

**CORPORATE SOCIAL RESPONSIBILITY**

# User Management Webinar

Adding Users & Assigning Permissions



# Meet your Trainer...

## Zoey Lake

Senior Training Specialist

Corporate Social Responsibility



# Agenda

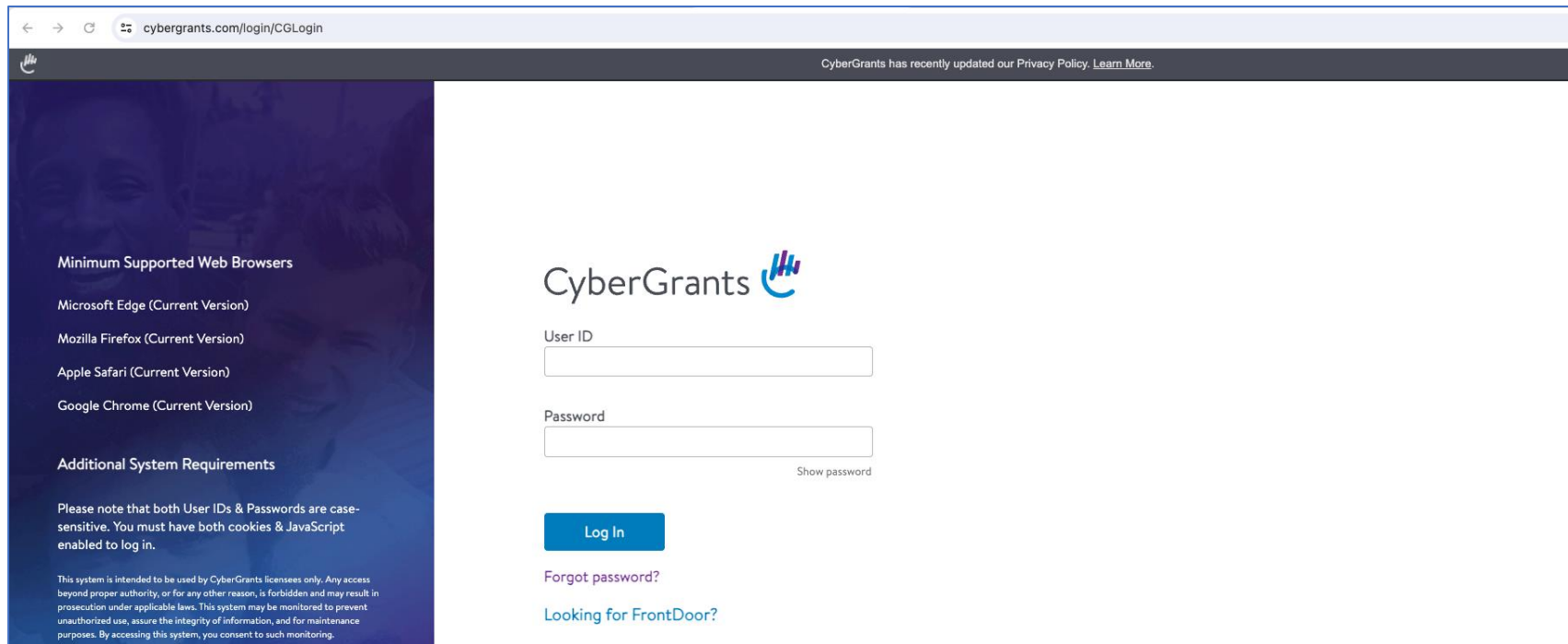
1. Logging in to your account
2. Getting familiar with the admin tab
  - Sandbox vs. production
  - Navigating your tabs
3. Adding and editing your user profile
4. Adding internal users
5. Assigning a user license
6. Security settings and user roles
7. Adding donors
8. Donor permissions and donor roles



# Logging in to your account

# Logging in during and after implementation

- During and after implementation you can log in with your username and password at [www.cybergrants.com/login/CGLogin](http://www.cybergrants.com/login/CGLogin)
- If you are implementing a new program with us for the first time, you may plan on shifting to SSO in the future.
- If you are an existing client, but are implementing a new program type, you can continue to log in as usual.



cybergrants.com/login/CGLogin

CyberGrants has recently updated our Privacy Policy. [Learn More.](#)

**Minimum Supported Web Browsers**

- Microsoft Edge (Current Version)
- Mozilla Firefox (Current Version)
- Apple Safari (Current Version)
- Google Chrome (Current Version)

**Additional System Requirements**

Please note that both User IDs & Passwords are case-sensitive. You must have both cookies & JavaScript enabled to log in.

