



SPECIAL ALERT

STATE OF
CALIFORNIA



Update from the California Student Aid Commission

June 20, 2023

GSA 2023-30

TO: High School Counselors
Financial Aid Administrators

FROM: Tae Kang *Tae Kang*
Deputy Director, Program Administration & Services Division

SUBJECT: **Renewal of WebGrants Access**

This Special Alert from the California Student Aid Commission (Commission) notifies institutions that System Administrator access must be renewed biennially. System Administrators (SA) will lose access if the institution does not submit the WebGrants Access Request – System Administrator form before the SA's effective end date.

To renew WebGrants access for two years, please submit the [WebGrants System Administrators Access Request form](#). All institution types may utilize the form to request WebGrants access.

For best results, please download the form to your computer, open using Adobe Acrobat, complete electronically, digitally sign it, and submit it to webgrantsaccess@csac.ca.gov. Please send renewal documents at least a month in advance to avoid interruption in your access to the WebGrants system.

In an effort to assist with accurate and timely completion of both sections of the document, the Commission has identified the following areas where errors are commonly made.

WebGrants System Administrator's Access Request Form

- Submit one Access Request Form for each System Administrator (SA).
- An institution can only have two active SAs. To remove access for an SA, select the "Disable Account" option in Section 2 of the form and provide the name or User ID you would like removed. Disabling an account can be done when adding a new SA or as a standalone submission. The Authorized Official (AO) must sign off on any *Disable Account* requests.
- The AO listed on the Access Request Form must be the same individual listed on the Confidentiality Agreement on page two of the WebGrants System Administrators Access Request Form.
- All accounts must be registered with an email address that is associated with the institution (for example, john.smith@centralcitycollege.edu). E-mail addresses from non-institutional service providers (Yahoo!, Gmail, Hotmail, etc.) are not allowed due to the sensitive information that may be provided in WebGrants notifications.

- To check your or your user's WebGrants access end date, from the WebGrants home screen, Home > Admin > User Access Report.

WebGrants Information Security and Confidentiality Agreement

- The AO can designate up to two individuals as the institution's SAs.
- The AO and the SAs cannot be the same individual. The AO will not have authorization to access the WebGrants.
- If the AO and the SAs are different at the institution's additional location(s), a separate Access Request Form must be completed for each additional institution location.

User Access

- The Institution's SAs will ensure that all Institution employees or agents who require WebGrants access will sign a [WebGrants User Access Request Form](#) prior to being granted access to the WebGrants System.
- CSAC does not need to be notified when School Users are added, renewed, or disabled for your institution, but schools must keep their User Access Request forms on-site for auditing purposes.
- Article VI, Item B(2) of the [Cal Grant Program Institutional Participation Agreement](#) states that user access is granted for a period of time not to exceed two (2) years.
- Users must complete annual training in the areas of information security, privacy, and confidentiality to renew access. This security training is [offered by CSAC](#) or can be provided by the institution.
- To check your User WebGrants access end date, from the WebGrants home screen, select the person icon next to the Logout button. Under your user profile, it lists your effective end date.

Need to contact us?

- School Support phone number: (888) 294-0153
- E-mail: schoolsupport@csac.ca.gov or webgrantsaccess@csac.ca.gov
- To report potential security issues: iso@csac.ca.gov

Working together to effectively promote education beyond high school!