.23.255.255
Enter the system's fully qualified host name. *e.g. TANG.UCR.EDU*	CHEM101A.UCR.EDU
Please list all the DNS aliases or URLs associated with this host.	CHEM-TEST CHEM-USER CHEM-DATA
Describe this system's use or purpose.	This system supports Chemistry applications, including student records and faculty/staff personnel information. Applications are developed, tested and put into production for Chemistry research.

Operating System					
Check Type of Operating System	☐ Windows	Version		Patch Level	
	☐ Solaris ☐ FreeBSD ☒ Linux ☐ Other	Version	CentOS 5.1	Patch Level	0
If Other, enter name		Version		Patch Level	
System's NetBIOS (WINS) name.	Doe_Domain				

Services and Applications

The following questions regard system services and applications. A "Service" is functionality offered to the end-user/customer like a web server, SSH, SMTP, SQL or Exchange. Whereas an "Application" would be, Internet Explorer used to browse the network or Eudora to read mail.

Service	Version/ Patch Level	Application	Version/ Patch Level
HTTP Apache	*2.2*	Thunderbird	2.0.0.9
SMTP Sendmail	*8.13.10*	OpenOffice.org	2.0
SQL	*2.6.18a*		
IP Filter	*3.4.35*		

Software Development Controls

Do you use change management when you develop applications that interact with or use restricted and/or essential data? Yes

If yes, please describe your change management system and procedures. If you are using a vendor product for change management, include the product name and version. Database source code control is managed using CVS. All files are checked in and out from the data repository which keeps all versions of all the files protecting users from accidental file loss. This system allows back-tracking to previous versions of a file as well as providing branching, sharing, merging, and management of file releases functionality. Changes are announced in a weekly Change Management meeting via phone with all Managers/assignees in Chemistry.

Provide the below information if there is a database administrator(s)			
First/Last Name	Dr. Jack Doe	Email Address(es)	jack.doe@ucr.edu
Work Number	22222	Additional Numbers	Cell - 222-222
Additional contact information	Another.doe@ucr.edu, x-22222, cell 222-2222		

How may people have access to databases on this system that contain protected data?	3	Has the Data Proprietor authorized all of the people with such access?	Yes	Do any of the people with access use a shared password?	No

Are logs kept of all database accesses?	Yes

If yes, please describe the logging procedure. Include log location, retention period, frequently of review and the person responsible for the review. SQL has been setup to write selected type of audit events to the operating system log directory. Dr. Jack Doe has written a script to hourly review privileged account access. This file is kept for 6 months on tape.

Data Security			
Is RAID technology deployed for disk storage/subsystem?	Yes	What RAID level is used?	Level0-7

Please describe in detail how RAID has been deployed. RAID1 is used for the operating system disk. Disks containing critical data are stored on disks sub-systems using RAID6.

Encryption			
What vendor is used for data encryption?	Pointsec	What version?	6.3-1

Is encryption used on this system?	Yes	Is whole disk encryption used?	No	Is specific file encryption used?	Yes

Please describe the encryption process including key management. Files containing protected data are encrypted. If the protected data is kept in the SQL database, the field containing the protected data is encrypted. Keys are stored on the central key management system as well as in a fire proof vault with access only allowed to three researchers.

Backups			
Are your information resources backed up?	Yes	What is the backup media?	Tape/Disk

In detail, please describe the schedule for performing backups. (Mon-Thurs perform incremental backups, Friday Full/Image backups) The disk subsystems are backed up Monday-Thursday with incremental (cumulative) backups with full image backups are done through the weekend. Nightly, databases are closed and database specific backups are performed to disk. Backups are kept for four (4) weeks and then the media is put back into the rotation. The exceptions are the quarterly backups kept for one year, archived database files kept five years, and user accounting files also kept for five years. Chemistry operation staff is responsible for ensuring proper tape rotation and archiving. Tapes are kept in the vault or are stored off-site.
Are backups kept locally or sent off-site. Please describe.

