**Purpose of the Third-Party Service Provider System Access Request**

This form is for vendors or consultants with a contract or purchase order from Cal State LA who require temporary access to a University infrastructure or support system (e.g., Point N Click, Blackbaud, Hershey, AdAstra, CashNet, Moodle, etc.) in order to perform required services.

**Instructions**

1. The third-party service provider must complete sections 2 and 3, and sign and date section 4.
2. Attach a copy of your FERPA certificate dated within the last two years to this form.
	1. For a new certificate, go through the FERPA tutorial at <http://www.calstatela.edu/ferpa> and take the test.
	2. When you reach the information screen, type “**vendor**” in *Empl ID* field, fill in the other requested fields, and click on the *Submit Your Information & Print Certificate* button.)
3. If a network account is need, also submit form ITS-8828 [*Third Party Network Access Request*](http://www.calstatela.edu/its/forms) form.
4. The responsible Cal State LA manager must complete section 1, approve section 5 and forward to the data owner.
5. If applicable, the data owner must assign access rights and indicate approval in section 6.
6. Make a copy of this form and all attachments for your records.
7. Submit the completed application to the ITS Help Desk, LIB PW Lobby.

**Note:** Be familiar with the laws, standards and guidelines available online at: <http://www.calstatela.edu/its/itsecurity/guidelines/index.php>.

# University Contact and Procurement Information *(To be completed by the Cal State LA manager or contact)*

|  |  |  |
| --- | --- | --- |
| Manager or Contact | Manager’s or Contact’s Extension      | Office Extension      |
| College or Division | Department or Unit | Office Location (Bldg. / Room)**/** |
| Purchase Order or Contract Number      | Start Date      | End Date      |

# Vendor Information *(To be completed by the vendor)*

|  |  |  |
| --- | --- | --- |
| Name | Title | Company Name |
| Business Phone | Cell Phone | Company Street Address |
| Business Email | Company City, State, Zip |
| Status (check one)[ ]  Vendor [ ]  Consultant [ ]  Other       | Company Telephone |

# Access Request *(To be completed by the vendor or the vendor’s Cal State LA contact or manager)*

|  |
| --- |
| System Name and Description       |
| If applicable, list all the database instances to which access is requested: |
|       |       |       |
|       |       |       |
|       |       |       |
| In general, how would you characterize the services you will be performing *(check all that apply)*[ ]  Incident Investigation [ ]  New System/Equipment [ ]  System Upgrade [ ]  Repair/Troubleshooting [ ]  Routine Maintenance[ ]  Other:       |
| Special Instructions       |
| **Is system administrator access required?** [ ]  Yes [ ]  No | **Is physical access to a secured area required?**[ ]  Yes [ ]  No |
| Where will service be performed?[ ]  Onsite [ ]  Remotely (explain how):       |
| Frequency of access[ ]  Daily [ ]  Periodically [ ]  Routinely [specify schedule]:       |
| Access Duration (Check one. If Other is checked, fill in start/stop dates and times.) **IMPORTANT**: This access may not extend beyond the contracted end date.[ ]  Contract Start-End Dates [ ]  Other: Start Date:      , Start Time:       -- End Date:      , End Time:       |

# Acknowledgment of Confidentiality and Appropriate Use of Access

All third-party service providers (vendors and consultants) who are granted temporary access to networks, systems and data of California State University, Los Angeles are entrusted with the maintenance of the security and confidentiality of institutional systems, records and information. All third-party service providers are expected to adhere to the following rules:

1. Unauthorized use or access to institutional system records and information is prohibited.
2. Access granted under this request is only for work associated with the programs of the California State University, Los Angeles and/or the California State University system.
3. Access, if granted, will be only for the period stated in this document. Thereafter, all accounts, passwords and access associated with this request will be revoked immediately.
4. If system administrator rights are granted, they will apply only to the specific actions identified in this document. Performance of any unrelated and/or unauthorized actions will result in the immediate termination of system administrator rights.
5. To maintain account and password security, disclosure of any account information and passwords to anyone is prohibited.
6. Exhibiting or divulging the contents of any record or report to any person except in the execution of normal duties and responsibilities is prohibited.
7. Using any data accessed with any accounts associated with this request for gender and/or ethnicity-based recruiting/selections, unauthorized fund raising, or other barred activities is prohibited.
8. Personally benefiting or allowing others to benefit from any confidential information gained by virtue of network or system access is prohibited.
9. Directly or indirectly causing the inclusion of any false, inaccurate or misleading entries into any records or reports is prohibited.
10. No official record or report or copy thereof, whether paper or electronic, may be removed from the office where it is maintained.
11. All systems must be completely exited before leaving a computer or server unattended.
12. All University security standards and guidelines for access, use, retention and disposal of data must be maintained.
13. Vendors and consultants must protect any accessed confidential information according to industry-accepted standards and no less rigorously than it protects its own customers’ confidential information.
14. Vendors and consultants must hold confidential information in strict confidence, and must access information only for the explicit business purposes outlined in its contract with the University.
15. Vendors and consultants must ensure compliance with the protective conditions outlined in its contract with the University.
16. Vendors and consultants will return or securely destroy all confidential information upon completion of its contract with the University.
17. Vendors and consultants agree to follow the ITS change management process and procedures for any production system changes, including shutting down and rebooting a system.
18. Violation of security precautions to protect confidential information may be a crime, and may be subject to appropriate legal action and/or criminal prosecution.

THIRD PARTY NAME\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Vendors and consultants must notify the University immediately upon the termination of any individuals connected with this project or contract so that account access, passwords, remote diagnostic access or other forms of access can be revoked.
2. Vendors and consultants must not aid, or act in conspiracy with, anyone to violate any of the rules listed above.

I have read and understand all the rules listed above, and I agree to abide by them. I will maintain the security and confidentiality of any institutional records and information entrusted to me in the manner stated in the rules above. If there is reason to believe there is a violation of University computer security and/or state and federal laws, statutes and regulations, I understand that my access, account, and account contents may become subject to monitoring and examination by authorized personnel.

Applicant Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Department Approval

*Sign only if you approve this request. Otherwise, check “Request Denied” and give the reason for denial.*

***Departments are responsible for notifying IT Security and Compliance if this third-party contract or individual is terminated.***

|  |  |
| --- | --- |
| Department Chair/Manager  | Date |
| Dean/Director | Date |
| [ ]  **Request Denied. Reason:** |

# Data Owner Approvals

*If a data owner is responsible for information contained in the system being accessed, then this section must be completed by the data owner(s). Otherwise, this section may be skipped.*

|  |
| --- |
| Role(s) assigned to this user:  |
| **Conditions Applied to this Request** *(Note: If conditions are not met, access may be revoked and renewal may be denied)* |
|  |
|  |
| **Data Owner Approval Signatures** *(Sign only if you approve this request. Otherwise, check “Request Denied” and give the reason for denial.)* |
| System Data Owner | Date |
| Functional Data Steward(s)  | Date |
| [ ]  **Request Denied. Reason:**  |

# ITS Approvals

*Sign only if you approve this request. Otherwise, check “Request Denied” and give the reason for denial.*

|  |  |
| --- | --- |
| Assistant Director, IT Infrastructure Services | Date |
| Director, IT Infrastructure Services | Date |
| Director, Enterprise Applications | Date |
| Director, IT Security and Compliance | Date |
| [ ]  **Request Denied. Reason:** |