This system is intended to be used by CyberGrants licensees only. Any access beyond proper authority, or for any other reason, is forbidden and may result in prosecution under applicable laws. This system may be monitored to prevent unauthorized use, assure the integrity of information, and for maintenance purposes. By accessing this system, you consent to such monitoring.

**CyberGrants**

User ID

Password  
 [Show password](#)

[Log In](#)

[Forgot password?](#)

[Looking for FrontDoor?](#)

# License types for internal users

# Full and limited license types

Your license allotment will be determined and included in your contract. If you require more licenses than you have available, you can make adjustments outside of the renewal period by contacting your account manager.

**Full Licenses** allow users to access all parts of all products. Limitations may be placed based on user's security level. Most users will require full licenses.

**Limited Licenses** allow a user to log in, send and receive emails, access and review grant applications, print applications, and provide approval or recommendation status. Limited licenses are intended to be used by grant reviewers who do not have other budgetary or grant making responsibilities.

# Security levels for internal users



# Security Levels (Full License Users)

Security Level	Permission Overview	Module (tab) Access
Administrator	<p>Highest level of system access. By default has access to all tabs</p> <p>Admins can add, delete, or edit information in the system</p> <p>Admins can grant or restrict access for other users</p>	All Tabs
Basic	<p><b>Most common security level.</b></p> <p>Basic users can add/edit information on requests they own and organization records.</p> <p>Basic users cannot change system configuration.</p> <p>Basic users cannot edit another user's requests</p>	Dashboard Main Reports Mail
Budget	<p>Same as Basic users, but also has access to the Budget.</p> <p>Cannot change program configuration but can make financial/budget updates.</p>	Dashboard Main Reports Mail Budget
Viewer	<p>A viewer can access all requests in read-only mode by default</p> <p>A viewer can participate in the approval process</p> <p>A viewer can access shared and scheduled reports, but they cannot create their own ad-hoc reports.</p>	Dashboard Main Reports Mail

# Security Levels (Limited License Users)

Strict users cannot access records that they do not own or are able to decision. Strict users are implemented for security reasons if the nature of grant funding should not be visible to users not involved with the grant directly. Strict users cannot transfer ownership to another user.

Security Level	Permission Overview	Module Access
Strict Basic	Similar to Basic users, Strict Basic users can send emails, edit organization information, and edit request information, but only for request types that they are the owner of, or that require their action for approval.	Dashboard Main Mail
Strict Viewer	Strict Viewer is the most restrictive security level option. Strict Viewers can only view and update approval status of requests that are currently pending their review. After they have reviewed a request, they will continue to have read-only access	Dashboard Main Mail

# Grouping internal users by user role

# Internal User Roles

User Roles are available to provide additional granularity for system access beyond the more broad security level settings.

User Roles can be configured to limit or provide access to certain proposal types or system admin functions. The majority of User Role settings are restrictive in nature.

Please contact your Implementation Consultant or Account Manager for more information if you would like to utilize User Roles.

# Donor Management

# Employee Access to Giving Programs

For Employee Engagement Programs (Giving & Matching or Volunteerism products) Employees are referred to as Donors.

Donors do not require individual licenses. They will access a donor portal, not the “backend” administrative site.

Donors are managed via an HR feed after your implementation is completed. During implementation you will need to manually set up a couple of test donors.

Test donors should use realistic data so that UAT can be accurately completed.

Test donors cannot be manually deleted, but much of the information can be edited.

Please be conscientious when creating test users.

# Restricting donor access by donor roles

# Event Management and other applications

Donor Roles are most commonly used to restrict access to Event Creation.

Users that are assigned the “Event Manager” role may submit Volunteer Event Opportunities via the Event Management page. Other donors may sign up for these events, but will have no access to create events of their own

Donor Roles can also be used to restrict access to specific portlets, program types, or set differing eligibility rules.



# Feedback & Training Survey

Please fill out the survey (link in chat or scan QR code):



Thank You for Attending!

