**Purpose of the Decentralized Systems Annual Review Form**

CSU Information Security Policy requires that the University implement proper physical and system configuration security, conduct routine vulnerability assessments, follow strict password standards, and implement and enforce user access controls for all decentralized campus systems (i.e., those systems not managed by ITS) that contain Levels 1 and 2 Confidential Data. In addition, the University must maintain a comprehensive inventory of all decentralized systems that includes verification that these requirements are consistently maintained. In order to comply with this requirement, departments that house and manage decentralized systems must complete an annual review and submit the report to the director, IT Security and Compliance.

**Instructions**

System data owners or system administrators are responsible for preparing this annual report of system, system data and user access. Department administrators are responsible for reviewing, approving and submitting the final report. Refer to *ITS-2011-S User Access Controls and Risk Management for Decentralized Systems* for specific information.

Completed annual reports must be submitted to the director, IT Security and Compliance by the date requested.

**Contact Information**

|  |  |  |
| --- | --- | --- |
| Name:       | Department:       | College/Division:       |
| Phone:       | Email:       | Job Title:       |

**System Information**

|  |  |
| --- | --- |
| System Name:       | System Administrator(s):       |
| Physical Location:       | Is location physically secured? [ ]  Yes [ ]  No |
| This system is a:  | [ ]  Server | [ ]  Computer | [ ]  Laptop | [ ]  Other Describe:       |
| Is this system: |
| Connected to the campus network? [ ]  Yes [ ]  No | If Yes, has ITS reviewed and approved the installation? [ ]  Yes [ ]  No |
| Accessed remotely? [ ]  Yes [ ]  No | If Yes, has ITS reviewed and approved the installation? [ ]  Yes [ ]  No |
| Used to process Credit Card payments? [ ]  Yes [ ]  No |  |
| What types of devices are allowed to access this system? | [ ]  Computer [ ]  Laptop [ ]  Tablet [ ]  Smartphone |
| Is this system: | [ ]  Campus-based | [ ]  CSU-wide | [ ]  Vendor-hosted |
| If vendor-hosted, can it support: | [ ]  NIST password standards*(Minimum length, change every 180 days, lock out after failed attempts)* | [ ]  2-Step authentication*(Use of a second form of identification, such as a cell phone or token)* |

**Data Information**

|  |  |
| --- | --- |
| Data Owner:       | Describe the data stored on the system:       |
| Data Classification *(Check all that apply):* |  |  |
| Level 1 [ ]  Yes [ ]  No | Level 2 [ ]  Yes [ ]  No | Level 3 [ ]  Yes [ ]  No |
| System data is encrypted? [ ]  Yes [ ]  No [ ]  Don’t know |
| System data backup exists? [ ]  Yes [ ]  No | Backup is encrypted? [ ]  Yes [ ]  No | Backup Location:       |

**User Access Information**

***Departments are required to use and retain a user access form for each individual approved to access the decentralized system.***

***IT Security and Compliance or CSU auditors may conduct a random sampling based on system user IDs and/or request form copies.***

|  |  |
| --- | --- |
| Every system user has submitted a user access form that documents approved access. | [ ]  Yes [ ]  No |
| All user access requests have been reviewed and user job duties warrant access to this data. | [ ]  Yes [ ]  No |
| Users are instructed to comply with password standards as described in *ITS-2008-S Password Standards*. | [ ]  Yes [ ]  No |
| How often is user access reviewed to ensure access is removed when job duties change or the employee is separated? |
| [ ]  Monthly | [ ]  Quarterly | [ ]  Annually | [ ]  Other Describe:       |
| Users accessing Level 1 Confidential Data remotely are using 2-step authentication? | [ ]  Yes [ ]  No [ ]  Don’t Know |

**Vulnerability Assessments**

|  |  |
| --- | --- |
| Has ITS notified the department regarding system risks identified during routine vulnerability scans this year? | [ ]  Yes [ ]  No [ ]  Don’t Know |
| If yes, were the vulnerabilities patched or fixed? | [ ]  Yes [ ]  No [ ]  Don’t Know |
| Has the department reported any lost or stolen equipment this year related to this system? | [ ]  Yes [ ]  No [ ]  Don’t Know |
| Are users allowed to back up the data onto USB or other electronic storage device? | [ ]  Yes [ ]  No [ ]  Don’t Know |
| If yes, are the storage devices password or biometrically protected? | [ ]  Yes [ ]  No [ ]  Don’t Know |

**Attachments to Include**

System administrators must run the following system reports for attachment to this form.

* Listing of system administrator accounts with name, Campus ID Number (CIN) and email address.
* Listing of user accounts with name, Campus ID Number (CIN) and email address.

Example format:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Account name | First Name | Last Name | CIN | Email |
| *Testaccount* | *Test* | *Account* | *123456789* | *tacct@calstatela.edu* |

**Approvals**

I certify that I have reviewed and approved all user applications for access to this system, the roles assigned to the users are appropriate for the job requirements and responsibilities, access for all separated employees has been removed, and the sys admin and user IDs on the attached reports correspond to the active user applications currently on file.

|  |  |  |
| --- | --- | --- |
| System Data Owner (please print or type) |  | Title |
|  |  |  |
| Signature |  | Date |
|  |  |  |
| Department Administrator (please print or type) |  | Title |
|  |  |  |
| Signature |  | Date |