The facility keeps tapes stored in a vault or are stored off-site. A vendor for offsite backup data storage services to enable storage of tape backups of critical data in a safe, secure environment located some distance from the computer center. The current vendor is Iron Mountain. The Iron Mountain process is to pick up and deliver storage containers that hold tape backups of campus systems.
Please describe the method for performing backups. For example: Remotely via Veritas NetBackup. Backup scheduling and performance is managed with Veritas NetBackup software. System software and applications (with their data) are backed up.
What is the retention period for keeping backups? 5 years
Do you transfer or make copies of restricted data to other systems? Yes
Do you use encryption when transferring restricted data to other systems? No If Yes, describe encryption cipher method and key management. N/A

Data Sanitization					
Is data sanitization performed on disks?	Yes	Is data sanitization performed on tapes?	Yes	Is data sanitization performed on Flash Drives?	Yes
Please describe the data sanitization procedure. Each disk is written over using the program CleanUp v. 3.5 with random write patterns with 5 passes. If the disk is inoperable and contains protected data, it is sent off-site to Safe Clean Ltd. for degaussing and physical destruction.					
Please describe the data sanitization documentation. Sanitization is performed in accordance to C&C Sanitization policy published Dec. 2007.					

Communications Security		
Is this system behind a network firewall? Yes	Who is the person responsible for managing the network based firewall?	Abott Doe
	Email address.	abott.doe@ucr.edu
	phone number(s)	22222
What appliance is used as the network firewall? Please include platform, version of code, and a brief description of the rule set. The firewall is installed on a Intel-based, rack mounted system running open-source FreeBSD operating system. Access is limited to only the local VLAN and access from off-campus is not permitted.		
How frequently are firewall logs reviewed? What is the most frequent incident found in these logs? Port scans		

Host-Based Security
Does this system have a host-based firewall? Yes
What software, including version, is used for the host based firewall? ipfilter 3.4.35
How frequently are firewall logs reviewed? Logs are reviewed via automated script hourly. In the event a predetermined threshold limit is reached, an automatic email is generated notifying the system administrator, database proprietor and security lead so immediate action can be taken. Weekly the logs are reviewed by the system administrator for anomalous

behavior the script may not be designed to alert so the script may be modified to add new alerting functionality.
What is the most frequent incident found in the firewall logs? Port scanning
Does this system have file system integrity checking? Yes
If Yes, describe what software, including version, is used? The file system had the checksums of all the files contained on the disk recorded in a database. Periodically the checksums are recomputed and checked against the original values contained in the database. The database of checksums are securely kept on another system to prevent unauthorized modification.

Logging and System Monitoring			
Are system logs kept?	Yes	Are system logs periodically reviewed?	Yes

List name of file, type log information contents, retention period, frequency of review and the contact information for the person responsible for the review.

Location/ File Name	Information	Retention Period	Review Frequency	Contact
/dev/sysmsg	err;kern.notice;auth.notice	6 months	Hourly/ weekly	Dr. Jane Doe
/var/adm/messages	*.err;kern.debug;daemon.notice;mail.crit	6 months	Hourly/ weekly	Dr. Jane Doe

Physical Security/ Location					
Building	CS	Floor	2	Room Number	231

Describe the physical security for this system. Building is locked and alarmed after hours. During normal business hours, room is locked unless occupied. Only selected individuals have key access to room 231. Campus police respond to all alarms.
Is this system a laptop? No
If yes, please describe methods used to ensure physical security of the laptop. Even thought this system is not a laptop, all users must re-log on with password after 15 minutes of no activity.
Are external ports disabled to prevent unauthorized access? Yes
Is the system's BIOS password protected? Yes

Managerial Controls	
What is done to ensure timely removal of accounts for users who no longer require access? A major aid to controlling and monitoring who may gain access to specified services and data is to utilize the campus user identity management (authentication) system, specifically, a directory service that is a central repository for campus entities and affiliates. Employing a centralized identify management system provides a structure for easier password use and control by users since it facilitates single sign on and the utilization of fewer usernames and passwords. When user's leave the University their access is revoked.	
Are you familiar with UCR's IS-3 escalation procedure? Yes	Are user's required to have background checks prior to accessing protected data? Yes
Is education given to investigators/researchers about safe handling of sensitive research data? Yes	

Disaster Recovery
Do you have a disaster recovery plan for this system? Yes Please describe. The disaster recovery plan includes emergency equipment leasing as well as installation locations in the event the current data center is uninhabitable. This plan is reviewed periodically.
Has this plan been tested? Yes If yes, what were the results? A test system had the system recovered from off-site backup tape and a database was successfully restored and verified.